Draft Investigatory Powers Bill

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

November 2015

Cm 9152

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 9781474125659
Web ISBN 9781474125666

ID 30101501 11/15

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

CONTENTS

FOREWORD FROM THE HOME SECRETARY

The means available to criminals, terrorists and hostile foreign states to co-ordinate, inspire and to execute their plans are evolving. Communications technologies that cross communications platforms and international borders increasingly allow those who would do us harm the opportunity to evade detection.

The use of investigatory powers is vital to locate missing people, to place a suspect at the scene of a crime or to identify who was in contact with whom. Powers to intercept communications, acquire communications data and interfere with equipment are essential to tackle child sexual exploitation, to dismantle serious crime cartels, take drugs and guns off our streets and prevent terrorist attacks.

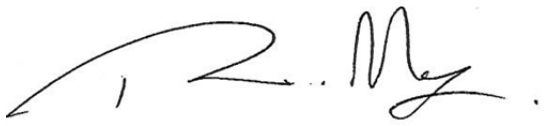
The Government is committed to ensuring law enforcement and the security and intelligence agencies have the powers they need to keep us safe in the face of an evolving threat and an increasingly complicated communications environment. The Investigatory Powers Bill will do that in a way that ensures the use of those powers is subject to robust safeguards and visible, effective oversight.

Over the past year, three independent reviews have been undertaken into the use and oversight of investigatory powers: by the Intelligence and Security Committee of Parliament, the Independent Reviewer of Terrorism, David Anderson QC, and a panel convened by the Royal United Services Institute. Between them, they made nearly 200 recommendations.

The Government has paid attention to the findings of those reviews. The draft Investigatory Powers Bill that has been published for pre-legislative scrutiny and public consultation builds on their recommendations to bring together all of the powers available to law enforcement and the security and intelligence agencies to acquire communications and communications data and make them subject to enhanced, consistent safeguards.

The provisions in the draft Bill are the product of discussion with industry, academia, technical experts and civil liberties groups. They seek to protect both privacy and security by improving transparency and through radical changes to the way investigatory powers are authorised and overseen. The draft Bill only proposes to enhance powers in one area – that of communications data retention – and then only because a strong operational case has been made.

The draft Bill provides a basis for further consultation over the coming weeks and months before a revised Bill is introduced to Parliament in the New Year. The issues covered in this draft Bill are matters of national importance and will rightly be subject to scrutiny and debate. I hope that you will take the time to share your views.



Rt Hon Theresa May MP

DRAFT INVESTIGATORY POWERS BILL: GUIDE TO POWERS AND SAFEGUARDS

GUIDE TO POWERS AND SAFEGUARDS: CONTENTS

CONTEXT

1. The draft Investigatory Powers Bill will govern the use and oversight of investigatory powers by law enforcement and the security and intelligence agencies. It builds on the work of three comprehensive reviews undertaken over the past year. 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 law enforcement and the security and intelligence agencies in the future. Collectively, they proposed reforms to the way these powers are overseen and recommended the introduction of consistent safeguards and greater openness.

3. The draft 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 draft Bill will do three things:

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

- Second, the draft Bill will radically overhaul the way these powers are authorised and overseen. It will introduce a 'double-lock' for interception warrants, so that, following Secretary of State authorisation, these – and other warrants – cannot come into force 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 draft 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.

4. This guide provides an overview of the key provisions in the draft Investigatory Powers Bill. It should be read alongside the draft Bill and the accompanying Explanatory Notes, which have been published at the same time for public consultation and pre-legislative scrutiny.

OVERSIGHT

What happens now?

5. 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.

6. 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 how public authorities use their interception and communications data powers under RIPA and powers under section 94 of the Telecommunications Act.

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

- The Intelligence Services Commissioner (ISCom) who oversees how the intelligence agencies use 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

7. 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?

8. 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 has all the skills and resources it needs.

What will happen in the future?

9. The draft Bill will create a single new independent and more powerful 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 how law enforcement and the security and intelligence agencies use the powers and capabilities available to them.

10. The IPC will be a senior judge and with his supporting staff will have three key roles. First, to authorise and approve the use of investigatory powers. Judicial Commissioners, who will be serving or former High Court judges, will undertake this role. Secondly, there will be an inspection role. The IPC will audit compliance and undertake investigations. Judicial Commissioners will undertake this role and will be supported by a team of expert inspectors.

11. Thirdly, the new 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 what he finds in the course of his work. He will also publish guidance when it is required on the proper use of investigatory powers. The Commissioner will have a strong public profile and active media and online presence so that he 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.

12. The draft 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 draft Bill?

- **The draft 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 a staff of experts**

- **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 of the powers under the draft 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 and the security and intelligence agencies**

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

INTERCEPTION

What is it?

13. Interception is the making available 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?

14. 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?

15. 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 (EWB) of the United Kingdom 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?

16. 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. The draft 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?

17. In line with the recommendations made by David Anderson QC, RUSI and the ISC, the draft 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 (see paragraph 15).

18. 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 draft 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 warrants issued by the Secretary of State (or a Scottish Minister) before they come into force. This will provide for a 'double- lock' of Executive and judicial approval for the use of interception.

19. 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 his findings annually.

What are the key provisions in the draft Bill?

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

- **The draft 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 must, as well as Ministers, approve warrants before they come into force**

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

- **The powers under which stored communications may be accessed will be limited and the use of covert powers made subject to IPC oversight**

Interception Case Study: Serious Crime Investigation

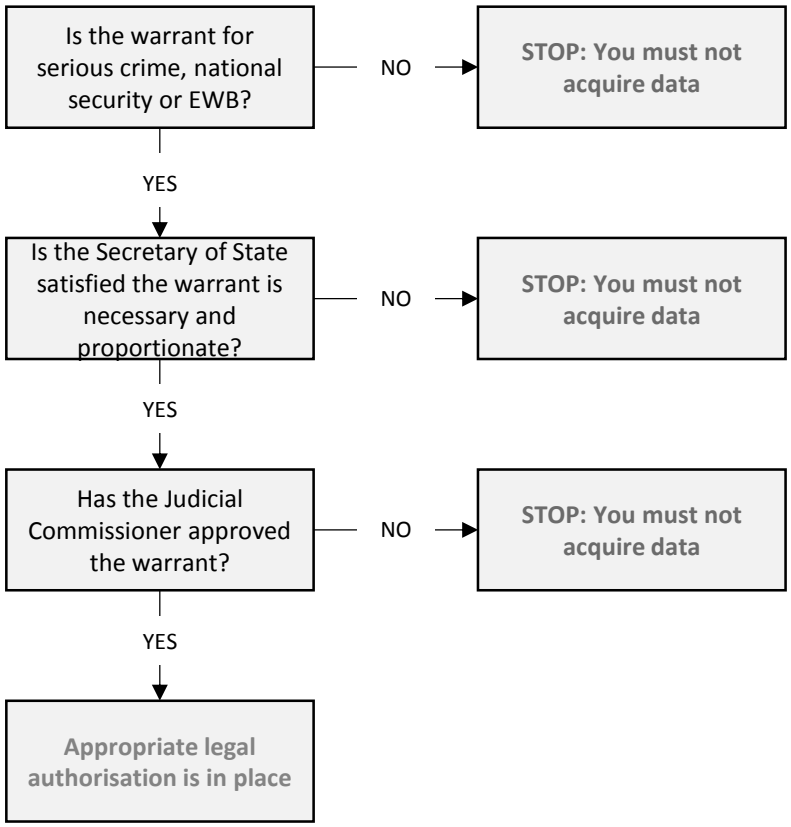
A criminal investigation was underway into a pattern of escalating violence between a number of rival organised crime groups, including street gangs linked to the London drug economy, operating across the capital.

Intelligence derived from interception indicated a conflict between 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, disrupting the supply of Class A drugs, preventing further loss of life 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 and over 100 arrests.

IP Bill: Interception Authorisations



COMMUNICATIONS DATA

What is it?

20. 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 or an itemised bill. Law enforcement and the security and intelligence agencies may acquire this data from Communications Service Providers (CSPs) who may be required to retain it.

Why do we need it?

21. 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?

22. 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. They must be necessary and proportionate. 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 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?

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

What safeguards will there be?

24. 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 and the security and intelligence agencies and CSPs and to facilitate lawful acquisition of communications data. They also play a quality control role, ensuring that applications meet the required standards.

25. Once it has gone through the SPoC, the authorisation will be signed off by a Designated Person (DP), who is independent of the investigation for which the communications data is needed. The draft Bill will provide a power that can ensure public authorities that 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.

26. 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 draft Bill?

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

- **Other powers for acquiring communications data will be repealed**

- **A new criminal offence of wilfully 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 will be updated to reflect changes in the way people communicate**

- **CSPs will be able to be required to retain ICRs. Access to this information will be limited, targeted and strictly controlled**

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.

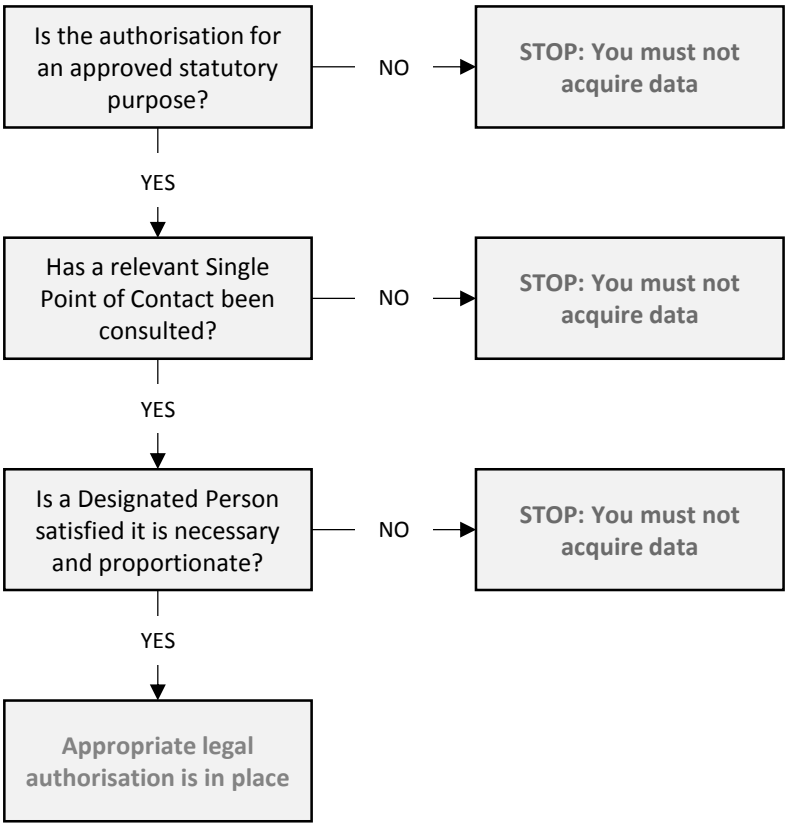
In the early stages of the inquiry neither child had any physical injuries consistent with sexual abuse; there were no witnesses and no substantive evidence to support charges for the serious sexual offences that were suspected. Communications data was used alongside other investigative techniques which 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?

27. 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?

28. Where necessary and proportionate, law enforcement agencies and the security and intelligence agencies need to be able to access communications or other private 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?

29. 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 general property interference powers in the Intelligence Services Act 1994 and the Police Act 1997. A draft Code of Practice was published earlier this year and governs the use of equipment interference powers by the security and intelligence agencies.

What will happen in the future?

30. Building on recommendations made by David Anderson QC and the ISC, the draft 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. It will limit the use of other powers to obtain stored communications and private information directly from devices in the absence of a warrant and will introduce new, enhanced safeguards. 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 only.

What safeguards are there?

31. Use of these powers by the security and intelligence agencies or the armed forces currently requires authorisation by the Secretary of State. Authorisations for law enforcement may be issued by the Chief Constable or equivalent. 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.

32. The IPC will oversee the use of equipment interference powers by law enforcement, the security and intelligence agencies, and the armed forces. He will ensure that the detailed safeguards set out in the legislation and accompanying Codes 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 report publicly on what he finds.

What are the key provisions in the draft Bill?

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

- **It will strengthen the authorisation regime so that warrants will only come into force having been approved by a Judicial Commissioner**

- **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**

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

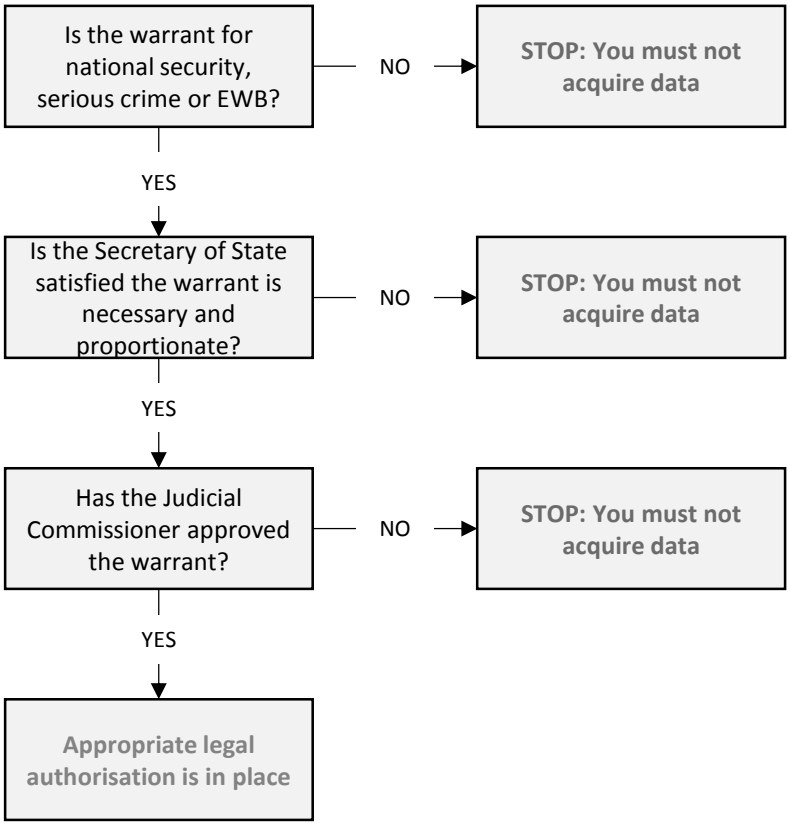
- **The draft Bill will create a new obligation on domestic CSPs to assist in giving effect to equipment interference warrants**

EI Case Study: Attempted Murder

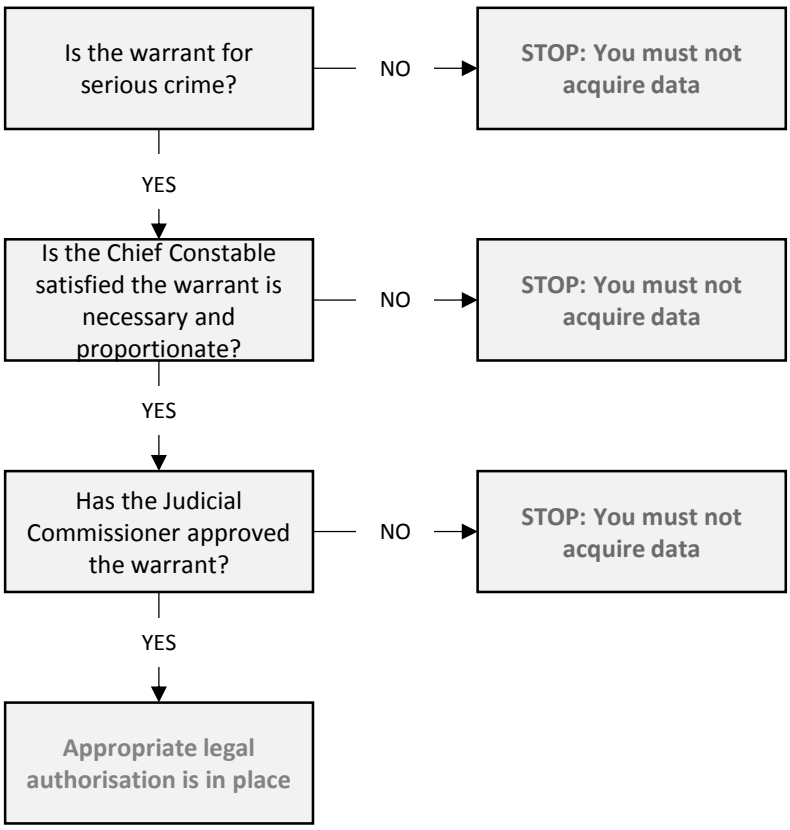
Equipment interference, when used with other intelligence gathering techniques, is vital in time-limited cases of threat-to-life when the police need to act quickly.

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?

33. Access to bulk data is crucial to monitor known and high-priority threats but is also a vital tool in discovering new targets and identifying emerging threats. 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?

34. 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 large volumes of data enables the security and intelligence agencies to piece together communications and other data and identify patterns of behaviour. This enables them to:

- Establish links between known subjects of interest, improving understanding of their behaviour and the connections they are making or the multiple communications methods they may be using; and,
- Search for traces of activity by individuals who may not yet be known to the agencies but who surface in the course of an investigation, or to identify potential threats and patterns of activity that might indicate national security concern.

35. 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?

36. 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.

37. 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.

What will happen in the future?

38. David Anderson QC, the ISC of Parliament and the panel convened by the 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?

39. The draft Bill will limit the ability to apply for a bulk warrant to the security and intelligence agencies. It will require that any bulk warrant must be necessary in the interests of national security. Warrants will be issued by the Secretary of State and must be approved by a Judicial Commissioner before coming into force.

40. The draft 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.

41. 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 related communications data that may be acquired under a bulk interception warrant. The draft 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.

42. 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 by these means, he or she will need to seek a targeted interception or equipment interference warrant from the Secretary of State and a Judicial Commissioner.

43. The draft 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 related communications data (CD that is within or connected to the content of a communication) only.

What are the key provisions in the draft Bill?

- **The draft 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**

- **The issue of a bulk warrant must be 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**

- **Bulk warrants will only come into force once they have been authorised by the Secretary of State and 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**

- **Additional safeguards will apply in respect of content acquired under bulk interception and bulk equipment interference warrants relating to persons in the UK**

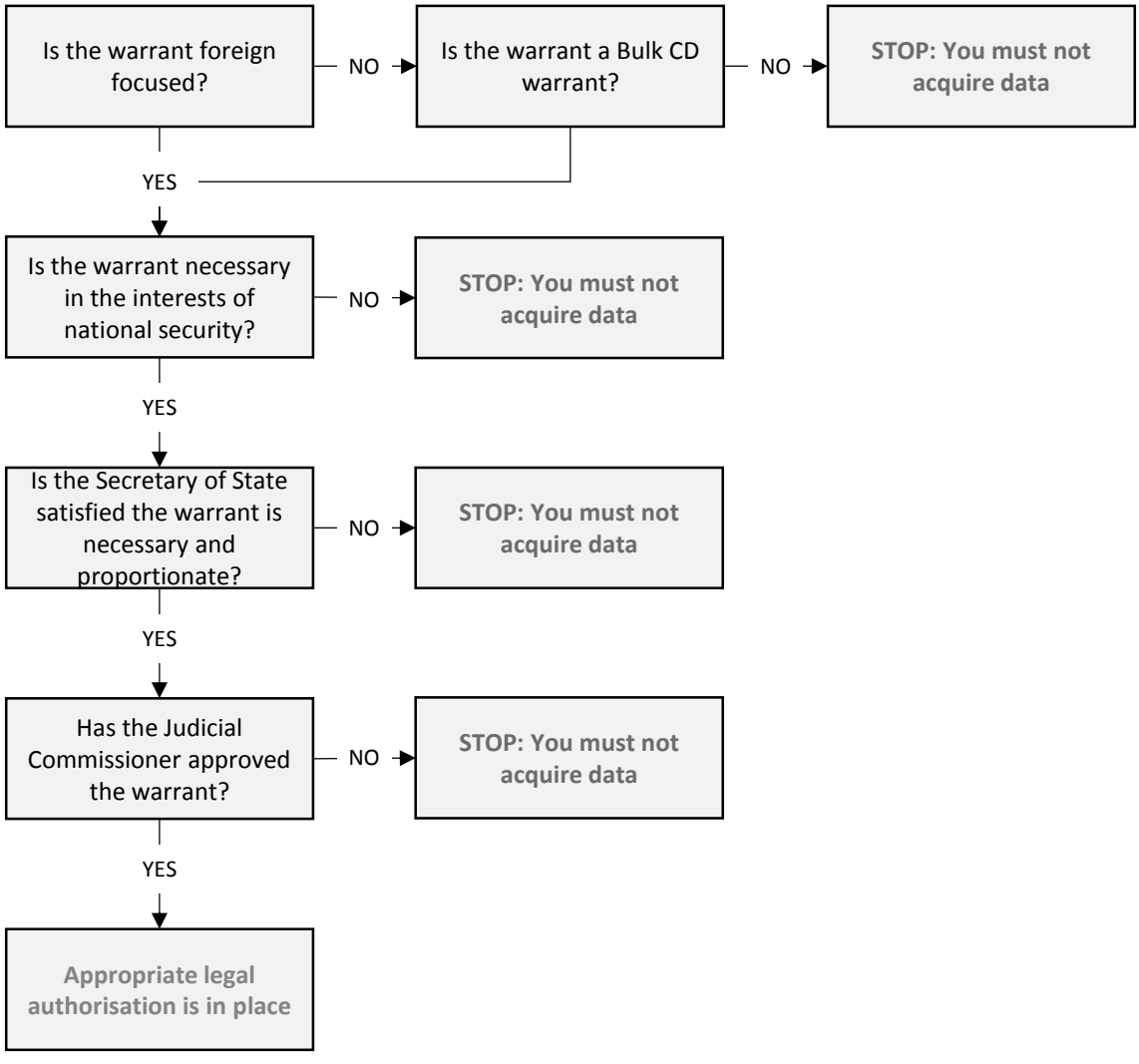
- **The draft Bill also provides additional safeguards for the acquisition and use of bulk personal datasets by the security and intelligence agencies**

Bulk powers Case Study

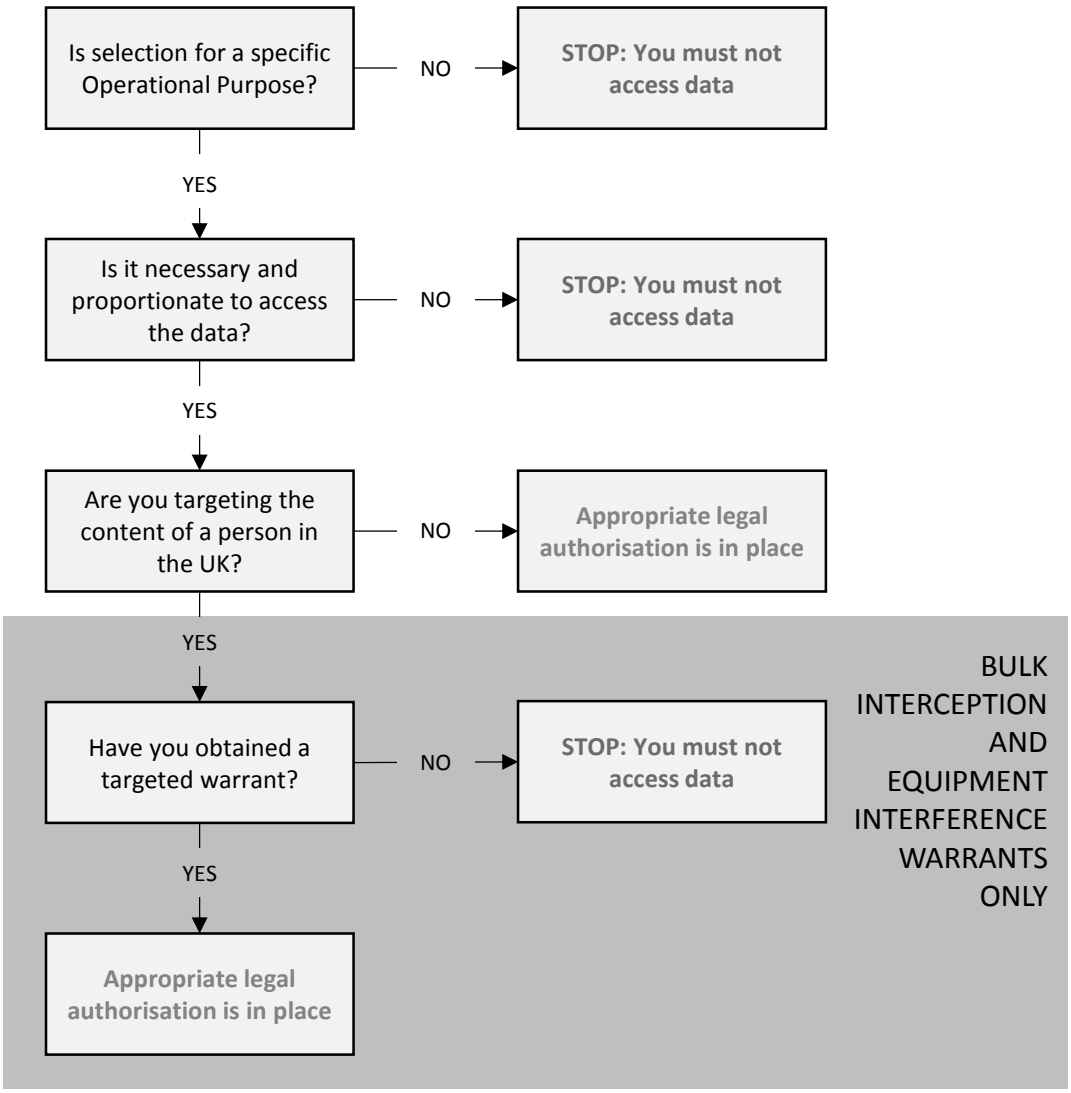
A group of terrorists were planning a firearms-based attack in the UK. The group had links to known terrorists overseas and as such the threat which they posed was credible. Close monitoring of the group by the police and intelligence agencies was necessary to ensure that their plans could be disrupted.

The ability to access communications data in bulk was critical to averting this plot. Using communications data, the agencies were quickly able to obtain identifying details for members of the group without needing to resort to more intrusive powers. With the network successfully identified, the intelligence agencies and police were able to put targeted disruptive measures in place to prevent this attack occurring.

IP Bill: Authorisation of Bulk Warrants



IP Bill: Access to data obtained under Bulk Warrants



INTERNET CONNECTION RECORDS

What are they?

44. A kind of communications data, an ICR is a record of the internet services a specific device has connected to, 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.

45. 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?

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

- 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?

47. There is no requirement in law for CSPs to keep ICRs. Requests for ICRs can therefore only be made on a forward-looking basis where it is necessary and proportionate to do so. As a result, law enforcement agencies can often only paint a fragmented intelligence picture of a known suspect. 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. 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%) cannot be progressed and would require the provisions in the Investigatory Powers Bill to have any prospect of doing so.

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

48. 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?

49. Internet service providers will be required to keep ICRs for a maximum period of 12 months. This will be invaluable to law enforcement to prevent and detect crime, to protect our 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?

50. Applications to acquire ICRs can only be approved using the stringent application process for communications data requests (see paragraph 24-25 above) and only for a limited set of statutory purposes and subject to strict controls. Local authorities will be prohibited from acquiring ICRs.

PROTECTIONS FOR COMMUNICATIONS INVOLVING SENSITIVE PROFESSIONS

51. 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

52. 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 therefore not 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.

53. 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 Designated Person 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.

54. 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.

55. The Investigatory Powers 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 draft 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 Warrant

56. 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 involves a higher level of intrusion, particularly where particularly confidential or sensitive information is involved.

57. The Investigatory Powers Bill will introduce a two stage authorisation process such that a Secretary of State must personally issue the warrant, and before it comes into force a Judicial Commissioner must approve the authorisation. Strict procedures will govern how any information collected under the warrant is used, kept and destroyed. Codes of Practice issued under the draft Bill in respect of interception and equipment interference (including in

bulk) will make provision for additional protections relating to persons in sensitive professions.

58. 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, such as that which is legally privileged. They must also notify the IPC that sensitive material has been obtained as soon as it is practical to do so.

59. 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.

60. The draft 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 an MP's communications. This will cover all warrants for targeted interception and all 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.

OBLIGATIONS ON COMMUNICATIONS SERVICE PROVIDERS

61. 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 using equipment interference powers.

CSP Obligations

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

a. The 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.

63. The Investigatory Powers Bill will bring together these obligations in a single, comprehensive piece of legislation. It will provide an explicit obligation on CSPs to assist in giving effect to equipment interference warrants. Only intercepting agencies will have the ability to serve such warrants, which must be authorised by the Secretary of State. The draft Bill will not impose any additional requirements in relation to encryption over and above the existing obligations in RIPA.

64. The draft Bill will provide for the Secretary of State to require CSPs to maintain permanent capabilities relating to the powers under the draft 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.

65. The new power will also require CSPs to provide wider assistance to law enforcement and the security and intelligence agencies in the interests of national security. 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.

66. The ability for CSPs to appeal obligations will be strengthened through the draft Bill. The draft 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 Investigatory Powers Commissioner. The circumstances in which appeals will be permitted will be broadened to take account of CSPs' changes to services and infrastructure.

Overseas Companies

67. 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 last year through DRIPA. Other investigatory powers (such as data retention) may rely on the support of overseas companies.

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

What are the key provisions in the draft Bill?

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

- **The draft Bill will provide for notices to be given to CSPs to maintain capabilities relating to the use of powers under the draft 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**

BULK PERSONAL DATASETS

What are they?

69. 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 purposes of analysis in the security and intelligence agencies. Examples of these datasets include the telephone directory or the electoral roll.

Why do we need them?

70. 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?

71. 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?

72. The Investigatory Powers Bill will significantly enhance the safeguards that apply to the acquisition and use of BPD under the Security Service Act 1989 and the Intelligence Services Act 1994.

What safeguards will there be?

73. The Secretary of State will have to approve class-based warrants for a period of six months if it is necessary and proportionate for the agency to have access to that class of BPDs. As will be the case for interception and equipment interference authorisations, a Judicial Commissioner must also approve the warrant. If the agencies need access to a BPD that is not covered by a class warrant they will need to seek a specific warrant which is also subject to both Secretary of State authorisation and Judicial Commissioner approval.

74. 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.

75. 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 draft Bill?

- **The draft Bill will provide for new safeguards in respect of the security and intelligence agencies' acquisition and use of BPD**

- **Class or specific warrants for the security and intelligence agencies will be issued by the Secretary of State and will be approved by a Judicial Commissioner.**

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 from 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	5 law enforcement agencies, MI5, GCHQ, SIS and the Ministry of Defence 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 will outline further details.
Communications Data (CD)	Obtain CD, usually via Communications Service Providers (CSPs)	Public authorities provided with the ability to acquire CD and statutory purposes will listed in the Bill.	Must be authorised by a designated person (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 private data covertly 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.	Secretary of State authorises warrants for MOD and security and intelligence agencies. Chief Constable authorises law enforcement use. All warrants subject to Judicial Commissioner check before coming 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	Secretary of State authorises warrants, subject to approval by a Judicial Commissioner 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 separate targeted warrant.	
Bulk Personal Datasets (BPD)	Additional safeguards for the acquisition and use of BPD	MI5, GCHQ, SIS Purposes: National Security, Serious Crime and Economic well-being	Authorisation to acquire particular classes of BPD issued by Secretary of State and subject to approval by a Judicial Commissioner	Examination of any material must be necessary for a specific Operational Purpose, authorised by a Secretary of State and approved by a Judicial Commissioner.	

CONSULTATION

76. The draft Investigatory Powers Bill will be subject to pre-legislative scrutiny by a Joint Committee of Parliament. The Committee will issue its own call for evidence and will invite views from the public and interested parties.

77. The Government welcomes views on the issues covered in the draft Bill and will continue to engage with industry, academia and civil liberties groups throughout the pre-legislative scrutiny period. If you would like to share your views on any of the issues addressed in the draft Bill directly with the Government rather than the Joint Committee, please contact us at: investigatorypowers@homeoffice.gsi.gov.uk.

EXPLANATORY NOTES

Explanatory notes are published alongside the draft Bill.

EUROPEAN CONVENTION ON HUMAN RIGHTS

[Name to be replaced] has made the following statement under section 19(1)(a) of the Human Rights Act 1998:

In my view the provisions of the Investigatory Powers Bill are compatible with the Convention rights.

Investigatory Powers Bill

CONTENTS

PART 5

EQUIPMENT INTERFERENCE

Warrants under this Part

Power to issue warrants

Further provision about warrants

Implementation of warrants

Supplementary provision

PART 6

BULK WARRANTS

CHAPTER 1

BULK INTERCEPTION WARRANTS

Bulk interception warrants

Duration, modification and cancellation of warrants

Implementation of warrants

Restrictions on use of intercepted material etc.

Interpretation

CHAPTER 2

BULK ACQUISITION WARRANTS

Bulk acquisition warrants

Duration, modification and cancellation of warrants

A

B I L L

TO

Make provision about the interception of communications and the acquisition, retention and disclosure of communications data; to make provision about equipment interference and bulk personal datasets; to establish Judicial Commissioners and make provision about them and other oversight arrangements; to make further provision about investigatory powers and national security; to amend sections 3 and 5 of the Intelligence Services Act 1994; and for connected purposes.

BE IT ENACTED by the Queen's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:—

PART 1

GENERAL PROTECTIONS

Overview of Act

1 Overview of Act

(1) This Part sets out offences and other penalties in relation to—
  (a) the unlawful interception of communications, and
  (b) the unlawful obtaining of communications data.

(2) It also abolishes various general powers to obtain communications data and restricts the circumstances in which equipment interference can take place.

(3) Other protections exist by virtue of the Human Rights Act 1998 and elsewhere in the law.

(4) Part 2 and Chapter 1 of Part 6 set out circumstances in which the interception of communications is lawful and make further provision about the interception of communications.

(5) Part 3 and Chapter 2 of Part 6 set out circumstances in which the obtaining of communications data is lawful and make further provision about the obtaining of communications data.

(6) Of the rest of the Act—

(a) Part 4 makes provision for the retention of certain communications data,

(b) Part 5 and Chapter 3 of Part 6 deal with equipment interference warrants,

(c) Part 7 deals with bulk personal dataset warrants,

(d) Part 8 deals with oversight arrangements for regimes in this Act and elsewhere, and

(e) Part 9 contains miscellaneous and general provisions including amendments to sections 3 and 5 of the Intelligence Services Act 1994 and provisions about national security and combined warrants and authorisations.

Prohibitions against unlawful interception

2 Offence of unlawful interception

(1) A person commits an offence if—

(a) the person intentionally intercepts any communication in the course of its transmission by means of—

(i) a public telecommunication system,

(ii) a private telecommunication system, or

(iii) a public postal service,

(b) the interception is carried out in the United Kingdom, and

(c) the person does not have lawful authority to carry out the interception.

(2) But it is not an offence under subsection (1) for a person to intercept a communication in the course of its transmission by means of a private telecommunication system if the person—

(a) is a person with a right to control the operation or use of the system, or

(b) has the express or implied consent of such a person to carry out the interception.

(3) Sections 3 and 4 contain provision about—

(a) the meaning of "interception", and

(b) when interception is to be regarded as carried out in the United Kingdom.

(4) Section 5 contains provision about when a person has lawful authority to carry out an interception.

(5) For the meaning of the terms used in subsection (1)(a)(i) to (iii), see sections 193 and 194.

(6) A person who is guilty of an offence under subsection (1) is liable—

(a) on summary conviction in England and Wales, to a fine;

(b) on summary conviction in Scotland or Northern Ireland, to a fine not exceeding the statutory maximum;

(c) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.

(7) No proceedings for any offence which is an offence by virtue of this section may be instituted—

(a) in England and Wales, except by or with the consent of the Director of Public Prosecutions;

(b) in Northern Ireland, except by or with the consent of the Director of Public Prosecutions for Northern Ireland.

3 Definition of "interception" etc.

Interception in relation to telecommunication systems

(1) For the purposes of this Act, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if—

(a) the person does a relevant act in relation to the system, and

(b) the effect of the relevant act is to make some or all of the content of the communication available, at a relevant time, to a person who is not the sender or intended recipient of the communication.

For the meaning of the "content" of a communication, see section 193(6).

(2) In this section "relevant act", in relation to a telecommunication system, means—

(a) modifying, or interfering with, the system or its operation;

(b) monitoring transmissions made by means of the system;

(c) monitoring transmissions made by wireless telegraphy to or from apparatus that is part of the system.

(3) For the purposes of this section references to modifying a telecommunication system include references to attaching any apparatus to, or otherwise modifying or interfering with—

(a) any part of the system, or

(b) any wireless telegraphy apparatus used for making transmissions to or from apparatus that is part of the system.

(4) In this section "relevant time", in relation to a communication transmitted by means of a telecommunication system, means—

(a) any time while the communication is being transmitted, and

(b) any time when the communication is stored in or by the system (whether before or after its transmission).

(5) For the purposes of this section, the cases in which any of the content of a communication is to be taken to be made available to a person at a relevant time include any case in which any of the content of the communication is diverted or recorded at a relevant time so as to be available to a person after that time.

(6) In this section—

"wireless telegraphy" and "wireless telegraphy apparatus" have the same meaning as in the Wireless Telegraphy Act 2006 (see sections 116 and 117 of that Act), and

"interfere", in relation to wireless telegraphy, has the same meaning as in that Act (see section 115(3) of that Act).

Interception in relation to postal services

(7) Section 125(3) of the Postal Services Act 2000 applies for the purposes of determining for the purposes of this Act whether a postal item is in the course of its transmission by means of a postal service as it applies for the purposes of determining for the purposes of that Act whether a postal packet is in course of transmission by post.

Interception carried out in the United Kingdom

(8) For the purposes of this Act the interception of a communication is carried out in the United Kingdom if, and only if—

(a) the relevant act or, in the case of a postal item, the interception is carried out by conduct within the United Kingdom, and

(b) the communication is intercepted—

(i) in the course of its transmission by means of a public postal service or public telecommunication system, or

(ii) in the course of its transmission by means of a private telecommunication system in a case where the sender or intended recipient of the communication is in the United Kingdom.

4 Conduct that is not interception

(1) References in this Act to the interception of a communication do not include references to the interception of any communication broadcast for general reception.

(2) References in this Act to the interception of a communication in the course of its transmission by means of a postal service do not include references to—

(a) any conduct that takes place in relation only to so much of the communication as consists in any postal data comprised in, included as part of, attached to, or logically associated with a communication (whether by the sender or otherwise) for the purposes of any postal service by means of which it is being or may be transmitted, or

(b) any conduct, in connection with conduct falling within paragraph (a), that gives a person who is neither the sender nor the intended recipient only so much access to a communication as is necessary for the purpose of identifying such postal data.

For the meaning of "postal data", see section 194.

5 Definition of "lawful authority"

(1) For the purposes of this Act, a person has lawful authority to carry out an interception if, and only if—

(a) the interception is carried out in accordance with any of the following—

(i) a targeted interception warrant or mutual assistance warrant under Chapter 1 of Part 2,

(ii) a targeted equipment interference warrant under Part 5,

(iii) a bulk interception warrant under Chapter 1 of Part 6, or

(iv) a bulk equipment interference warrant under Chapter 3 of Part 6,

(b) the interception is authorised by any of sections 32 to 39, or

(c) in the case of a communication stored in or by a telecommunication system, the interception—

(i) is in the exercise of any statutory power that is exercised for the purpose of obtaining information or taking possession of any document or other property, or

(ii) is carried out in accordance with a court order made for that purpose.

(2) Conduct which has lawful authority for the purposes of this Act by virtue of subsection (1)(a) or (b) is to be treated as lawful for all other purposes.

(3) Any other conduct which—

(a) is carried out in accordance with a warrant under Chapter 1 of Part 2 or a bulk interception warrant, or

(b) is authorised by any of sections 32 to 39,

is to be treated as lawful for all purposes.

6 Monetary penalties for certain unlawful interceptions

(1) The Investigatory Powers Commissioner may serve a monetary penalty notice on a person if conditions A and B are met.

(2) A monetary penalty notice is a notice requiring the person on whom it is served to pay to the Investigatory Powers Commissioner ("the Commissioner") a monetary penalty of an amount determined by the Commissioner and specified in the notice.

(3) Condition A is that the Commissioner considers that—

(a) the person has intercepted, in the United Kingdom, any communication in the course of its transmission by means of a public telecommunication system,

(b) the person did not have lawful authority to carry out the interception, and

(c) the person was not, at the time of the interception, making an attempt to act in accordance with an interception warrant which might, in the opinion of the Commissioner, explain the interception.

(4) Condition B is that the Commissioner does not consider that the person has committed an offence under section 2.

(5) The amount of a monetary penalty determined by the Commissioner under this section must not exceed £50,000.

(6) Schedule 1 (which makes further provision about monetary penalty notices) has effect.

(7) In this section "interception warrant" means—

(a) a targeted interception warrant or mutual assistance warrant under Chapter 1 of Part 2, or

(b) a bulk interception warrant under Chapter 1 of Part 6.

(8) For the meaning of "interception" and other key expressions used in this section, see sections 3 to 5.

7 Restriction on requesting overseas interception

(1) This section applies to—
(a) a request for assistance under an EU mutual assistance instrument, and
(b) a request for assistance in accordance with an international mutual assistance agreement.

(2) The Secretary of State must ensure that no request to which this section applies is made on behalf of a person in the United Kingdom to the competent authorities of a country or territory outside the United Kingdom unless a mutual assistance warrant has been issued under Chapter 1 of Part 2 authorising the making of the request.

(3) In this section—
"EU mutual assistance instrument" means an EU instrument which—
(a) relates to the provision of mutual assistance in connection with, or in the form of, the interception of communications,
(b) requires the issue of a warrant, order or equivalent instrument in cases in which assistance is given, and
(c) is designated as an EU mutual assistance instrument by regulations made by the Secretary of State;
"international mutual assistance agreement" means an international agreement which—
(a) relates to the provision of mutual assistance in connection with, or in the form of, the interception of communications,
(b) requires the issue of a warrant, order or equivalent instrument in cases in which assistance is given, and
(c) is designated as an international mutual assistance agreement by regulations made by the Secretary of State.

Prohibition against unlawful obtaining of communications data

8 Offence of unlawfully obtaining communications data

(1) A relevant person who knowingly or recklessly obtains communications data from a telecommunications operator or postal operator without lawful authority is guilty of an offence.

(2) "Relevant person" means a person who holds an office, rank or position with a relevant public authority (within the meaning of Part 3).

(3) A person guilty of an offence under this section is liable—
(a) on summary conviction in England and Wales—
(i) to imprisonment for a term not exceeding 12 months (or 6 months, if the offence was committed before the commencement of section 154(1) of the Criminal Justice Act 2003), or
(ii) to a fine,
or both;
(b) on summary conviction in Scotland—
(i) to imprisonment for a term not exceeding 12 months, or
(ii) to a fine not exceeding the statutory maximum,
or both;

(c) on summary conviction in Northern Ireland—

(i) to imprisonment for a term not exceeding 6 months, or

(ii) to a fine not exceeding the statutory maximum,

or both;

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or both.

Abolition of powers to obtain communications data

9 Abolition of certain powers to obtain data

(1) Schedule 2 (which repeals certain general information powers so far as they enable public authorities to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator) has effect.

(2) Any general information power which—

(a) would (apart from this subsection) enable a public authority to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator, and

(b) does not involve a court order or other judicial authorisation or warrant and is not a regulatory power,

is to be read as not enabling the public authority to secure such a disclosure.

(3) A regulatory power which enables a public authority to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator may only be exercised by the public authority if it is not possible for the authority to use a power under this Act to secure the disclosure of the data.

(4) The Secretary of State may by regulations modify any enactment in consequence of subsection (2).

(5) In this section "general information power" means—

(a) in relation to disclosure by a telecommunications operator, any power to obtain information or documents (however expressed) which—

(i) is conferred by or under an enactment other than this Act or the Regulation of Investigatory Powers Act 2000, and

(ii) does not deal (whether alone or with other matters) specifically with telecommunications operators or any class of telecommunications operators, and

(b) in relation to disclosure by a postal operator, any power to obtain information or documents (however expressed) which—

(i) is conferred by or under an enactment other than this Act or the Regulation of Investigatory Powers Act 2000, and

(ii) does not deal (whether alone or with other matters) specifically with postal operators or any class of postal operators.

(6) In this section—

"power" includes part of a power;

"regulatory power" means any general information power to obtain information or documents for the purpose of exercising regulatory functions in relation to telecommunications services or postal services,

and references to powers include duties (and references to enabling are accordingly to be read as including references to requiring).

Restrictions on interference with equipment

10 Mandatory use of targeted equipment interference warrants

(1) A relevant service may not, for the purpose of facilitating the obtaining of communications, private information or equipment data, engage in conduct that could be authorised by a targeted equipment interference warrant or a bulk equipment interference warrant except under the authority of such a warrant if—

(a) the service considers that the conduct would (unless done under lawful authority) constitute one or more offences under sections 1 to 3A of the Computer Misuse Act 1990 (computer misuse offences), and

(b) there is a British Islands connection.

(2) For the purpose of this section, there is a British Islands connection if—

(a) any of the conduct would take place in the British Islands (regardless of the location of the equipment that would, or may, be interfered with),

(b) the service believes that any of the equipment that would, or may, be interfered with would, or may, be in the British Islands at some time while the interference is taking place, or

(c) a purpose of the interference is to facilitate the obtaining of—

(i) communications sent by, or to, a person who is, or whom the intelligence service believes to be, for the time being in the British Islands, or

(ii) private information relating to an individual who is, or whom the intelligence service believes to be, for the time being in the British Islands.

(3) This section does not restrict the ability of a relevant service to apply for a targeted equipment interference warrant or a bulk equipment interference warrant in cases where—

(a) the service does not consider that the conduct for which it is seeking authorisation would (unless done under lawful authority) constitute one or more offences under sections 1 to 3A of the Computer Misuse Act 1990, or

(b) there is no British Islands connection.

(4) In this section, "relevant service" means—

(a) the Security Service;

(b) the Secret Intelligence Service;

(c) GCHQ;

(d) the Ministry of Defence.

11 Restriction on use of section 93 of the Police Act 1997

A person may not, for the purpose of facilitating the obtaining of communications, information or equipment data, make an application under section 93 of the Police Act 1997 for authorisation to engage in conduct that could be authorised by a targeted equipment interference warrant if the applicant considers that the conduct would (unless done under lawful

authority) constitute one or more offences under sections 1 to 3A of the Computer Misuse Act 1990 (computer misuse offences).

PART 2

LAWFUL INTERCEPTION OF COMMUNICATIONS

CHAPTER 1

INTERCEPTION AND EXAMINATION WITH A WARRANT

Warrants under this Chapter

12 Warrants that may be issued under this Chapter

(1) There are three kinds of warrant that may be issued under this Chapter—
- (a) targeted interception warrants (see subsection (2)),
- (b) targeted examination warrants (see subsection (3)), and
- (c) mutual assistance warrants (see subsection (4)).

(2) A targeted interception warrant is a warrant which authorises or requires the person to whom it is addressed to secure, by any conduct described in the warrant, any one or more of the following—
- (a) the interception, in the course of their transmission by means of a postal service or telecommunication system, of the communications described in the warrant;
- (b) the obtaining of related communications data from communications described in the warrant (see subsection (6));
- (c) the disclosure, in any manner described in the warrant, of intercepted material or related communications data obtained under the warrant to the person to whom the warrant is addressed or to any person acting on that person's behalf.

(3) A targeted examination warrant is a warrant which authorises the person to whom it is addressed to carry out the examination of intercepted material obtained under a bulk interception warrant.

For provision about bulk interception warrants, see Chapter 1 of Part 6.

(4) A mutual assistance warrant is a warrant which authorises or requires the person to whom it is addressed to secure, by any conduct described in the warrant, any one or more of the following—
- (a) the making of a request, in accordance with an EU mutual assistance instrument or an international mutual assistance agreement, for the provision of any assistance of a kind described in the warrant in connection with, or in the form of, an interception of communications;
- (b) the provision to the competent authorities of a country or territory outside the United Kingdom, in accordance with such an instrument or agreement, of any assistance of a kind described in the warrant in connection with, or in the form of, an interception of communications;
- (c) the disclosure, in any manner described in the warrant, of any intercepted material or related communications data obtained under the warrant to the person to whom the warrant is addressed or to any person acting on that person's behalf.

(5) A targeted interception warrant or mutual assistance warrant also authorises the following conduct (in addition to the conduct described in the warrant)—

(a) any conduct which it is necessary to undertake in order to do what is expressly authorised or required by the warrant, including—

(i) the interception of communications not described in the warrant, and

(ii) conduct for obtaining related communications data from such communications;

(b) any conduct by any person which is conduct in pursuance of a requirement imposed by or on behalf of the person to whom the warrant is addressed to be provided with assistance in giving effect to the warrant.

(6) In this Part "related communications data" means—

(a) in relation to a communication intercepted in the course of its transmission by means of a postal service, data falling within subsection (7);

(b) in relation to a communication intercepted in the course of its transmission by means of a telecommunication system, data falling within subsection (7) or (8).

(7) The data falling within this subsection is so much of any data as is obtained by, or in connection with, the interception and—

(a) is communications data relating to the communication or to the sender or recipient, or intended recipient, of the communication, or

(b) is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise) and enables or otherwise facilitates the functioning of—

(i) a postal service,

(ii) a telecommunication system (including any apparatus forming part of the system), or

(iii) any telecommunications service provided by means of a telecommunication system.

For the meaning of "communications data", see sections 193 and 194.

(8) The data falling within this subsection is so much of the content of the communication (see section 193(6)) as—

(a) is capable of being logically separated from the remainder of the content of the communication, and

(b) if it were so separated—

(i) would not reveal anything of what might reasonably be expected to be the meaning of the communication, disregarding any meaning arising from the fact of the communication or from any data relating to the transmission of the communication, and

(ii) would be data falling within subsection (9).

(9) The data falling within this subsection is—

(a) data which may be used to identify, or assist in identifying, any person, apparatus, telecommunication system or telecommunications service, and

(b) data which describes an event or the location of any person, event or thing.

(10) For provision enabling the combination of targeted interception warrants with certain other warrants or authorisations (including targeted examination warrants), see Schedule 7.

13 Subject-matter of warrants

(1) A warrant under this Chapter may relate to—
  (a) a particular person or organisation, or
  (b) a single set of premises.

(2) In addition, a targeted interception warrant may relate to—
  (a) a group of persons who share a common purpose or who carry on, or may carry on, a particular activity;
  (b) more than one person or organisation, or more than one set of premises, where the conduct authorised or required by the warrant is for the purposes of the same investigation or operation;
  (c) the testing, maintenance or development of apparatus, systems or other capabilities relating to the interception of communications in the course of their transmission by means of a telecommunication system or to the obtaining of related communications data;
  (d) the training of persons who carry out, or are likely to carry out, such interception or the obtaining of such data.

Power to issue warrants

14 Power of Secretary of State to issue warrants

(1) The Secretary of State may, on an application made by or on behalf of an intercepting authority (see section 15), issue a targeted interception warrant or a mutual assistance warrant if—
  (a) the Secretary of State considers that the warrant is necessary on grounds falling within subsection (3),
  (b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,
  (c) the Secretary of State considers that satisfactory arrangements made for the purposes of section 40 (general safeguards) are in force in relation to the warrant, and
  (d) except where the Secretary of State considers that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner.

  This is subject to subsection (7).

(2) The Secretary of State may, on an application made by or on behalf of the head of an intelligence service, issue a targeted examination warrant if—
  (a) the Secretary of State considers that the warrant is necessary on grounds falling within subsection (3)(a) to (c),
  (b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,
  (c) the Secretary of State considers that the warrant is or may be necessary to authorise the selection of intercepted material for examination in

breach of the prohibition in section 119(4) (prohibition on seeking to identify communications of individuals in the British Islands), and

(d) the decision to issue the warrant has been approved by a Judicial Commissioner.

This is subject to subsection (7).

(3) A warrant is necessary on grounds falling within this subsection if it is necessary—

(a) in the interests of national security,

(b) for the purpose of preventing or detecting serious crime,

(c) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security (but see subsection (4)), or

(d) for the purpose of giving effect to the provisions of an EU mutual assistance instrument or an international mutual assistance agreement, in a case where—

(i) the application is for the issue of a mutual assistance warrant, and

(ii) the circumstances appear to the Secretary of State to be equivalent to those in which the Secretary of State would issue a warrant by virtue of paragraph (b).

(4) A warrant may be considered necessary on the ground falling within subsection (3)(c) only if the information which it is considered necessary to obtain is information relating to the acts or intentions of persons outside the British Islands.

(5) A warrant may not be considered necessary on grounds falling within subsection (3) if it is considered necessary only for the purpose of gathering evidence for use in any legal proceedings.

(6) The matters to be taken into account in considering whether the conditions in paragraphs (a) and (b) of subsection (1) are met include whether the information which it is considered necessary to obtain under the warrant could reasonably be obtained by other means.

(7) The Secretary of State may not issue a warrant under this section if—

(a) the application is a relevant Scottish application (see section 18), and

(b) the Secretary of State considers that the warrant is necessary only on grounds falling within subsection (3)(b) or (d).

For the power of the Scottish Ministers to issue warrants under this Chapter, see section 17.

(8) But subsection (7) does not prevent the Secretary of State from doing anything under this section for the purposes specified in section 2(2) of the European Communities Act 1972.

15 Persons who may apply for issue of a warrant

(1) Each of the following is an "intercepting authority" for the purposes of this Part—

(a) a person who is the head of an intelligence service;

(b) the Director General of the National Crime Agency;

(c) the Commissioner of Police of the Metropolis;

(d) the Chief Constable of the Police Service of Northern Ireland;
(e) the chief constable of the Police Service of Scotland;
(f) the Commissioners for Her Majesty's Revenue and Customs;
(g) the Chief of Defence Intelligence;
(h) a person who is the competent authority of a country or territory outside the United Kingdom for the purposes of an EU mutual assistance instrument or an international mutual assistance agreement.

(2) For the meaning of "head of an intelligence service", see section 195.

(3) An application for the issue of a warrant under this Chapter may only be made on behalf of an intercepting authority by a person holding office under the Crown.

16 Additional protection for Members of Parliament etc.

(1) This section applies where—
(a) an application is made to the Secretary of State for the issue of a targeted interception warrant or a targeted examination warrant, and
(b) the purpose of the warrant is—
(i) in the case of a targeted interception warrant, to authorise or require the interception of communications sent by, or intended for, a person who is a member of a relevant legislature, or
(ii) in the case of a targeted examination warrant, to authorise the examination of the content of such communications.

(2) Before deciding whether to issue the warrant, the Secretary of State must consult the Prime Minister.

(3) In this section "member of a relevant legislature" means—
(a) a member of either House of Parliament;
(b) a member of the Scottish Parliament;
(c) a member of the National Assembly for Wales;
(d) a member of the Northern Ireland Assembly;
(e) a member of the European Parliament elected for the United Kingdom.

17 Power of Scottish Ministers to issue warrants

(1) The Scottish Ministers may, on an application made by or on behalf of an intercepting authority, issue a targeted interception warrant or a mutual assistance warrant if—
(a) the application is a relevant Scottish application (see section 18),
(b) the Scottish Ministers consider that the warrant is necessary on grounds falling within subsection (3),
(c) the Scottish Ministers consider that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,
(d) the Scottish Ministers consider that satisfactory arrangements made for the purposes of section 40 (general safeguards) are in force in relation to the warrant, and
(e) except where the Scottish Ministers consider that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner.

(2) The Scottish Ministers may, on an application made by or on behalf of the head of an intelligence service, issue a targeted examination warrant if—

(a) the application is a relevant Scottish application,

(b) the Scottish Ministers consider that the warrant is necessary for the purpose of preventing or detecting serious crime,

(c) the Scottish Ministers consider that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(d) the Scottish Ministers consider that the warrant is or may be necessary to authorise the selection of intercepted material for examination in breach of the prohibition in section 119(4) (prohibition on seeking to identify communications of individuals in the British Islands), and

(e) the decision to issue the warrant has been approved by a Judicial Commissioner.

(3) A warrant is necessary on grounds falling within this subsection if it is necessary—

(a) for the purpose of preventing or detecting serious crime, or

(b) for the purpose of giving effect to the provisions of an EU mutual assistance instrument or an international mutual assistance agreement, in a case where—

(i) the application is for the issue of a mutual assistance warrant, and

(ii) the circumstances appear to the Scottish Ministers to be equivalent to those in which the Scottish Ministers would issue a warrant by virtue of paragraph (a).

(4) A warrant may not be considered necessary on grounds falling within subsection (3) if it is considered necessary only for the purpose of gathering evidence for use in any legal proceedings.

(5) The matters to be taken into account in considering whether the conditions in paragraphs (b) and (c) of subsection (1) are met include whether the information which it is considered necessary to obtain under the warrant could reasonably be obtained by other means.

18 "Relevant Scottish applications"

(1) An application for the issue of a warrant under this Chapter is a "relevant Scottish application" for the purposes of this Chapter if any of conditions A to C is met.

In this section "the applicant" means the person by whom, or on whose behalf, the application is made.

(2) Condition A is that—

(a) the application is for the issue of a targeted interception warrant or a targeted examination warrant, and

(b) the warrant, if issued, would relate to—

(i) a person who is in Scotland, or is reasonably believed by the applicant to be in Scotland, at the time of the issue of the warrant, or

(ii) premises which are in Scotland, or are reasonably believed by the applicant to be in Scotland, at that time.

(3) Condition B is that—

(a) the application is for the issue of a mutual assistance warrant which, if issued, would authorise or require—

(i) the making of a request falling within paragraph (a) of section 12(4), or

(ii) the making of such a request and disclosure falling within section 12(4)(c), and

(b) the application—

(i) is made by, or on behalf of, the chief constable of the Police Service of Scotland, or

(ii) is made by, or on behalf of, the Commissioners for Her Majesty's Revenue and Customs or the Director General of the National Crime Agency for the purpose of preventing or detecting serious crime in Scotland.

(4) Condition C is that—

(a) the application is for the issue of a mutual assistance warrant which, if issued, would authorise or require—

(i) the provision of assistance falling within paragraph (b) of section 12(4), or

(ii) the provision of such assistance and disclosure falling within section 12(4)(c), and

(b) the warrant, if issued, would relate to—

(i) a person who is in Scotland, or is reasonably believed by the applicant to be in Scotland, at the time of the issue of the warrant, or

(ii) premises which are in Scotland, or are reasonably believed by the applicant to be in Scotland, at that time.

Approval of warrants by Judicial Commissioners

19 Approval of warrants by Judicial Commissioners

(1) In deciding whether to approve a person's decision to issue a warrant under this Chapter, a Judicial Commissioner must review the person's conclusions as to the following matters—

(a) whether the warrant is necessary on relevant grounds (see subsection (3)), and

(b) whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

(2) In doing so, the Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review.

(3) In subsection (1)(a) "relevant grounds" means—

(a) in the case of a warrant to be issued by the Secretary of State, grounds falling within section 14(3);

(b) in the case of a warrant to be issued by the Scottish Ministers, grounds falling within section 17(3).

(4) Where a Judicial Commissioner refuses to approve a decision to issue a warrant under this Chapter, the Judicial Commissioner must give the person who made that decision written reasons for the refusal.

(5) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to issue a warrant under this Chapter, the person who made that decision may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant.

20 Approval of warrants issued in urgent cases

(1) This section applies where—
  (a) a targeted interception warrant or mutual assistance warrant is issued without the approval of a Judicial Commissioner, and
  (b) the person who issued the warrant considered that there was an urgent need to issue it.

(2) The person who issued the warrant must inform a Judicial Commissioner that it has been issued.

(3) The Judicial Commissioner must, before the end of the relevant period—
  (a) decide whether to approve the decision to issue the warrant, and
  (b) notify the person of the Judicial Commissioner's decision.

"The relevant period" means the period ending with the fifth working day after the day on which the warrant was issued.

(4) But subsection (3) does not apply if the Judicial Commissioner is notified that the warrant is to be renewed under section 25 before the end of the relevant period.

(5) If a Judicial Commissioner refuses to approve the decision to issue a warrant, the warrant ceases to have effect.

(6) Section 21 contains further provision about what happens when a warrant ceases to have effect as a result of this section.

21 Warrants ceasing to have effect under section 20

(1) This section applies where a warrant ceases to have effect as a result of section 20.

(2) The person to whom the warrant is addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible.

(3) The Judicial Commissioner who refused to approve the warrant may—
  (a) direct that any of the intercepted material or related communications data obtained under the warrant is destroyed;
  (b) impose conditions as to the use or retention of any of that material or data.

(4) The Judicial Commissioner—
  (a) may require an affected party to make representations about how the Judicial Commissioner should exercise any function under subsection (3), and
  (b) must have regard to any such representations made by an affected party (whether or not as a result of a requirement imposed under paragraph (a)).

(5) Each of the following is an "affected party" for the purposes of subsection (4)—

(a) the person who decided to issue the warrant;
(b) the person to whom the warrant is addressed.

(6) The person who decided to issue the warrant may ask the Investigatory Powers Commissioner to review a decision made by any other Judicial Commissioner under subsection (3).

(7) On a review under subsection (6), the Investigatory Powers Commissioner may—
(a) confirm the Judicial Commissioner's decision, or
(b) make a fresh determination.

(8) Nothing in this section or section 20 affects the lawfulness of—
(a) anything done under the warrant before it ceases to have effect;
(b) if anything is in the process of being done under the warrant when it ceases to have effect—
(i) anything done before that thing could be stopped, or
(ii) anything done which it is not reasonably practicable to stop.

Further provision about warrants

22 Decisions to issue warrants to be taken personally by Ministers

(1) The decision to issue a warrant under this Chapter must be taken personally by—
(a) the Secretary of State, or
(b) in the case of a warrant to be issued by the Scottish Ministers, a member of the Scottish Government.

(2) Before a warrant under this Chapter is issued, it must be signed by the person who has taken the decision to issue it.

(3) Subsections (1) and (2) are subject to—
(a) subsection (4) (urgent cases), and
(b) section 28 (special rules for certain mutual assistance warrants).

(4) In an urgent case, the warrant may be signed by a senior official designated by the Secretary of State or (as the case may be) the Scottish Ministers for that purpose.

(5) In such a case, the warrant must contain a statement that the case is an urgent case in which the Secretary of State or (as the case may be) the Scottish Ministers have personally expressly authorised the issue of the warrant.

(6) In this section "senior official" means—
(a) in the case of a warrant to be issued by the Secretary of State, a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service;
(b) in the case of a warrant to be issued by the Scottish Ministers, a member of the staff of the Scottish Administration who is a member of the Senior Civil Service.

23 Requirements that must be met by warrants

(1) A warrant under this Chapter must contain a provision stating whether it is a targeted interception warrant, a targeted examination warrant or a mutual assistance warrant.

(2) A warrant issued under this Chapter must be addressed to the person by whom, or on whose behalf, the application for the warrant was made.

(3) A warrant that relates to a particular person or organisation, or to a single set of premises, must name or describe that person or organisation or those premises.

(4) A warrant that relates to a group of persons who share a common purpose or who carry on (or may carry on) a particular activity must—
  (a) describe that purpose or activity, and
  (b) name or describe as many of those persons as it is reasonably practicable to name or describe.

(5) A warrant that relates to more than one person or organisation, or more than one set of premises, where the conduct authorised or required by the warrant is for the purposes of the same investigation or operation, must—
  (a) describe the investigation or operation, and
  (b) name or describe as many of those persons or organisations, or as many of those sets of premises, as it is reasonably practicable to name or describe.

(6) A warrant that relates to any testing or training activities must—
  (a) describe those activities, and
  (b) name or describe as many of the persons whose communications will or may be intercepted as it is reasonably practicable to name or describe.

(7) In subsection (6) "testing or training activities" means—
  (a) the testing, maintenance or development of apparatus, systems or other capabilities relating to the interception of communications in the course of their transmission by means of a telecommunication system or to the obtaining of related communications data, or
  (b) the training of persons who carry out, or are likely to carry out, such interception or the obtaining of such data.

(8) Where a warrant under this Chapter authorises or requires the interception of communications, the warrant must describe those communications by specifying the addresses, numbers, apparatus, or other factors, or combination of factors, that are to be used for identifying the communications.

(9) Any factor, or combination of factors, specified in accordance with subsection (8) must be one that identifies communications which are likely to be or to include—
  (a) communications from, or intended for, any person named or described in the warrant, or
  (b) communications originating on, or intended for transmission to, any premises named or described in the warrant.

24 Duration of warrants

(1) A warrant under this Chapter, if it is not renewed before the end of the relevant period (see subsection (2)), ceases to have effect at the end of that period.

(2) In this section "the relevant period"—

(a) in the case of an urgent warrant (see subsection (3)), means the period ending with the fifth working day after the day on which the warrant was issued;

(b) in any other case, means the period of 6 months beginning with—

(i) the day on which the warrant was issued, or

(ii) in the case of a warrant that has been renewed, the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed.

(3) For the purposes of subsection (2)(a) an "urgent warrant" is a warrant which—

(a) was issued in an urgent case as mentioned in section 22(4), and

(b) has not been renewed.

(4) For provision about the renewal of warrants, see section 25.

25 Renewal of warrants

(1) If the renewal conditions are met, a warrant issued under this Chapter may be renewed, at any time before the end of the relevant period, by an instrument issued by the appropriate person.

(2) The renewal conditions are—

(a) that the appropriate person considers that the warrant continues to be necessary on any relevant grounds,

(b) that the appropriate person considers that the conduct that would be authorised by the renewed warrant continues to be proportionate to what is sought to be achieved by that conduct,

(c) that, in the case of a targeted examination warrant, the appropriate person considers that the warrant continues to be necessary to authorise the selection of intercepted material for examination in breach of the prohibition in section 119(4), and

(d) that the decision to renew the warrant has been approved by a Judicial Commissioner.

(3) The appropriate person is—

(a) in the case of a warrant issued by the Secretary of State, the Secretary of State;

(b) in the case of a warrant issued by the Scottish Ministers, a member of the Scottish Government.

(4) "Relevant grounds" means—

(a) in the case of a warrant issued by the Secretary of State, grounds falling within section 14(3);

(b) in the case of a warrant issued by the Scottish Ministers, grounds falling within section 17(3).

(5) The decision to renew a warrant must be taken personally by the appropriate person, and the instrument renewing the warrant must be signed by that person.

(6) Section 16 (additional protection for Members of Parliament etc.) applies in relation to a decision to renew a warrant as it applies in relation to a decision to issue a warrant.

(7) Section 19 (approval of warrants by Judicial Commissioners) applies in relation to a decision to renew a warrant as it applies in relation to a decision to issue a warrant (and accordingly any reference in that section to the person who decided to issue the warrant is to be read as a reference to the person who decided to renew it).

(8) In this section "the relevant period" has the same meaning as in section 24.

(9) This section is subject to section 28 (special rules for certain mutual assistance warrants).

26 Modification of warrants

(1) The provisions of a warrant issued under this Chapter may be modified at any time by an instrument issued by the person making the modification.

(2) The only modifications that may be made under this section are—
- (a) adding or removing the name or description of a person, organisation or set of premises to which the warrant relates,
- (b) varying such a name or description, and
- (c) adding, varying or removing any factor specified in the warrant in accordance with section 23(8).

(3) The decision to modify the provisions of a warrant must be taken personally by the person making the modification, and the instrument making the modification must be signed by that person.

(4) In this section—
- (a) a modification within paragraph (a) of subsection (2) is referred to as a "major modification", and
- (b) a modification within paragraph (b) or (c) of that subsection is referred to as a "minor modification".

(5) A major modification may be made by—
- (a) the Secretary of State,
- (b) a member of the Scottish Government, or
- (c) a senior official acting on behalf of the Secretary of State or (as the case may be) the Scottish Ministers.

(6) A minor modification may be made by—
- (a) the Secretary of State,
- (b) a member of the Scottish Government,
- (c) a senior official acting on behalf of the Secretary of State or (as the case may be) the Scottish Ministers,
- (d) the person to whom the warrant is addressed, or
- (e) a person who holds a senior position in the same public authority as the person mentioned in paragraph (d).

(7) For the purposes of subsection (6)(e) a person holds a senior position in a public authority if—

(a) in the case of any of the intelligence services, the person is a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service;

(b) in the case of the National Crime Agency, the person is a National Crime Agency officer of the grade of Deputy Director or above;

(c) in the case of the metropolitan police force, the Police Service of Northern Ireland or the Police Service of Scotland, a person is of or above the rank of Commander or Assistant Chief Constable;

(d) in the case of Her Majesty's Revenue and Customs, the person is a member of the Senior Civil Service;

(e) in the case of the Ministry of Defence—

(i) the person is a member of the Senior Civil Service, or

(ii) the person is of or above the rank of brigadier, commodore or air commodore.

(8) A person may make a major modification of a warrant by adding a name or description as mentioned in subsection (2)(a) only if the person considers—

(a) that the modification is necessary on any relevant grounds (see subsection (9)), and

(b) that the conduct authorised by the modification is proportionate to what is sought to be achieved by that conduct.

(9) In subsection (8)(a) "relevant grounds" means—

(a) in the case of a warrant issued by the Secretary of State, grounds falling within section 14(3);

(b) in the case of a warrant issued by the Scottish Ministers, grounds falling within section 17(3).

(10) Section 16 (additional protection for Members of Parliament etc.) applies in relation to a decision to make a major modification of a warrant by adding a name or description as mentioned in subsection (2)(a) as it applies in relation to a decision to issue a warrant; and accordingly where that section applies only the Secretary of State may make the modification.

(11) Where a major modification of a warrant is made by a senior official, the Secretary of State or (in the case of a warrant issued by the Scottish Ministers) a member of the Scottish Government must be notified personally of the modification and the reasons for making it.

(12) In this section "senior official" means—

(a) in the case of a warrant issued by the Secretary of State, a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service;

(b) in the case of a warrant issued by the Scottish Ministers, a member of the staff of the Scottish Administration who is a member of the Senior Civil Service.

(13) Nothing in this section applies in relation to modifying the provisions of a warrant in a way which does not affect the conduct authorised or required by it.

27 Cancellation of warrants

(1) Any of the appropriate persons may cancel a warrant issued under this Chapter at any time.

(2) If any of the appropriate persons considers that—
  (a) a warrant issued under this Chapter is no longer necessary on any relevant grounds, or
  (b) that the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved by that conduct,

the person must cancel the warrant.

(3) In subsection (2)(a) "relevant grounds" means—
  (a) in the case of a warrant issued by the Secretary of State, grounds falling within section 14(3);
  (b) in the case of a warrant issued by the Scottish Ministers, grounds falling within section 17(3).

(4) For the purpose of this section "the appropriate persons" are—
  (a) in the case of a warrant issued by the Secretary of State, the Secretary of State or a senior official acting on behalf of the Secretary of State;
  (b) in the case of a warrant issued by the Scottish Ministers, a member of the Scottish Government or a senior official acting on behalf of the Scottish Ministers.

(5) In this section "senior official" means—
  (a) in the case of a warrant issued by the Secretary of State, a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service;
  (b) in the case of a warrant issued by the Scottish Ministers, a member of the staff of the Scottish Administration who is a member of the Senior Civil Service.

(6) See also section 28 (which imposes a duty to cancel mutual assistance warrants in certain circumstances).

28 Special rules for certain mutual assistance warrants

(1) For the purposes of this section a warrant is a "relevant mutual assistance warrant" if—
  (a) the warrant is for the purposes of a request for assistance made under an EU mutual assistance instrument or an international mutual assistance agreement by the competent authorities of a country or territory outside the United Kingdom, and
  (b) either—
    (i) it appears that the interception subject is outside the United Kingdom, or
    (ii) the interception to which the warrant relates is to take place in relation only to premises outside the United Kingdom.

(2) The decision to issue a relevant mutual assistance warrant may be taken by a senior official designated by the Secretary of State for that purpose.

(3) In such a case, the warrant must contain—
  (a) a statement that the warrant is issued for the purposes of a request for assistance made under an EU mutual assistance instrument or an international mutual assistance agreement (as the case may be) by the competent authorities of a country or territory outside the United Kingdom, and

(b) whichever of the following statements is applicable—

(i) a statement that the interception subject appears to be outside the United Kingdom;

(ii) a statement that the interception to which the warrant relates is to take place in relation only to premises outside the United Kingdom.

(4) A relevant mutual assistance warrant may be renewed by a senior official designated by the Secretary of State for that purpose; and references in section 25 to the appropriate person include, in the case of such a warrant, references to that senior official.

(5) Where a senior official renews a relevant mutual assistance warrant in accordance with subsection (4), the instrument renewing the warrant must contain—

(a) a statement that the renewal is for the purposes of a request for assistance made under an EU mutual assistance instrument or an international mutual assistance agreement (as the case may be) by the competent authorities of a country or territory outside the United Kingdom, and

(b) whichever of the following statements is applicable—

(i) a statement that the interception subject appears to be outside the United Kingdom;

(ii) a statement that the interception to which the warrant relates is to take place in relation only to premises outside the United Kingdom.

(6) Subsection (7) applies in a case where—

(a) a relevant mutual assistance warrant—

(i) was issued containing the statement set out in subsection (3)(b)(i), or

(ii) has been renewed by an instrument containing the statement set out in subsection (5)(b)(i), and

(b) the last renewal (if any) of the warrant was a renewal by a senior official in accordance with subsection (4).

(7) If the Secretary of State, or a senior official acting on behalf of the Secretary of State, believes that the person, group or organisation named or described in the warrant as the interception subject is in the United Kingdom, that person must cancel the warrant.

(8) In this section—

"the interception subject", in relation to a warrant, means the person, group of persons or organisation about whose communications information is sought by the interception to which the warrant relates;

"senior official" means a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service.

Implementation of warrants

29 Implementation of warrants

(1) This section applies to targeted interception warrants and mutual assistance warrants.

(2) In giving effect to a warrant to which this section applies, the person to whom it is addressed ("the implementing authority") may (in addition to acting alone) act through, or together with, such other persons as the implementing authority may require (whether under subsection (3) or otherwise) to provide the authority with assistance in giving effect to the warrant.

(3) For the purpose of requiring any person to provide assistance in relation to a warrant to which this section applies, the implementing authority may—

(a) serve a copy of the warrant on any person who the implementing authority considers may be able to provide such assistance, or

(b) make arrangements for the service of a copy of the warrant on any such person.

(4) A copy of a warrant may be served under subsection (3) on a person outside the United Kingdom for the purpose of requiring the person to provide such assistance in the form of conduct outside the United Kingdom.

(5) For the purposes of this Act, the provision of assistance in giving effect to a warrant to which this section applies includes any disclosure to the implementing authority, or to persons acting on behalf of the implementing authority, of intercepted material or related communications data obtained under the warrant.

(6) References in this section and sections 30 and 31 to the service of a copy of a warrant include—

(a) the service of a copy of one or more schedules contained in the warrant with the omission of the remainder of the warrant, and

(b) the service of a copy of the warrant with the omission of any schedule contained in the warrant.

30 Service of warrants

(1) This section applies to the service of warrants under section 29(3).

(2) A copy of a warrant may be served on a person outside the United Kingdom in any of the following ways (as well as by electronic or other means of service)—

(a) by serving it at the person's principal office within the United Kingdom or, if the person has no such office in the United Kingdom, at any place in the United Kingdom where the person carries on business or conducts activities;

(b) if the person has specified an address in the United Kingdom as one at which the person, or someone on the person's behalf, will accept service of documents of the same description as a copy of a warrant, by serving it at that address;

(c) by making it available for inspection (whether to the person or to someone acting on the person's behalf) at a place in the United Kingdom (but this is subject to subsection (3)).

(3) A copy of a warrant may be served on a person outside the United Kingdom in the way mentioned in subsection (2)(c) only if—

(a) it is not reasonably practicable for a copy to be served by any other means (whether as mentioned in subsection (2)(a) or (b) or otherwise), and

(b) the implementing authority takes such steps as the authority considers appropriate for the purpose of bringing the contents of the warrant, and the availability of a copy for inspection, to the attention of the person.

(4) The steps mentioned in subsection (3)(b) must be taken as soon as reasonably practicable after the copy of the warrant is made available for inspection.

(5) In this section "the implementing authority" has the same meaning as in section 29.

31 Duty of operators to assist with implementation

(1) A relevant operator that has been served with a copy of a warrant to which section 29 applies by (or on behalf of) the implementing authority must take all steps for giving effect to the warrant that are notified to the relevant operator by (or on behalf of) the implementing authority.

This is subject to subsection (4).

(2) In this section "relevant operator" means—

(a) a public postal operator, or

(b) a telecommunications operator.

(3) Subsection (1) applies whether or not the relevant operator is in the United Kingdom.

(4) The relevant operator is not required to take any steps which it is not reasonably practicable for the relevant operator to take.

(5) In determining for the purposes of subsection (4) whether it is reasonably practicable for a relevant operator outside the United Kingdom to take any steps in a country or territory outside the United Kingdom for giving effect to a warrant, the matters to be taken into account include the following—

(a) any requirements or restrictions under the law of that country or territory that are relevant to the taking of those steps, and

(b) the extent to which it is reasonably practicable to give effect to the warrant in a way that does not breach any of those requirements or restrictions.

(6) Where obligations have been imposed on a relevant operator ("P") under section 189 (maintenance of technical capability), for the purposes of subsection (4) the steps which it is reasonably practicable for P to take include every step which it would have been reasonably practicable for P to take if P had complied with all of those obligations.

(7) A person who knowingly fails to comply with subsection (1) is guilty of an offence and liable—

(a) on summary conviction in England and Wales—

(i) to imprisonment for a term not exceeding 12 months (or 6 months, if the offence was committed before the commencement of section 154(1) of the Criminal Justice Act 2003), or

(ii) to a fine,

or both;

(b) on summary conviction in Scotland—

(i) to imprisonment for a term not exceeding 12 months, or

(ii) to a fine not exceeding the statutory maximum,

or both;

(c) on summary conviction in Northern Ireland—

(i) to imprisonment for a term not exceeding 6 months, or

(ii) to a fine not exceeding the statutory maximum,

or both;

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or both.

(8) The duty imposed by subsection (1) is enforceable (whether or not the person is in the United Kingdom) by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.

CHAPTER 2

OTHER FORMS OF LAWFUL INTERCEPTION

Interception with consent

32 Interception with the consent of the sender or recipient

(1) The interception of a communication is authorised by this section if the sender and the intended recipient of the communication have each consented to its interception.

(2) The interception of a communication is authorised by this section if—

(a) the communication is one sent by, or intended for, a person who has consented to the interception, and

(b) surveillance by means of that interception has been authorised under—

(i) Part 2 of the Regulation of Investigatory Powers Act 2000, or

(ii) the Regulation of Investigatory Powers (Scotland) Act 2000.

Interception for administrative or enforcement purposes

33 Interception by providers of postal or telecommunications services

(1) The interception of a communication is authorised by this section if the interception is carried out—

(a) by, or on behalf of, a person who provides a postal service or a telecommunications service, and

(b) for any of the purposes in subsection (2).

(2) The purposes referred to in subsection (1) are—

(a) purposes relating to the provision or operation of the service;

(b) purposes relating to the enforcement, in relation to the service, of any enactment relating to—

(i) the use of postal or telecommunications services, or
(ii) the content of communications transmitted by means of such services;

(c) purposes relating to the provision of services or facilities aimed at preventing or restricting the viewing or publication of the content of communications transmitted by means of postal or telecommunications services.

(3) A reference in this section to anything carried out for purposes relating to the provision or operation of a telecommunications service includes, among other things, a reference to anything done for the purposes of identifying, combating or preventing anything which could affect—

(a) the telecommunication system by means of which the service is provided, or
(b) any apparatus attached to that system.

34 Interception by businesses etc. for monitoring and record-keeping purposes

(1) Conduct is authorised by this section if it is authorised by regulations made under subsection (2).

(2) The Secretary of State may by regulations authorise conduct of a description specified in the regulations if that conduct appears to the Secretary of State to constitute a legitimate practice reasonably required for the purpose, in connection with the carrying on of any relevant activities (see subsection (4)), of monitoring or keeping a record of—

(a) communications by means of which transactions are entered into in the course of the relevant activities, or
(b) other communications relating to the relevant activities or taking place in the course of the carrying on of those activities.

(3) But nothing in any regulations under subsection (2) may authorise the interception of any communication except in the course of its transmission using apparatus or services provided by or to the person carrying on the relevant activities for use (whether wholly or partly) in connection with those activities.

(4) In this section "relevant activities" means—

(a) any business,
(b) any activities of a government department, the Welsh Government, a Northern Ireland department or any part of the Scottish Administration,
(c) any activities of a public authority, and
(d) any activities of any person or office holder on whom functions are conferred by or under any enactment.

35 Postal services: interception for enforcement purposes

(1) The interception of a communication in the course of its transmission by means of a public postal service is authorised by this section if it is carried out by an officer of Revenue and Customs under section 159 of the Customs and Excise Management Act 1979, as applied by virtue of—

(a) section 105 of the Postal Services Act 2000 (power to open postal items etc.), or

(b) that section and another enactment.

(2) The interception of a communication in the course of its transmission by means of a public postal service is authorised by this section if it is carried out under paragraph 9 of Schedule 7 to the Terrorism Act 2000 (port and border controls).

36 Interception by OFCOM in connection with wireless telegraphy

(1) Conduct falling within subsection (2) is authorised by this section if it is carried out by OFCOM for purposes connected with a relevant matter (see subsection (3)).

(2) The conduct referred to in subsection (1) is—
- (a) the interception of a communication in the course of its transmission;
- (b) the obtaining, by or in connection with the interception, of information about the sender or recipient of the communication;
- (c) the disclosure of anything obtained by conduct falling within paragraph (a) or (b).

(3) Each of the following is a relevant matter for the purposes of subsection (1)—
- (a) the grant of wireless telegraphy licences under the Wireless Telegraphy Act 2006 ("the 2006 Act");
- (b) the prevention or detection of anything which constitutes interference with wireless telegraphy;
- (c) the enforcement of—
  - (i) any provision of Part 2 (other than Chapter 2 and sections 27 to 31) or Part 3 of the 2006 Act, or
  - (ii) any enactment not falling within sub-paragraph (i) that relates to interference with wireless telegraphy.

(4) In this section "OFCOM" means the Office of Communications established by section 1 of the Office of Communications Act 2002.

Interception taking place in certain institutions

37 Interception in prisons

(1) Conduct taking place in a prison is authorised by this section if it is conduct in exercise of any power conferred by or under prison rules.

(2) In this section "prison rules" means any rules made under—
- (a) section 47 of the Prison Act 1952,
- (b) section 39 of the Prisons (Scotland) Act 1989, or
- (c) section 13 of the Prison Act (Northern Ireland) 1953.

(3) In this section "prison" means—
- (a) any prison, young offender institution, young offenders centre, secure training centre, secure college or remand centre which is under the general superintendence of, or is provided by, the Secretary of State under the Prison Act 1952 or the Prison Act (Northern Ireland) 1953, or
- (b) any prison, young offenders institution or remand centre which is under the general superintendence of the Scottish Ministers under the Prisons (Scotland) Act 1989,

and includes any contracted out prison, within the meaning of Part 4 of the Criminal Justice Act 1991 or section 106(4) of the Criminal Justice and Public Order Act 1994, and any legalised police cells within the meaning of section 14 of the Prisons (Scotland) Act 1989.

38 Interception in psychiatric hospitals

(1) Conduct is authorised by this section if—

(a) it takes place in any hospital premises where high security psychiatric services are provided, and

(b) it is conduct in pursuance of, and in accordance with, any relevant direction given to the body providing those services at those premises.

(2) "Relevant direction" means—

(a) a direction under section 4(3A)(a) of the National Health Service Act 2006, or

(b) a direction under section 19 or 23 of the National Health Service (Wales) Act 2006.

(3) Conduct is authorised by this section if—

(a) it takes place in a state hospital, and

(b) it is conduct in pursuance of, and in accordance with, any direction given to the State Hospitals Board for Scotland under section 2(5) of the National Health Service (Scotland) Act 1978 (regulations and directions as to the exercise of their functions by health boards).

The reference to section 2(5) of that Act is to that provision as applied by Article 5(1) of, and the Schedule to, the State Hospitals Board for Scotland Order 1995 (which applies certain provisions of that Act to the State Hospitals Board).

(4) In this section—

"high security psychiatric services" has the same meaning as in section 4 of the National Health Service Act 2006;

"hospital premises" has the same meaning as in section 4(3) of that Act;

"state hospital" has the same meaning as in the National Health Service (Scotland) Act 1978.

Interception in accordance with overseas requests

39 Interception in accordance with overseas requests

(1) The interception of a communication by a person in the course of its transmission by means of a telecommunication system is authorised by this section if conditions A to D are met.

(2) Condition A is that the person provides a telecommunications service which is—

(a) a public telecommunications service, or

(b) a telecommunications service that would be a public telecommunications service if the persons to whom it is offered or provided were members of the public in a part of the United Kingdom.

(3) Condition B is that the interception relates to the use of the telecommunications service.

(4) Condition C is that the interception is carried out in response to a request made in accordance with a relevant international agreement by the competent authorities of a country or territory outside the United Kingdom.
In this subsection "relevant international agreement" means an international agreement to which the United Kingdom is a party.

(5) Condition D is that any further conditions specified in regulations made by the Secretary of State for the purposes of this section are met.

CHAPTER 3

OTHER PROVISIONS ABOUT INTERCEPTION

Restrictions on use of intercepted material etc.

40 General safeguards

(1) The appropriate issuing authority must ensure, in relation to every targeted interception warrant or mutual assistance warrant issued by that authority, that arrangements are in force for securing that the requirements of subsections (2) and (5) are met in relation to the intercepted material and related communications data obtained under the warrant.
This is subject to subsection (8).

(2) The requirements of this subsection are met in relation to the intercepted material and related communications data obtained under a warrant if each of the following is limited to the minimum that is necessary for the authorised purposes (see subsection (3))—
(a) the number of persons to whom any of the material or data is disclosed or otherwise made available;
(b) the extent to which any of the material or data is disclosed or otherwise made available;
(c) the extent to which any of the material or data is copied;
(d) the number of copies that are made.

(3) For the purposes of this section something is necessary for the authorised purposes if, and only if—
(a) it is, or is likely to become, necessary on any of the grounds falling within section 14(3),
(b) it is necessary for facilitating the carrying out of any functions under this Act of the Secretary of State, the Scottish Ministers or the person to whom the warrant is addressed,
(c) it is necessary for facilitating the carrying out of any functions of the Judicial Commissioners or the Investigatory Powers Tribunal under or in relation to this Act,
(d) it is necessary to ensure that a person ("P") who is conducting a criminal prosecution has the information P needs to determine what is required of P by P's duty to secure the fairness of the prosecution, or
(e) it is necessary for the performance of any duty imposed on any person by the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923.

(4) The arrangements for the time being in force under this section for securing that the requirements of subsection (2) are met in relation to the intercepted material and related communications data obtained under the warrant must include arrangements for securing that every copy made of any of that material or data is stored, for so long as it is retained, in a secure manner.

(5) The requirements of this subsection are met in relation to the intercepted material and related communications data obtained under a warrant if every copy made of any of that material or data (if not destroyed earlier) is destroyed as soon as there are no longer any relevant grounds for retaining it (see subsection (6)).

(6) For the purposes of subsection (5), there are no longer any relevant grounds for retaining a copy of any material or data if, and only if—

(a) its retention is not necessary, or not likely to become necessary, on any of the grounds falling within section 14(3), and

(b) its retention is not necessary for any of the purposes mentioned in paragraphs (b) to (e) of subsection (3) above.

(7) Subsection (8) applies if—

(a) any intercepted material or related communications data obtained under the warrant has been handed over to any overseas authorities, or

(b) a copy of any such material or data has been given to any overseas authorities.

(8) To the extent that the requirements of subsections (2) and (5) relate to any of the material or data mentioned in subsection (7)(a), or to the copy mentioned in subsection (7)(b), the arrangements made for the purposes of this section are not required to secure that those requirements are met (see instead section 41).

(9) In this section—

"appropriate issuing authority" means—

(a) the Secretary of State, in the case of a warrant issued by the Secretary of State;

(b) the Scottish Ministers, in the case of a warrant issued by the Scottish Ministers;

"copy", in relation to intercepted material or related communications data obtained under a warrant, means any of the following (whether or not in documentary form)—

(a) any copy, extract or summary of the material or data which identifies itself as having been obtained under the warrant, and

(b) any record referring to an interception which is a record of the identities of the persons to or by whom the material was sent, or to whom the data relates,

and "copied" is to be read accordingly;

"overseas authorities" means authorities of a country or territory outside the United Kingdom.

41 Safeguards relating to disclosure of material or data overseas

(1) The appropriate issuing authority must ensure, in relation to every targeted interception warrant or mutual assistance warrant issued by that authority, that arrangements are in force for securing that—

(a) any of the intercepted material or related communications data obtained under the warrant is handed over to overseas authorities only if the requirements of subsection (2) are met, and

(b) copies of any of that material or data are given to overseas authorities only if those requirements are met.

(2) The requirements of this subsection are met in the case of a warrant if it appears to the appropriate issuing authority—

(a) that requirements corresponding to the requirements of section 40(2) and (5) ("the relevant requirements") will apply, to such extent (if any) as the appropriate issuing authority considers appropriate, in relation to any of the intercepted material or related communications data which is handed over, or any copy of which is given, to the authorities in question, and

(b) that restrictions are in force which would prevent, to such extent (if any) as the appropriate issuing authority considers appropriate, the doing of anything in, for the purposes of or in connection with any proceedings outside the United Kingdom which would result in an unauthorised disclosure.

(3) In subsection (2)(b) "unauthorised disclosure" means a disclosure which, by virtue of section 42, could not be made in the United Kingdom.

(4) In this section—

"appropriate issuing authority" means—

(a) the Secretary of State, in the case of a warrant issued by the Secretary of State;

(b) the Scottish Ministers, in the case of a warrant issued by the Scottish Ministers;

"copy" has the same meaning as in section 40;

"overseas authorities" means authorities of a country or territory outside the United Kingdom.

42 Exclusion of matters from legal proceedings

(1) No evidence may be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings or Inquiries Act proceedings which (in any manner)—

(a) discloses, in circumstances from which its origin in interception-related conduct may be inferred, any of the content of an intercepted communication or any related communications data, or

(b) tends to suggest that any interception-related conduct has or may have occurred or may be going to occur.

This is subject to Schedule 3 (exceptions).

(2) "Interception-related conduct" means—

(a) conduct by a person within subsection (3) that was or would be an offence under—

(i) section 2(1) of this Act,

(ii) section 1(1) or (2) of the Regulation of Investigatory Powers Act 2000 ("RIPA"), or

(iii) section 1 of the Interception of Communications Act 1985;

(b) a breach by the Secretary of State of—

(i) the duty under section 7 of this Act, or
(ii) the duty under section 1(4) of RIPA;

(c) the making of an application by any person for a warrant, or the issue of a warrant, under—
(i) Chapter 1 of this Part,
(ii) Chapter 1 of Part 1 of RIPA, or
(iii) the Interception of Communications Act 1985;

(d) the imposition of any requirement on any person to provide assistance in giving effect to—
(i) a targeted interception warrant or mutual assistance warrant, or
(ii) a warrant under Chapter 1 of Part 1 of RIPA.

(3) The persons referred to in subsection (2)(a) are—
(a) any person who is an intercepting authority (see section 15);
(b) any person holding office under the Crown;
(c) any person deemed to be the proper officer of Revenue and Customs by virtue of section 8(2) of the Customs and Excise Management Act 1979;
(d) any person employed by, or for the purposes of, a police force;
(e) any public postal operator or any telecommunications operator;
(f) any person employed or engaged for the purposes of any business of providing a public postal service or a telecommunications service.

(4) In this section—
"Inquiries Act proceedings" means proceedings of an inquiry under the Inquiries Act 2005;
"intercepted communication" means any communication intercepted in the course of its transmission by means of a postal service or telecommunication system.

43 Duty not to make unauthorised disclosures

(1) A person to whom this section applies must not make an unauthorised disclosure to another person.

(2) A person makes an unauthorised disclosure for the purposes of this section if—
(a) the person discloses any of the matters within subsection (4) in relation to a warrant under Chapter 1, and
(b) the disclosure is not an authorised disclosure (see subsection (5)).

(3) This section applies to the following persons—
(a) any person who is an intercepting authority (see section 15);
(b) any person holding office under the Crown;
(c) any person employed by, or for the purposes of, a police force;
(d) any public postal operator or any telecommunications operator;
(e) any person employed or engaged for the purposes of any business of providing a public postal service or a telecommunications service;
(f) any person to whom any of the matters within subsection (4) have been disclosed in relation to a warrant under Chapter 1.

(4) The matters referred to in subsection (2)(a) are—
(a) the existence or contents of the warrant;

(b) the details of the issue of the warrant or of any renewal or modification of the warrant;
(c) the existence or contents of any requirement to provide assistance in giving effect to the warrant;
(d) the steps taken in pursuance of the warrant or of any such requirement;
(e) any of the intercepted material or related communications data obtained under the warrant.

(5) Each of the following is an authorised disclosure for the purposes of this section—
(a) a disclosure that is made to, or authorised by, a Judicial Commissioner;
(b) a disclosure authorised by the warrant;
(c) a disclosure authorised by the person to whom the warrant is or was addressed or under any arrangements made by that person for the purposes of this section;
(d) a disclosure authorised—
(i) by the terms of any requirement to provide assistance in giving effect to the warrant, or
(ii) by section 29(5);
(e) a disclosure made by a legal adviser—
(i) in contemplation of, or in connection with, any legal proceedings, and
(ii) for the purposes of those proceedings;
(f) a disclosure made—
(i) by a professional legal adviser ("L") to L's client or a representative of L's client, or
(ii) by L's client, or by a representative of L's client, to L,
in connection with the giving, by L to L's client, of advice about the effect of provisions of this Part;
(g) a disclosure that—
(i) is made by a public postal operator or a telecommunications operator in accordance with a direction given by the Secretary of State, and
(ii) relates to the number of warrants under Chapter 1 to which the operator has given effect or has been involved in giving effect;
(h) a disclosure of information that does not relate to any particular warrant under Chapter 1 but relates to such warrants in general.

(6) But a disclosure within subsection (5)(e) or (f) is not an authorised disclosure if it is made with a view to furthering any criminal purpose.

(7) The Secretary of State must take such steps as the Secretary of State considers appropriate for bringing a direction given for the purposes of subsection (5)(g) to the attention of any public postal operator or telecommunications operator who may be affected by it.

44 Offence of making unauthorised disclosures

(1) A person who fails to comply with section 43(1) commits an offence.

(2) A person who is guilty of an offence under this section is liable—
(a) on summary conviction in England and Wales—

(i) to imprisonment for a term not exceeding 12 months (or 6 months, if the offence was committed before the commencement of section 154(1) of the Criminal Justice Act 2003), or

(ii) to a fine,

or both;

(b) on summary conviction in Scotland—

(i) to imprisonment for a term not exceeding 12 months, or

(ii) to a fine not exceeding the statutory maximum,

or both;

(c) on summary conviction in Northern Ireland—

(i) to imprisonment for a term not exceeding 6 months, or

(ii) to a fine not exceeding the statutory maximum,

or both;

(d) on conviction on indictment, to imprisonment for a term not exceeding 5 years or to a fine, or both.

(3) In proceedings against any person for an offence under this section in respect of any disclosure, it is a defence for the person to show that the person could not reasonably have been expected, after first becoming aware of the matter disclosed, to take steps to prevent the disclosure.

Interpretation

45 Part 2: interpretation

(1) In this Part—

"EU mutual assistance instrument" has the meaning given by section 7(3);

"intercepted material", in relation to a warrant, means the content of any communications intercepted by an interception authorised or required by the warrant;

"intercepting authority" is to be read in accordance with section 15;

"interception" is to be read in accordance with section 3;

"interfere" and "interference", in relation to wireless telegraphy, have the same meaning as in the Wireless Telegraphy Act 2006 (see section 115(3) of that Act);

"international mutual assistance agreement" has the meaning given by section 7(3);

"lawful authority" is to be read in accordance with section 5;

"mutual assistance warrant" has the meaning given by section 12(4);

"police force" means any of the following—

(a) any police force maintained under section 2 of the Police Act 1996;

(b) the metropolitan police force;

(c) the City of London police force;

(d) the Police Service of Scotland;

(e) the Police Service of Northern Ireland;

(f) the Ministry of Defence Police;

(g) the Royal Navy Police;

(h) the Royal Military Police;

(i) the Royal Air Force Police;
(j) the British Transport Police;

"related communications data" has the meaning given by section 12(6);
"relevant Scottish application" has the meaning given by section 18;
"targeted examination warrant" has the meaning given by section 12(3);
"wireless telegraphy" has the same meaning as in the Wireless Telegraphy Act 2006 (see section 116 of that Act).

(2) References in this Part to the examination of intercepted material are references to the material being read, looked at or listened to by the persons to whom it becomes available as a result of the warrant.

(3) In this Part references to a member of a police force, in relation to the Royal Navy Police, the Royal Military Police or the Royal Air Force Police, do not include any member of that force who is not for the time being attached to, or serving with, that force or another of those police forces.

(4) For the meaning of the following expressions, see section 193—
"public telecommunications service"
"public telecommunication system"
"telecommunications operator"
"telecommunications service"
"telecommunication system".

(5) For the meaning of the following expressions, see section 194—
"postal item"
"postal service"
"public postal operator"
"public postal service".

PART 3

AUTHORISATIONS FOR OBTAINING COMMUNICATIONS DATA

Targeted authorisations for obtaining data

46 Power to grant authorisations

(1) Subsection (2) applies if a designated senior officer of a relevant public authority considers—
(a) that it is necessary to obtain communications data for a purpose falling within subsection (7),
(b) that it is necessary to obtain the data—
(i) for the purposes of a specific investigation or a specific operation, or
(ii) for the purposes of testing, maintaining or developing equipment, systems or other capabilities relating to the availability or obtaining of communications data, and
(c) that the conduct authorised by the authorisation is proportionate to what is sought to be achieved.

(2) The designated senior officer may authorise any officer of the authority to engage in any conduct which—

(a) is for the purpose of obtaining the data from any person, and
(b) relates to—
(i) a telecommunication system, or
(ii) data derived from a telecommunication system.

(3) Subsections (1) and (2) are subject to—
(a) section 47 (additional restrictions on grant of authorisations),
(b) sections 54 and 57 to 59 and Schedule 4 (restrictions relating to certain relevant public authorities),
(c) section 60 (requirement to consult a single point of contact), and
(d) section 61 (Commissioner approval for authorisations to identify or confirm journalistic sources).

(4) Authorised conduct may, in particular, consist of an authorised officer—
(a) obtaining the communications data themselves from any person or telecommunication system,
(b) asking any person whom the authorised officer believes is, or may be, in possession of the communications data to disclose it to a person identified by, or in accordance with, the authorisation,
(c) asking any person whom the authorised officer believes is not in possession of the communications data but is capable of obtaining it, to obtain it and disclose it to a person identified by, or in accordance with, the authorisation, or
(d) requiring by notice a telecommunications operator—
(i) whom the authorised officer believes is, or may be, in possession of the communications data to disclose the data to a person identified by, or in accordance with, the authorisation, or
(ii) whom the authorised officer believes is not in possession of the communications data but is capable of obtaining the data, to obtain it and disclose it to a person identified by, or in accordance with, the authorisation.

(5) An authorisation—
(a) may relate to data whether or not in existence at the time of the authorisation,
(b) may authorise the obtaining or disclosure of data by a person who is not an authorised officer, or any other conduct by such a person, which enables or facilitates the obtaining of the communications data concerned, and
(c) may, in particular, require a telecommunications operator who controls or provides a telecommunication system to obtain or disclose data relating to the use of a telecommunications service provided by another telecommunications operator in relation to that system.

(6) An authorisation—
(a) may not authorise any conduct consisting in the interception of communications in the course of their transmission by means of a telecommunication system, and
(b) may not authorise an authorised officer to ask or require, in the circumstances mentioned in subsection (4)(b), (c) or (d), a person to disclose the data to any person other than—
(i) an authorised officer, or

(ii) an officer of the same relevant public authority as an authorised officer.

(7) It is necessary and proportionate to obtain communications data for a purpose falling within this subsection if it is necessary and proportionate to obtain the data—

(a) in the interests of national security,

(b) for the purpose of preventing or detecting crime or of preventing disorder,

(c) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security,

(d) in the interests of public safety,

(e) for the purpose of protecting public health,

(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department,

(g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health,

(h) to assist investigations into alleged miscarriages of justice,

(i) where a person ("P") has died or is unable to identify themselves because of a physical or mental condition—

(i) to assist in identifying P, or

(ii) to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition, or

(j) for the purpose of exercising functions relating to—

(i) the regulation of financial services and markets, or

(ii) financial stability.

(8) See—

(a) sections 54 and 57 for the meanings of "designated senior officer" and "relevant public authority";

(b) section 68 for the way in which this Part applies to postal operators and postal services.

47 Additional restrictions on grant of authorisations

(1) A designated senior officer may not grant an authorisation for the purposes of a specific investigation or a specific operation if the officer is working on that investigation or operation.

(2) But, if the designated senior officer considers that there are exceptional circumstances which mean that subsection (1) should not apply in a particular case, that subsection does not apply in that case.

(3) Examples of exceptional circumstances include—

(a) an imminent threat to life or another emergency,

(b) the interests of national security, or

(c) the size of the relevant public authority concerned being such that it is not practicable to have a designated senior officer who is not working on the investigation or operation concerned.

(4) A designated senior officer of a relevant public authority which is not a local authority may not grant an authorisation for the purpose of obtaining data which is already held by a telecommunications operator and which is, or can only be obtained by processing, an internet connection record unless the purpose of obtaining the data is to identify—

(a) which person or apparatus is using an internet service where—

(i) the service and time of use are already known, but

(ii) the identity of the person or apparatus using the service is not known,

(b) which internet communications service is being used, and when and how it is being used, by a person or apparatus whose identity is already known, or

(c) where or when a person or apparatus whose identity is already known is obtaining access to, or running, a computer file or computer program which wholly or mainly involves making available, or acquiring, material whose possession is a crime.

(5) A designated senior officer of a local authority may not grant an authorisation for the purpose of obtaining data which is already held by a telecommunications operator and which is, or can only be obtained by processing, an internet connection record.

(6) In this section "internet connection record" means data which—

(a) may be used to identify a telecommunications service to which a communication is transmitted through a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program, and

(b) is generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person).

48 Procedure for authorisations and authorised notices

(1) An authorisation must specify—

(a) the office, rank or position held by the designated senior officer granting it,

(b) the matters falling within section 46(7) by reference to which it is granted,

(c) the conduct that is authorised,

(d) the data or description of data to be obtained, and

(e) the persons or descriptions of persons to whom the data is to be, or may be, disclosed or how to identify such persons.

(2) An authorisation which authorises a person to impose requirements by notice on a telecommunications operator must specify—

(a) the operator concerned, and

(b) the nature of the requirements that are to be imposed,

but need not specify the other contents of the notice.

(3) The notice itself—

(a) must specify—

(i) the office, rank or position held by the person giving it,

(ii) the requirements that are being imposed, and

(iii) the telecommunications operator on whom the requirements are being imposed, and

(b) must be given in writing or (if not in writing) in a manner that produces a record of its having been given.

(4) An authorisation must be applied for, and granted, in writing or (if not in writing) in a manner that produces a record of its having been applied for or granted.

49 Duration and cancellation of authorisations and notices

(1) An authorisation ceases to have effect at the end of the period of one month beginning with the date on which it is granted.

(2) An authorisation may be renewed at any time before the end of that period by the grant of a further authorisation.

(3) Subsection (1) has effect in relation to a renewed authorisation as if the period of one month mentioned in that subsection did not begin until the end of the period of one month applicable to the authorisation that is current at the time of the renewal.

(4) A designated senior officer who has granted an authorisation must cancel it if the designated senior officer considers that the position is no longer as mentioned in section 46(1)(a), (b) and (c).

(5) The Secretary of State may by regulations provide for the person by whom any duty imposed by subsection (4) is to be performed in a case in which it would otherwise fall on a person who is no longer available to perform it.

(6) Such regulations may, in particular, provide for the person on whom the duty is to fall to be a person appointed in accordance with the regulations.

(7) A notice given in pursuance of an authorisation (and any requirement imposed by the notice)—

(a) is not affected by the authorisation subsequently ceasing to have effect under subsection (1), but

(b) is cancelled if the authorisation is cancelled under subsection (4).

50 Duties of telecommunications operators in relation to authorisations

(1) It is the duty of a telecommunications operator on whom a requirement is imposed by notice given in pursuance of an authorisation to comply with that requirement.

(2) It is the duty of a telecommunications operator who is obtaining or disclosing communications data, in response to a request or requirement for the data in pursuance of an authorisation, to obtain or disclose the data in a way that minimises the amount of data that needs to be processed for the purpose concerned.

(3) A person who is under a duty by virtue of subsection (1) or (2) is not required to do anything in pursuance of that duty that it is not reasonably practicable for that person to do.

(4) The duty imposed by subsection (1) or (2) is enforceable by the Secretary of State by civil proceedings for an injunction, or for specific performance of a

statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.

Filtering arrangements for obtaining data

51 Filtering arrangements for obtaining data

(1) The Secretary of State may establish, maintain and operate arrangements for the purposes of—
  (a) assisting a designated senior officer to determine whether, in any case, the officer considers as mentioned in section 46(1)(a), (b) and (c) in relation to the grant of an authorisation in respect of communications data, or
  (b) facilitating the lawful, efficient and effective obtaining of communications data from any person by relevant public authorities in pursuance of an authorisation.

(2) Arrangements under subsection (1) ("filtering arrangements") may, in particular, involve the obtaining of communications data in pursuance of an authorisation ("the target data") by means of—
  (a) a request to the Secretary of State to obtain the target data on behalf of an authorised officer, and
  (b) the Secretary of State—
    (i) obtaining the target data or data from which the target data may be derived,
    (ii) processing the target data or the data from which it may be derived (and retaining data temporarily for that purpose), and
    (iii) disclosing the target data to the person identified for this purpose by, or in accordance with, the authorisation.

(3) Filtering arrangements may, in particular, involve the generation or use by the Secretary of State of information—
  (a) for the purpose mentioned in subsection (1)(a), or
  (b) for the purposes of—
    (i) the support, maintenance, oversight, operation or administration of the arrangements, or
    (ii) the functions of the Investigatory Powers Commissioner mentioned in subsection (4) or (5).

(4) Filtering arrangements must involve the generation and retention of such information or documents as the Investigatory Powers Commissioner considers appropriate for the purposes of the functions of the Commissioner under section 169(1) of keeping under review the exercise by public authorities of functions under this Part.

(5) The Secretary of State must consult the Investigatory Powers Commissioner about the principles on the basis of which the Secretary of State intends to establish, maintain or operate any arrangements for the purpose mentioned in subsection (1)(a).

52 Use of filtering arrangements in pursuance of an authorisation

(1) This section applies in relation to the use of the filtering arrangements in pursuance of an authorisation.

(2) The filtering arrangements may be used—

(a) to obtain and disclose communications data in pursuance of an authorisation, only if the authorisation specifically authorises the use of the arrangements to obtain and disclose the data,

(b) to process data in pursuance of an authorisation (and to retain the data temporarily for that purpose), only if the authorisation specifically authorises processing data of that description under the arrangements (and their temporary retention for that purpose).

(3) An authorisation must record the designated senior officer's decision as to—

(a) whether the communications data to be obtained and disclosed in pursuance of the authorisation may be obtained and disclosed by use of the filtering arrangements,

(b) whether the processing of data under the filtering arrangements (and its temporary retention for that purpose) is authorised,

(c) if the processing of data under the filtering arrangements is authorised, the description of data that may be processed.

(4) A designated senior officer must not grant an authorisation which authorises—

(a) use of the filtering arrangements, or

(b) processing under the filtering arrangements,

unless the condition in subsection (5) is met.

(5) The condition is that the designated senior officer (as well as considering as mentioned in section 46(1)(a), (b) and (c)) considers that what is authorised in relation to the filtering arrangements is proportionate to what is sought to be achieved.

53 Duties in connection with operation of filtering arrangements

(1) The Secretary of State must secure—

(a) that no authorisation data is obtained or processed under the filtering arrangements except for the purposes of an authorisation,

(b) that data which—

(i) has been obtained or processed under the filtering arrangements, and

(ii) is to be disclosed in pursuance of an authorisation or for the purpose mentioned in section 51(1)(a),

is disclosed only to the person to whom the data is to be disclosed in pursuance of the authorisation or (as the case may be) to the designated senior officer concerned,

(c) that any authorisation data which is obtained under the filtering arrangements in pursuance of an authorisation is immediately deleted in such a way as to make access to the data impossible—

(i) when the purposes of the authorisation have been met, or

(ii) if at any time it ceases to be necessary to retain the data for the purposes or purpose concerned.

(2) The Secretary of State must secure that data (other than authorisation data) which is retained under the filtering arrangements is disclosed only—

(a) for the purpose mentioned in section 51(1)(a),

(b) for the purposes of support, maintenance, oversight, operation or administration of the arrangements,

(c) to the Investigatory Powers Commissioner for the purposes of the functions of the Commissioner mentioned in section 51(4) or (5), or

(d) otherwise as authorised by law.

(3) The Secretary of State must secure that—

(a) only the Secretary of State and designated individuals are permitted to read, obtain or otherwise process data for the purposes of support, maintenance, oversight, operation or administration of the filtering arrangements, and

(b) no other persons are permitted to access or use the filtering arrangements except in pursuance of an authorisation or for the purpose mentioned in section 51(1)(a).

(4) In subsection (3)(a) "designated" means designated by the Secretary of State; and the Secretary of State may designate an individual only if the Secretary of State thinks that it is necessary for the individual to be able to act as mentioned in subsection (3)(a).

(5) The Secretary of State must—

(a) put in place and maintain an adequate security system to govern access to, and use of, the filtering arrangements and to protect against any abuse of the power of access, and

(b) impose measures to protect against unauthorised or unlawful data retention, processing, access or disclosure.

(6) The Secretary of State must—

(a) put in place and maintain procedures (including the regular testing of relevant software and hardware) to ensure that the filtering arrangements are functioning properly, and

(b) report, as soon as possible after the end of each calendar year, to the Investigatory Powers Commissioner about the functioning of the filtering arrangements during that year.

(7) A report under subsection (6)(b) must, in particular, contain information about the deletion of authorisation data during the calendar year concerned.

(8) If the Secretary of State believes that significant processing errors have occurred giving rise to a contravention of any of the requirements of this Part which relate to the filtering arrangements, the Secretary of State must report that fact immediately to the Investigatory Powers Commissioner.

(9) In this section "authorisation data", in relation to an authorisation, means communications data that is, or is to be, obtained in pursuance of the authorisation or any data from which that data is, or may be, derived.

Relevant public authorities other than local authorities

54 Relevant public authorities and designated senior officers

(1) Schedule 4 (relevant public authorities and designated senior officers) has effect.

(2) A public authority listed in column 1 of the table in the Schedule is a relevant public authority for the purposes of this Part.

(3) In this Part "designated senior officer", in relation to a relevant public authority listed in column 1 of the table, means an individual who holds with the authority—

(a) an office, rank or position specified in relation to the authority in column 2 of the table, or

(b) an office, rank or position higher than that specified in relation to the authority in column 2 of the table (subject to subsections (4) and (5)).

(4) Subsection (5) applies where an office, rank or position specified in relation to a relevant public authority in column 2 of the table is specified by reference to—

(a) a particular branch, agency or other part of the authority, or

(b) responsibility for functions of a particular description.

(5) A person is a designated senior officer by virtue of subsection (3)(b) only if the person—

(a) holds an office, rank or position in that branch, agency or part, or

(b) has responsibility for functions of that description.

(6) A person who is a designated senior officer of a relevant public authority by virtue of subsection (3) and an entry in column 2 of the table may grant an authorisation—

(a) only for obtaining communications data of the kind specified in the corresponding entry in column 3 of the table, and

(b) only if section 46(1)(a) is satisfied in relation to a purpose within one of the paragraphs of section 46(7) specified in the corresponding entry in column 4 of the table.

(7) Where there is more than one entry in relation to a relevant public authority in column 2 of the table, and a person is a designated senior officer of the authority by virtue of subsection (3) as it applies to more than one of those entries, subsection (6) applies in relation to each entry.

55 Power to modify section 54 and Schedule 4

(1) The Secretary of State may by regulations modify section 54 or Schedule 4.

(2) Regulations under subsection (1) may in particular—

(a) add a public authority to, or remove a public authority from, the list in column 1 of the table,

(b) modify an entry in column 2 of the table,

(c) impose or remove restrictions on the authorisations that may be granted by a designated senior officer with a specified public authority,

(d) impose or remove restrictions on the circumstances in which or purposes for which such authorisations may be granted by a designated senior officer.

(3) The power to make regulations under subsection (1) includes power to make such modifications in any enactment (including this Act) as the Secretary of State considers appropriate in consequence of a person becoming, or ceasing to be, a relevant public authority because of regulations under that subsection.

56 Certain regulations under section 55: supplementary

(1) This section applies to regulations under section 55 other than—

(a) regulations which remove a public authority from the list in column 1 of the table in Schedule 4 and make consequential modifications, and

(b) regulations which modify only column 2 of the table.

(2) Before making regulations to which this section applies, the Secretary of State must consult—

(a) the Investigatory Powers Commissioner, and

(b) the public authority to which the modifications relate.

(3) Regulations to which this section applies may not be made except in accordance with the enhanced affirmative procedure.

Local authorities

57 Local authorities as relevant public authorities

(1) A local authority is a relevant public authority for the purposes of this Part.

(2) In this Part "designated senior officer", in relation to a local authority, means an individual who holds with the authority—

(a) the position of director, head of service or service manager (or equivalent), or

(b) a higher position.

(3) A designated senior officer of a local authority may grant an authorisation for obtaining communications data only if section 46(1)(a) is satisfied in relation to a purpose within section 46(7)(b).

(4) The Secretary of State may by regulations amend subsection (2).

(5) Sections 58 and 59 impose further restrictions in relation to the grant of authorisations by local authorities.

58 Requirement to be party to collaboration agreement

(1) A designated senior officer of a local authority may not grant an authorisation unless—

(a) the local authority is a party to a collaboration agreement (whether as a supplying authority or a subscribing authority or both), and

(b) that collaboration agreement is certified by the Secretary of State (having regard to guidance given by virtue of section 63(6) and (7)) as being appropriate for the local authority.

(2) A designated senior officer of a local authority may only grant an authorisation to a person within subsection (3).

(3) A person is within this subsection if the person is an officer of a relevant public authority which is a supplying authority under a collaboration agreement to which the local authority is a party.

(4) If a local authority is itself a supplying authority under a collaboration agreement, the persons within subsection (3) include officers of the local authority.

(5) In this section "collaboration agreement", "subscribing authority" and "supplying authority" have the same meaning as in section 62.

59 Judicial approval for local authority authorisations

(1) This section applies to an authorisation granted by a designated senior officer of a local authority other than an authorisation to which section 61 applies.

(2) The authorisation is not to take effect until such time (if any) as the relevant judicial authority has made an order under this section approving it.

(3) The local authority may apply to the relevant judicial authority for an order under this section approving the authorisation.

(4) The local authority is not required to give notice of the application to—
(a) any person to whom the authorisation relates, or
(b) that person's legal representatives.

(5) The relevant judicial authority may approve the authorisation if, and only if, the relevant judicial authority considers that—
(a) at the time of the grant, there were reasonable grounds for considering that the requirements of this Part were satisfied in relation to the authorisation, and
(b) at the time when the relevant judicial authority is considering the matter, there are reasonable grounds for considering that the requirements of this Part would be satisfied if an equivalent new authorisation were granted at that time.

(6) Where, on an application under this section, the relevant judicial authority refuses to approve the grant of the authorisation, the relevant judicial authority may make an order quashing the authorisation.

(7) In this section "the relevant judicial authority" means—
(a) in relation to England and Wales, a justice of the peace,
(b) in relation to Scotland, a sheriff, and
(c) in relation to Northern Ireland, a district judge (magistrates' courts) in Northern Ireland.

Additional protections

60 Requirement to consult a single point of contact

(1) Before granting an authorisation, the designated senior officer must consult a person who is acting as a single point of contact.

(2) But, if the designated senior officer considers that there are exceptional circumstances which mean that subsection (1) should not apply in a particular case, that subsection does not apply in that case.

(3) Examples of exceptional circumstances include—
(a) an imminent threat to life or another emergency, or
(b) the interests of national security.

(4) A person is acting as a single point of contact if that person—
(a) is an officer of a relevant public authority, and
(b) is responsible for advising—
(i) officers of the relevant public authority about applying for authorisations, or

(ii) designated senior officers of the relevant public authority about granting authorisations.

(5) A person acting as a single point of contact may, in particular, advise an officer of a relevant public authority who is considering whether to apply for an authorisation about—

(a) the most appropriate methods for obtaining data where the data concerned is processed by more than one telecommunications operator,

(b) the cost, and resource implications, for—

(i) the relevant public authority concerned of obtaining the data, and

(ii) the telecommunications operator concerned of disclosing the data,

(c) any unintended consequences of the proposed authorisation, and

(d) any issues as to the lawfulness of the proposed authorisation.

(6) A person acting as a single point of contact may, in particular, advise a designated senior officer who is considering whether to grant an authorisation about—

(a) whether it is reasonably practical to obtain the data sought in pursuance of the proposed authorisation,

(b) the cost, and resource implications, for—

(i) the relevant public authority concerned of obtaining the data, and

(ii) the telecommunications operator concerned of disclosing the data,

(c) any unintended consequences of the proposed authorisation, and

(d) any issues as to the lawfulness of the proposed authorisation.

(7) A person acting as a single point of contact may also provide advice about—

(a) whether requirements imposed by virtue of an authorisation have been met,

(b) the use in support of operations or investigations of communications data obtained in pursuance of such an authorisation, and

(c) any other effects of an authorisation.

61 Commissioner approval for authorisations to identify or confirm journalistic sources

(1) Subsection (2) applies if—

(a) a designated senior officer has granted an authorisation in relation to the obtaining by a relevant public authority (other than an intelligence service) of communications data for the purpose of identifying or confirming a source of journalistic information, and

(b) the authorisation is not necessary because of an imminent threat to life.

(2) The authorisation is not to take effect until such time (if any) as a Judicial Commissioner has made an order under this section approving it.

(3) The relevant public authority for which the authorisation has been granted may apply to a Judicial Commissioner for an order under this section approving the authorisation.

(4) The applicant is not required to give notice of the application to—
  (a) any person to whom the authorisation relates, or
  (b) that person's legal representatives.

(5) A Judicial Commissioner may approve the authorisation if, and only if, the Judicial Commissioner considers that—
  (a) at the time of the grant, there were reasonable grounds for considering that the requirements of this Part were satisfied in relation to the authorisation, and
  (b) at the time when the Judicial Commissioner is considering the matter, there are reasonable grounds for considering that the requirements of this Part would be satisfied if an equivalent new authorisation were granted at that time.

(6) Where, on an application under this section, the Judicial Commissioner refuses to approve the grant of the authorisation, the Judicial Commissioner may make an order quashing the authorisation.

(7) In this Act "source of journalistic information" means an individual who provides material intending the recipient to use it for the purposes of journalism or knowing that it is likely to be so used.

Collaboration agreements

62 Collaboration agreements

(1) A collaboration agreement is an agreement (other than a police collaboration agreement) under which—
  (a) a relevant public authority ("the supplying authority") puts the services of designated senior officers of that authority or other officers of that authority at the disposal of another relevant public authority ("the subscribing authority") for the purposes of the subscribing authority's functions under this Part, and
  (b) either—
    (i) a designated senior officer of the supplying authority is permitted to grant authorisations to officers of the subscribing authority,
    (ii) officers of the supplying authority are permitted to be granted authorisations by a designated senior officer of the subscribing authority, or
    (iii) officers of the supplying authority act as single points of contact for officers of the subscribing authority.

(2) The persons by whom, or to whom, authorisations may be granted (or who may act as single points of contact) under a collaboration agreement are additional to those persons by whom, or to whom, authorisations would otherwise be granted under this Part (or who could otherwise act as single points of contact).

(3) In a case falling within subsection (1)(b)(i)—
  (a) section 46 has effect as if—
    (i) in subsection (2) the reference to an officer of the authority were a reference to an officer of the subscribing authority, and

(ii) in subsection (6)(b)(ii) the reference to an officer of the same relevant public authority as an authorised officer included a reference to an officer of the supplying authority, and

(b) section 47(3)(c) has effect as if the reference to the relevant public authority concerned were a reference to both authorities.

(4) In a case falling within subsection (1)(b)(ii)—

(a) section 46 has effect as if—

(i) in subsection (2) the reference to an officer of the authority were a reference to an officer of the supplying authority, and

(ii) in subsection (6)(b)(ii) the reference to an officer of the same relevant public authority as an authorised officer included a reference to an officer of the subscribing authority, and

(b) section 47(3)(c) has effect as if the reference to the relevant public authority concerned were a reference to both authorities.

(5) In a case falling within subsection (1)(b)(iii), section 60(4)(b) has effect as if the references to the relevant public authority were references to the subscribing authority.

(6) In this section "police collaboration agreement" means a collaboration agreement under section 22A of the Police Act 1996 which contains force collaboration provision (within the meaning of section 22A(2)(a) of that Act).

63 Collaboration agreements: supplementary

(1) A collaboration agreement may provide for payments to be made between parties to the agreement.

(2) A collaboration agreement—

(a) must be in writing,

(b) may be varied by a subsequent collaboration agreement, and

(c) may be brought to an end by agreement between the parties to it.

(3) A person who makes a collaboration agreement must—

(a) publish the agreement, or

(b) publish the fact that the agreement has been made and such other details about it as the person considers appropriate.

(4) A relevant public authority may enter into a collaboration agreement as a supplying authority, a subscribing authority or both (whether or not it would have power to do so apart from this section).

(5) The Secretary of State may, after consulting a relevant public authority, direct it to enter into a collaboration agreement if the Secretary of State considers that entering into the agreement would assist the effective exercise by the authority, or another relevant public authority, of its functions under this Part.

(6) A code of practice under Schedule 6 must include guidance to relevant public authorities about collaboration agreements.

(7) The guidance must include guidance about the criteria the Secretary of State will use in considering whether a collaboration agreement is appropriate for a relevant public authority.

64 Police collaboration agreements

(1) This section applies if—

(a) the chief officer of police of an England and Wales police force ("force 1") has entered into a police collaboration agreement, and

(b) under the terms of the agreement—

(i) a designated senior officer of force 1 is permitted to grant authorisations to officers of a collaborating police force,

(ii) officers of force 1 are permitted to be granted authorisations by a designated senior officer of a collaborating police force, or

(iii) officers of force 1 act as single points of contact for officers of a collaborating police force.

(2) The persons by whom, or to whom, authorisations may be granted (or who may act as single points of contact) under a police collaboration agreement are additional to those persons by whom, or to whom, authorisations would otherwise be granted under this Part (or who could otherwise act as single points of contact).

(3) In a case falling within subsection (1)(b)(i)—

(a) section 46 has effect as if—

(i) in subsection (2) the reference to an officer of the authority were a reference to an officer of the collaborating police force, and

(ii) in subsection (6)(b)(ii) the reference to an officer of the same relevant public authority as an authorised officer included a reference to an officer of force 1, and

(b) section 47(3)(c) has effect as if the reference to the relevant public authority concerned were a reference to force 1 and the collaborating police force.

(4) In a case falling within subsection (1)(b)(ii)—

(a) section 46 has effect as if—

(i) in subsection (2) the reference to an officer of the authority were a reference to an officer of force 1, and

(ii) in subsection (6)(b)(ii) the reference to an officer of the same relevant public authority as an authorised officer included a reference to an officer of the collaborating police force, and

(b) section 47(3)(c) has effect as if the reference to the relevant public authority concerned were a reference to force 1 and the collaborating police force.

(5) In a case falling within subsection (1)(b)(iii), section 60(4)(b) has effect as if the references to the relevant public authority were references to the collaborating police force.

(6) In this section—

"collaborating police force", in relation to a police collaboration agreement, means a police force (other than force 1) whose chief officer of police is a party to the agreement,

"England and Wales police force" means—

(a) any police force maintained under section 2 of the Police Act 1996 (police forces in England and Wales outside London),

(b) the metropolitan police force, or

(c) the City of London police force,

"police collaboration agreement" means a collaboration agreement under section 22A of the Police Act 1996 which contains force collaboration provisions (within the meaning of section 22A(2)(a) of that Act).

Further and supplementary provision

65 Lawfulness of conduct authorised by this Part

(1) Conduct is lawful for all purposes if—
  (a) it is conduct in which any person is authorised to engage by an authorisation or required to undertake by virtue of a notice given in pursuance of an authorisation, and
  (b) the conduct is in accordance with, or in pursuance of, the authorisation or notice.

(2) A person (whether or not the person so authorised or required) is not to be subject to any civil liability in respect of conduct that—
  (a) is incidental to, or is reasonably undertaken in connection with, conduct that is lawful by virtue of subsection (1), and
  (b) is not itself conduct for which an authorisation or warrant—
    (i) is capable of being granted under any of the enactments mentioned in subsection (3), and
    (ii) might reasonably have been expected to have been sought in the case in question.

(3) The enactments referred to in subsection (2)(b)(i) are—
  (a) an enactment contained in this Act,
  (b) an enactment contained in the Regulation of Investigatory Powers Act 2000,
  (c) an enactment contained in Part 3 of the Police Act 1997 (powers of the police and of customs officers), or
  (d) section 5 of the Intelligence Services Act 1994 (warrants for the intelligence services).

66 Offence of making unauthorised disclosure

(1) It is an offence for a telecommunications operator, or any person employed for the purposes of the business of a telecommunications operator, to disclose, without reasonable excuse, to any person the existence of—
  (a) any requirement imposed on the operator by virtue of this Part to disclose communications data relating to that person, or
  (b) any request made in pursuance of an authorisation for the operator to disclose such data.

(2) For the purposes of subsection (1), it is, in particular, a reasonable excuse if the disclosure is made with the permission of the relevant public authority which is seeking to obtain the data from the operator (whether the permission is contained in any notice requiring the operator to disclose the data or otherwise).

(3) A person guilty of an offence under this section is liable—
  (a) on summary conviction in England and Wales—

(i) to imprisonment for a term not exceeding 12 months (or 6 months, if the offence was committed before the commencement of section 154(1) of the Criminal Justice Act 2003), or

(ii) to a fine,

or both;

(b) on summary conviction in Scotland—

(i) to imprisonment for a term not exceeding 12 months, or

(ii) to a fine not exceeding the statutory maximum,

or both;

(c) on summary conviction in Northern Ireland—

(i) to imprisonment for a term not exceeding 6 months, or

(ii) to a fine not exceeding the statutory maximum,

or both;

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or both.

67 Certain transfer and agency arrangements with public authorities

(1) The Secretary of State may by regulations provide for—

(a) any function under sections 51 to 53 which is exercisable by the Secretary of State to be exercisable instead by another public authority, or

(b) any function under sections 51 to 53 which is exercisable by a public authority by virtue of paragraph (a) to be exercisable instead by the Secretary of State.

(2) The Secretary of State may by regulations modify any enactment about a public authority for the purpose of enabling or otherwise facilitating any function exercisable by the Secretary of State under this Part to be exercisable on behalf of the Secretary of State by the authority concerned.

(3) Regulations under subsection (2) do not affect the Secretary of State's responsibility for the exercise of the functions concerned.

(4) Subsection (2) does not apply in relation to any function of the Secretary of State of making regulations.

(5) Schedule 5 (which contains further safeguards and provisions supplementing this section) has effect.

68 Application of Part 3 to postal operators and postal services

(1) This Part applies to postal operators and postal services as it applies to telecommunications operators and telecommunications services.

(2) In its application by virtue of subsection (1), this Part has effect as if—

(a) any reference to a telecommunications operator were a reference to a postal operator,

(b) any reference to a telecommunications service were a reference to a postal service,

(c) any reference to a telecommunication system were a reference to a postal service,

(d) in section 47, subsections (4) to (6) were omitted, and

(e) in Part 2 of Schedule 4, for "which is entity data" there were substituted "within paragraph (c) of the definition of "communications data" in section 194(3)".

69 Extra-territorial application of Part 3

(1) An authorisation may relate to conduct outside the United Kingdom and persons outside the United Kingdom.

(2) A notice given in pursuance of an authorisation may relate to conduct outside the United Kingdom and persons outside the United Kingdom.

(3) Where such a notice is to be given to a person outside the United Kingdom, the notice may (in addition to electronic or other means of giving a notice) be given to the person in any of the following ways—

(a) by delivering it to the person's principal office within the United Kingdom or, if the person has no such office in the United Kingdom, to any place in the United Kingdom where the person carries on business or conducts activities,

(b) if the person has specified an address in the United Kingdom as one at which the person, or someone on the person's behalf, will accept documents of the same description as a notice, by delivering it to that address,

(c) by notifying the person by such other means as the authorised officer considers appropriate (which may include notifying the person orally).

(4) In determining for the purposes of subsection (3) of section 50 whether it is reasonably practicable for a telecommunications operator outside the United Kingdom to take any steps in a country or territory outside the United Kingdom for the purpose of complying with a duty imposed by virtue of subsection (1) or (2) of that section, the matters to be taken into account include the following—

(a) any requirements or restrictions under the law of that country or territory that are relevant to the taking of those steps, and

(b) the extent to which it is reasonably practicable to comply with the duty in a way that does not breach any of those requirements or restrictions.

(5) Nothing in the definition of "telecommunications operator" limits the type of communications data in relation to which an authorisation, or a request or requirement of a kind which gives rise to a duty under section 50(1) or (2), may apply.

70 Part 3: interpretation

(1) In this Part—

"authorisation" means an authorisation under section 46 (including that section as modified by sections 62 and 64),

"designated senior officer"—

(a) in relation to a relevant public authority which is a local authority, has the meaning given by section 57(2), and

(b) in relation to any other relevant public authority, has the meaning given by section 54(3),

"filtering arrangements" means any arrangements under section 51(1),

"officer", in relation to a relevant public authority, means a person holding an office, rank or position with that authority,

"relevant public authority" means a public authority which is a relevant public authority for the purposes of this Part by virtue of section 54(2) or 57(1).

(2) In this Part "local authority" means—

(a) a district or county council in England,

(b) a London borough council,

(c) the Common Council of the City of London in its capacity as a local authority,

(d) the Council of the Isles of Scilly,

(e) a county council or county borough council in Wales,

(f) a council constituted under section 2 of the Local Government etc. (Scotland) Act 1994, and

(g) a district council in Northern Ireland.

(3) See also—

section 193 (telecommunications definitions),

section 194 (postal definitions),

section 195 (general definitions).

PART 4

RETENTION OF COMMUNICATIONS DATA

General

71 Powers to require retention of certain data

(1) The Secretary of State may by notice (a "retention notice") require a telecommunications operator to retain relevant communications data if the Secretary of State considers that the requirement is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (j) of section 46(7) (purposes for which communications data may be obtained).

(2) A retention notice may—

(a) relate to a particular operator or any description of operators,

(b) require the retention of all data or any description of data,

(c) identify the period or periods for which data is to be retained,

(d) contain other requirements, or restrictions, in relation to the retention of data,

(e) make different provision for different purposes,

(f) relate to data whether or not in existence at the time of the giving, or coming into force, of the notice.

(3) A retention notice must not require any data to be retained for more than 12 months beginning with—

(a) in the case of communications data relating to a specific communication, the day of the communication concerned,

(b) in the case of entity data which does not fall within paragraph (a) above but does fall within paragraph (a)(i) of the definition of "communications data" in section 193(5), the day on which the entity

concerned ceases to be associated with the telecommunications service concerned or (if earlier) the day on which the data is changed, and

(c) in any other case, the day on which the data is first held by the operator concerned.

(4) A retention notice which relates to data already in existence when the notice comes into force imposes a requirement to retain the data for only so much of a period of retention as occurs on or after the coming into force of the notice.

(5) A retention notice comes into force—

(a) when the notice is given to the operator (or description of operators) concerned, or

(b) (if later) at the time or times specified in the notice.

(6) A retention notice is given to an operator (or description of operators) by giving, or publishing, it in such manner as the Secretary of State considers appropriate for bringing it to the attention of the operator (or description of operators) to whom it relates.

(7) A retention notice must specify—

(a) the operator (or description of operators) to whom it relates,

(b) the data which is to be retained,

(c) the period or periods for which the data is to be retained,

(d) any other requirements, or any restrictions, in relation to the retention of the data,

(e) the information required by section 185(7) (the level or levels of contribution in respect of costs incurred as a result of the notice).

(8) The requirements or restrictions mentioned in subsection (7)(d) may, in particular, include—

(a) a requirement to retain the data in such a way that it can be transmitted efficiently and effectively in response to requests,

(b) requirements or restrictions in relation to the obtaining (whether by collection, generation or otherwise), generation or processing of—

(i) data for retention, or

(ii) retained data.

(9) In this Part "relevant communications data" means communications data which may be used to identify, or assist in identifying, any of the following—

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

(b) the time or duration of a communication,

(c) the type, method or pattern, or fact, of communication,

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

(e) the location of any such system, or

(f) the internet protocol address, or other identifier, of any apparatus to which a communication is transmitted for the purpose of obtaining access to, or running, a computer file or computer program.

In this subsection "identifier" means an identifier used to facilitate the transmission of a communication.

Safeguards

72 Matters to be taken into account before giving retention notices

(1) Before giving a retention notice, the Secretary of State must, among other matters, take into account—

(a) the likely benefits of the notice,

(b) the likely number of users (if known) of any telecommunications service to which the notice relates,

(c) the technical feasibility of complying with the notice,

(d) the likely cost of complying with the notice, and

(e) any other effect of the notice on the telecommunications operator (or description of operators) to whom it relates.

(2) Before giving such a notice, the Secretary of State must take reasonable steps to consult any operator to whom it relates.

73 Review by the Secretary of State

(1) A telecommunications operator to whom a retention notice is given may, within such period or circumstances as may be provided for by regulations made by the Secretary of State, refer the notice back to the Secretary of State.

(2) Such a reference may be in relation to the whole of a notice or any aspect of it.

(3) In the case of a notice given to a description of operators—

(a) each operator falling within that description may make a reference under subsection (1), but

(b) each such reference may only be in relation to the notice, or aspect of the notice, so far as it applies to that operator.

(4) There is no requirement for an operator who has referred a retention notice under subsection (1) to comply with the notice, so far as referred, until the Secretary of State has reviewed the notice in accordance with subsection (5).

(5) The Secretary of State must review any notice so far as referred to the Secretary of State under subsection (1).

(6) Before deciding the review, the Secretary of State must consult—

(a) the Technical Advisory Board, and

(b) the Investigatory Powers Commissioner.

(7) The Board must consider the technical requirements and the financial consequences, for the operator who has made the reference, of the notice so far as referred.

(8) The Commissioner must consider whether the notice so far as referred is proportionate.

(9) The Board and the Commissioner must—

(a) give the operator concerned the opportunity to provide evidence to them before reaching their conclusions, and

(b) report their conclusions to—

(i) the operator, and

(ii) the Secretary of State.

(10) The Secretary of State may, after considering the conclusions of the Board and the Commissioner—

(a) vary or revoke the retention notice under section 76, or

(b) give a notice under this section to the operator concerned confirming its effect.

(11) A report or notice under this section is given to an operator by giving or publishing it in such manner as the Secretary of State considers appropriate for bringing it to the attention of the operator.

(12) The Secretary of State must keep a retention notice under review (whether or not referred under subsection (1)).

74 Data integrity and security

(1) A telecommunications operator who retains relevant communications data by virtue of this Part must—

(a) secure that the data is of the same integrity, and subject to at least the same security and protection, as the data on any system from which it is derived,

(b) secure, by appropriate technical and organisational measures, that the data can be accessed only by specially authorised personnel, and

(c) protect, by appropriate technical and organisational measures, the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful retention, processing, access or disclosure.

(2) A telecommunications operator who retains relevant communications data by virtue of this Part must destroy the data if the retention of the data ceases to be authorised by virtue of this Part and is not otherwise authorised by law.

(3) The requirement in subsection (2) to destroy the data is a requirement to delete the data in such a way as to make access to the data impossible.

(4) The deletion of the data may take place at such monthly or shorter intervals as appear to the operator to be practicable.

75 Disclosure of retained data

A telecommunications operator must put in place adequate security systems (including technical and organisational measures) governing access to relevant communications data retained by virtue of this Part in order to protect against any unlawful disclosure.

Variation or revocation of notices

76 Variation or revocation of notices

(1) The Secretary of State may vary a retention notice.

(2) The Secretary of State must give, or publish, notice of the variation in such manner as the Secretary of State considers appropriate for bringing the variation to the attention of the telecommunications operator (or description of operators) to whom it relates.

(3) A variation comes into force—

(a) when notice of it is given or published in accordance with subsection (2), or

(b) (if later) at the time or times specified in the notice of variation.

(4) A retention notice may not be varied so as to require the retention of additional relevant communications data unless the Secretary of State considers that the requirement is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (j) of section 46(7) (purposes for which communications data may be obtained).

(5) Section 71(2) and (4) apply in relation to a retention notice as varied as they apply in relation to a retention notice, but as if the references to the notice coming into force included references to the variation coming into force.

(6) Sections 71(3) and (8), 77 and 79, and subsections (1), (4), (9) and (12) of this section, apply in relation to a retention notice as varied as they apply in relation to a retention notice.

(7) Section 72 applies in relation to the making of a variation as it applies in relation to the giving of a retention notice.

(8) Section 73 applies in relation to a retention notice as varied (other than one varied as mentioned in subsection (10)(a) of that section) as it applies in relation to a retention notice.

(9) The Secretary of State may revoke (whether wholly or in part) a retention notice.

(10) The Secretary of State must give or publish notice of the revocation in such manner as the Secretary of State considers appropriate for bringing the revocation to the attention of the operator (or description of operators) to whom it relates.

(11) A revocation comes into force—

(a) when notice of it is given or published in accordance with subsection (10), or

(b) (if later) at the time or times specified in the notice of revocation.

(12) The fact that a retention notice has been revoked in relation to a particular description of communications data and a particular operator (or description of operators) does not prevent the giving of another retention notice in relation to the same description of data and the same operator (or description of operators).

Enforcement

77 Enforcement of notices and certain other requirements and restrictions

(1) It is the duty of a telecommunications operator on whom a requirement or restriction is imposed by—

(a) a retention notice, or

(b) section 74 or 75,

to comply with the requirement or restriction.

(2) A telecommunications operator, or any person employed for the purposes of the business of a telecommunications operator, must not disclose the existence and contents of a retention notice to any other person.

(3) The duty under subsection (1) or (2) is enforceable by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.

Further and supplementary provision

78 Application of Part 4 to postal operators and postal services

(1) This Part applies to postal operators and postal services as it applies to telecommunications operators and telecommunications services.

(2) In its application by virtue of subsection (1), this Part has effect as if—

(a) any reference to a telecommunications operator were a reference to a postal operator,

(b) any reference to a telecommunications service were a reference to a postal service,

(c) any reference to a telecommunication system were a reference to a postal service,

(d) in section 71(3), for paragraph (b) there were substituted—

"(b) in the case of communications data which does not fall within paragraph (a) above but does fall within paragraph (c) of the definition of "communications data" in section 194(3), the day on which the person concerned leaves the postal service concerned or (if earlier) the day on which the data is changed,", and

(e) in section 71(9), in the definition of "relevant communications data", paragraph (f) were omitted.

79 Extra-territorial application of Part 4

(1) A retention notice, and any requirement or restriction imposed by virtue of a retention notice or by section 74 or 75, may relate to conduct outside the United Kingdom and persons outside the United Kingdom.

(2) Section 77(1) has effect, in relation to a requirement or restriction imposed by virtue of a retention notice or by section 74 or 75 and which relates to conduct or persons outside the United Kingdom, as a duty to have regard to the requirement or restriction (rather than comply with it).

80 Part 4: interpretation

(1) In this Part—

"notice" means notice in writing,

"relevant communications data" has the meaning given by section 71(9),

"retention notice" has the meaning given by section 71(1).

(2) See also—

section 193 (telecommunications definitions),

section 194 (postal definitions),

section 195 (general definitions).

PART 5

EQUIPMENT INTERFERENCE

Warrants under this Part

81 Warrants under this Part: general

(1) There are two kinds of warrants that may be issued under this Part—
  (a) targeted equipment interference warrants (see subsection (2));
  (b) targeted examination warrants (see subsection (9)).

(2) A targeted equipment interference warrant is a warrant that authorises the person to whom it is addressed to secure interference with any equipment for the purpose of facilitating the obtaining of one or more of the following—
  (a) communications (see section 105);
  (b) private information (see section 105);
  (c) equipment data (see section 82).

(3) A targeted equipment interference warrant may also authorise the person to whom it is addressed to secure—
  (a) the obtaining of any communications, private information or equipment data to which the purpose of the warrant relates;
  (b) the obtaining of any information that does not fall within paragraph (a) but is connected with the equipment to which the warrant relates;
  (c) the disclosure, in such manner as may be described in the warrant, of any material obtained under the warrant by virtue of paragraph (a) or (b).

(4) The reference in subsections (2) and (3) to the obtaining of communications or private information includes doing so by—
  (a) monitoring, observing or listening to a person's communications or other activities;
  (b) recording anything that is monitored, observed or listened to.

(5) A targeted equipment interference warrant also authorises the following conduct (in addition to the conduct described in the warrant)—
  (a) any conduct that it is necessary to undertake in order to do what is expressly authorised by the warrant, including conduct for securing the obtaining of—
    (i) communications;
    (ii) private information;
    (iii) equipment data;
    (iv) information that does not fall within sub-paragraphs (i) to (iii) but is connected with the equipment to which the warrant relates; and
  (b) any conduct by any person that is in pursuance of a requirement imposed by or on behalf of the person to whom the warrant is addressed to be provided with assistance in giving effect to the warrant.

(6) A targeted equipment interference warrant may not, by virtue of subsection (3), authorise a person to engage in conduct, in relation to a communication

other than a stored communication, that would (unless done with lawful authority) constitute an offence under section 2(1) (unlawful interception).

(7) Subsection (5)(a) does not authorise a person to engage in conduct that could not be expressly authorised under the warrant because of the restriction imposed by subsection (6).

(8) In subsection (6), "stored communication" means a communication stored in or by a telecommunication system.

(9) A targeted examination warrant is a warrant that authorises the person to whom it is addressed to carry out the examination of material obtained under a bulk equipment interference warrant.

For provision about bulk equipment interference warrants, see Chapter 3 of Part 6.

(10) For provision enabling the combination of targeted equipment interference warrants with certain other warrants or authorisations (including targeted examination warrants), see Schedule 7.

82 Meaning of "equipment data"

(1) In this Part, "equipment data" means—
- (a) communications data (see section 193(5));
- (b) data that falls within subsection (2) or (4).

(2) Data falls within this subsection if it identifies or describes anything connected with enabling or otherwise facilitating the functioning of a relevant system (including any apparatus in it) or of any service provided by means of the system.

(3) For the purposes of subsection (2), a system is a relevant system if any communications or private information are held on or by means of the system.

(4) Data falls within this subsection if, for the purposes of a relevant system, it is comprised in, included as part of, attached to or logically associated with a communication or an item of private information and either—
- (a) it does not form part of the content of the communication or the item of private information, or
- (b) if it does, it is capable of being logically separated from the remainder of the content in such a way that (after being separated)—
  - (i) it would not reveal anything of what might reasonably be expected to be the meaning of the communication or item of information, disregarding any meaning arising from the fact of the communication or the existence of the item of information or from any data relating to that fact, and
  - (ii) it would be data falling within subsection (5).

(5) The data falling within this subsection is—
- (a) data which may be used to identify, or assist in identifying, any person, apparatus, system or service;
- (b) data which may be used to identify any event;
- (c) data which may be used to identify the location of any person, event or thing.

(6) For the purposes of subsection (5), the reference to data which may be used to identify any event includes—

(a) data relating to the fact of the event;

(b) data relating to the type, method or pattern of event;

(c) data relating to the time or duration of the event.

(7) In subsection (4), "relevant system" means any system on or by means of which the data is held.

(8) For the purposes of this section, the content of a communication or an item of private information is the elements of the communication or item, and any data attached to or logically associated with it, which reveal anything of what might reasonably be expected to be the meaning of the communication or item, disregarding any meaning arising from the fact of the communication or the existence of the item or from any data relating to that fact.

83 Subject-matter of warrants

A targeted equipment interference warrant may relate to—

(a) equipment belonging to, used by or in the possession of a particular person or organisation;

(b) equipment belonging to, used by or in the possession of persons who form a group that shares a common purpose or who carry on, or may be carrying on, a particular activity;

(c) equipment belonging to, used by or in the possession of more than one person or organisation, where the interference is for the purpose of the same investigation or operation;

(d) equipment in a particular location;

(e) equipment in more than one location, where the interference is for the purpose of the same investigation or operation;

(f) equipment that is being, or may be being used, for the purposes of a particular activity or activities of a particular description;

(g) equipment that is being, or may be used, to test, maintain or develop capabilities relating to interference with equipment for the purpose of obtaining communications, private information or equipment data.

Power to issue warrants

84 Power to issue warrants to intelligence services: the Secretary of State

(1) The Secretary of State may, on an application made by or on behalf of the head of an intelligence service, issue a targeted equipment interference warrant if—

(a) the Secretary of State considers that the warrant is necessary on grounds falling within subsection (4),

(b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(c) where the warrant includes provision by virtue of section 81(3), the Secretary of State considers that satisfactory arrangements made for the purposes of section 103 (general safeguards) are in force in relation to the warrant, and

(d) except where the Secretary of State considers that there is an urgent need to issue the warrant, the decision to issue it has been approved by a Judicial Commissioner.

(2) But the Secretary of State may not issue a targeted equipment interference warrant under subsection (1) if—

(a) the Secretary of State considers that the only ground for considering the warrant to be necessary is for the purpose of preventing or detecting serious crime, and

(b) the warrant, if issued, would authorise interference only with equipment that would be in Scotland at the time of the issue of the warrant or that the Secretary of State believes would be in Scotland at that time.

For the power of the Scottish Ministers to issue a targeted equipment interference warrant, see section 86.

(3) The Secretary of State may, on an application made by or on behalf of the head of an intelligence service, issue a targeted examination warrant if—

(a) the Secretary of State considers that the warrant is necessary on grounds falling within subsection (4),

(b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(c) the Secretary of State considers that the warrant is or may be necessary to authorise the selection of protected material in breach of the prohibition in section 147(4), and

(d) the decision to issue the warrant has been approved by a Judicial Commissioner.

For the meaning of protected material, see section 147(8).

(4) A warrant is necessary on grounds falling within this subsection if it is necessary—

(a) in the interests of national security,

(b) for the purpose of preventing or detecting serious crime, or

(c) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security.

(5) A warrant may be considered necessary on the ground falling within subsection (4)(c) only if the interference with equipment that would be authorised by the warrant is considered necessary to facilitate the obtaining of information relating to the acts or intentions of persons outside the British Islands.

(6) The matters to be taken into account in considering whether the conditions in paragraphs (a) and (b) of subsection (1) are met include whether what is sought to be achieved by the warrant could reasonably be achieved by other means.

(7) An application for the issue of a warrant under this section may only be made on behalf of the head of an intelligence service by a person holding office under the Crown.

(8) Nothing in subsection (2) prevents the Secretary of State from doing anything under this section for the purposes specified in section 2(2) of the European Communities Act 1972.

85 Additional protection for Members of Parliament etc.

(1) This section applies where—

(a) an application is made to the Secretary of State for the issue of a targeted equipment interference warrant or a targeted examination warrant, and

(b) the purpose of the warrant is—

(i) in the case of a targeted equipment interference warrant, to facilitate the obtaining of communications sent by, or intended for, a person who is a member of a relevant legislature or the obtaining of private information in the possession of a member of a relevant legislature, or

(ii) in the case of a targeted examination warrant, to authorise the examination of such communications or private information.

(2) Before deciding whether to issue the warrant, the Secretary of State must consult the Prime Minister.

(3) In this section "member of a relevant legislature" means—

(a) a member of either House of Parliament;

(b) a member of the Scottish Parliament;

(c) a member of the National Assembly for Wales;

(d) a member of the Northern Ireland Assembly;

(e) a member of the European Parliament elected for the United Kingdom.

86 Power to issue warrants to intelligences services: the Scottish Ministers

(1) The Scottish Ministers may, on an application made by or on behalf of the head of an intelligence service, issue a targeted equipment interference warrant if—

(a) the warrant authorises interference only with equipment that is in Scotland at the time the warrant is issued or that the Scottish Ministers believe to be in Scotland at that time,

(b) the Scottish Ministers consider that the warrant is necessary for the purpose of preventing or detecting serious crime,

(c) the Scottish Ministers consider that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(d) where the warrant includes provision by virtue of section 81(3), the Scottish Ministers consider that satisfactory arrangements made for the purposes of section 103 (general safeguards) are in force in relation to the warrant, and

(e) except where the Scottish Ministers consider that there is an urgent need to issue the warrant, the decision to issue the warrant has been approved by a Judicial Commissioner.

(2) The matters to be taken into account in considering whether the conditions in paragraphs (b) and (c) of subsection (1) are met include whether what is sought to be achieved by the warrant could reasonably be achieved by other means.

(3) An application for the issue of a warrant under this section may only be made on behalf of the head of an intelligence service by a person holding office under the Crown.

87 Power to issue warrants to the Chief of Defence Intelligence

(1) The Secretary of State may, on an application made by or on behalf of the Chief of Defence Intelligence, issue a targeted equipment interference warrant if—

(a) the Secretary of State considers that the warrant is necessary in the interests of national security,

(b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(c) where the warrant includes provision by virtue of section 81(3), the Secretary of State considers that satisfactory arrangements made for the purposes of section 103 (general safeguards) are in force in relation to the warrant, and

(d) except where the Secretary of State considers that there is an urgent need to issue a warrant, the decision to issue it has been approved by a Judicial Commissioner.

(2) The matters to be taken into account in considering whether the conditions in paragraphs (a) and (b) of subsection (1) are met include whether what is sought to be achieved by the warrant could reasonably be achieved by other means.

(3) An application for the issue of a warrant under this section may only be made on behalf of the Chief of Defence Intelligence by a person holding office under the Crown.

88 Decision to issue warrants under sections 84 to 87 to be taken personally by Ministers

(1) The decision to issue a warrant under section 84 or 87 must be taken personally by the Secretary of State.

(2) The decision to issue a warrant under section 86 must be taken personally by a member of the Scottish Government.

(3) A warrant issued under section 84 or 87 must, before it is issued, be signed—

(a) by the Secretary of State, or

(b) in an urgent case, by a senior official designated by the Secretary of State for that purpose.

(4) A warrant issued under section 86 must, before it is issued, be signed—

(a) by the member of the Scottish Government who issued it, or

(b) in an urgent case, by a senior official designated by the Scottish Ministers for that purpose.

(5) Where a warrant is signed by a senior official, the warrant must contain a statement that the case is an urgent case in which the Secretary of State or (as the case may be) the Scottish Ministers have personally expressly authorised the issue of the warrant.

89 Power to issue warrants to law enforcement officers

(1) A law enforcement chief may, on an application made by a person who is an appropriate law enforcement officer in relation to the chief, issue a targeted equipment interference warrant if—

(a) the law enforcement chief considers that the warrant is necessary for the purpose of preventing or detecting serious crime,

(b) the law enforcement chief considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(c) where the warrant includes provision by virtue of section 81(3), the law enforcement chief considers that satisfactory arrangements made for the purposes of section 103 (general safeguards) are in force in relation to the warrant, and

(d) except where the law enforcement chief considers that there is an urgent need to issue the warrant, the decision to issue it has been approved by a Judicial Commissioner.

(2) The matters to be taken into account in considering whether the conditions in paragraphs (a) and (b) of subsection (1) are met include whether what is sought to be achieved by the warrant could reasonably be achieved by other means.

(3) If it is not reasonably practicable for a law enforcement chief to consider an application under this section, an appropriate delegate may, in an urgent case, exercise the power to issue a targeted equipment interference warrant.

(4) For the purposes of this section—

(a) a person is a law enforcement chief if the person is listed in the first column of the table set out below;

(b) a person is an appropriate delegate in relation to a law enforcement chief listed in the first column if the person is listed in the corresponding entry in the second column;

(c) a person is an appropriate law enforcement officer in relation to a law enforcement chief listed in the first column if the person is listed in the corresponding entry in the third column.

Law enforcement chiefs	*Appropriate delegates*	*Appropriate law enforcement officers*
The Chief Constable of a police force maintained under section 2 of the Police Act 1996.	The person who is the appropriate deputy chief constable for the purposes of section 12A(1) of the Police Act 1996. The person holding the rank of assistant chief constable designated to act under section 12A(2) of that Act. If it is not reasonably practicable for either of those persons to act, any other person holding the rank of assistant chief constable in the force.	A member of the police force or a member of a collaborative force.

Law enforcement chiefs	*Appropriate delegates*	*Appropriate law enforcement officers*
The Commissioner, or an Assistant Commissioner, of the metropolitan police force.	A person holding the rank of commander in the metropolitan police force.	A member of the metropolitan police force or a member of a collaborative force.
The Commissioner of Police for the City of London.	The person authorised to act under section 25 of the City of London Police Act 1839 or, if it is not reasonably practicable for that person to act, a person holding the rank of commander in the City of London police force.	A member of the City of London police force or a member of a collaborative force.
The chief constable of the Police Service of Scotland.	Any deputy chief constable or assistant chief constable of the Police Service of Scotland who is designated for the purpose by the chief constable.	A constable of the Police Service of Scotland.
The Chief Constable or a Deputy Chief Constable of the Police Service of Northern Ireland.	A person holding the rank of assistant chief constable in the Police Service of Northern Ireland.	A member of the Police Service of Northern Ireland.
The Director General of the National Crime Agency.	A senior National Crime Agency Officer designated for the purpose by the Director General of the National Crime Agency.	A National Crime Agency officer.
An officer of Revenue and Customs who is a senior official within the meaning of the Regulation of Investigatory Powers Act 2000 and who is designated for the purpose by the Commissioners for Her Majesty's Revenue and Customs.	An officer of Revenue and Customs who is a senior official within the meaning of the Regulation of Investigatory Powers Act 2000 and who is designated for the purpose by the Commissioners for Her Majesty's Revenue and Customs.	An officer of Revenue and Customs.

Law enforcement chiefs	*Appropriate delegates*	*Appropriate law enforcement officers*
The Chief Constable of the Ministry of Defence Police.	A person holding the rank of deputy chief constable or assistant chief constable in the Ministry of Defence Police.	A member of the Ministry of Defence Police.
The Provost Marshal of the Royal Navy Police.	A person holding the position of Assistant Provost Marshal in the Royal Navy Police.	A member of the Royal Navy Police.
The Provost Marshal of the Royal Military Police.	A person holding the position of deputy Provost Marshal in the Royal Military Police.	A member of the Royal Military Police.
The Provost Marshal of the Royal Air Force Police.	A person holding the position of deputy Provost Marshal in the Royal Air Force Police.	A member of the Royal Air Force Police.

(5) For the purposes of the first three entries in the third column of the table in subsection (4), a police force (police force 1) is a collaborative force in relation to another police force (police force 2) if—

(a) the chief officers of both police forces are parties to the same agreement under section 22A of the Police Act 1996, and

(b) the members of police force 1 are permitted by the terms of the agreement to make applications under this section to the chief officer of police force 2.

(6) In subsection (5), "police force" means—

(a) any police force maintained under section 2 of the Police Act 1996;

(b) the metropolitan police force;

(c) the City of London police force.

(7) Where the law enforcement chief is the Chief Constable or the Deputy Chief Constable of the Police Service of Northern Ireland, the reference in subsection (1)(a) to the purpose of preventing or detecting serious crime includes a reference to the interests of national security.

90 Approval of warrants by Judicial Commissioners

(1) In deciding whether to approve a person's decision to issue a warrant under this Part, a Judicial Commissioner must review the person's conclusions on the following matters—

(a) whether the warrant is necessary on any relevant grounds (see subsection (3)), and

(b) whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

(2) In doing so, the Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review.

(3) In subsection (1)(a), "relevant grounds" means—

(a) in the case of a warrant to be issued under section 84, grounds falling within section 84(4);

(b) in the case of a warrant to be issued under section 86, the purpose of preventing or detecting serious crime;

(c) in the case of a warrant to be issued under section 87, the interests of national security;

(d) in the case of a warrant to be issued under section 89, the purpose of preventing or detecting serious crime.

(4) Where a Judicial Commissioner refuses to approve a decision to issue a warrant, the Judicial Commissioner must give the person who made that decision written reasons for the refusal.

(5) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to issue a warrant, the person who made that decision may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant.

91 Approval of warrants issued in urgent cases

(1) This section applies where—

(a) a targeted equipment interference warrant is issued without the approval of a Judicial Commissioner, and

(b) the person who issued the warrant considered that there was an urgent need to issue it.

(2) The person who issued the warrant must inform a Judicial Commissioner that it has been issued.

(3) The Judicial Commissioner must, before the end of the relevant period—

(a) decide whether to approve the decision to issue the warrant, and

(b) notify the person of the Judicial Commissioner's decision.

"The relevant period" means the period ending with the fifth working day after the day on which the warrant was issued.

(4) But subsection (3) does not apply if the Judicial Commissioner is notified that the warrant is to be renewed under section 95 before the end of the relevant period.

(5) If a Judicial Commissioner refuses to approve the decision to issue a warrant, the warrant ceases to have effect.

(6) Section 92 contains further provision about what happens when a warrant ceases to have effect as a result of this section.

92 Warrants ceasing to have effect under section 91

(1) This section applies where a warrant ceases to have effect as a result of section 91.

(2) The person to whom the warrant is addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible.

(3) The Judicial Commissioner who refused to approve the warrant—

(a) may authorise further interference with equipment for the purpose of enabling the person to whom the warrant is addressed to secure that anything in the process of being done under the warrant stops as soon as possible;
(b) may direct that any material obtained under the warrant is destroyed;
(c) may impose conditions as to the use or retention of any of that material.

(4) The Judicial Commissioner—
(a) may require an affected party to make representations about how the Judicial Commissioner should exercise any function under subsection (3), and
(b) must have regard to any such representations made by an affected party (whether or not as a result of a requirement imposed under paragraph (a)).

(5) Each of the following is an "affected party" for the purposes of subsection (4)—
(a) the person who decided to issue the warrant;
(b) the person to whom the warrant is addressed.

(6) The person who decided to issue the warrant may ask the Investigatory Powers Commissioner to review a decision made by any other Judicial Commissioner under subsection (3).

(7) On a review under subsection (6), the Investigatory Powers Commissioner may—
(a) confirm the Judicial Commissioner's decision, or
(b) make a fresh determination.

(8) Nothing in this section or section 91 affects the lawfulness of—
(a) anything done under the warrant before it ceases to have effect;
(b) if anything is in the process of being done under the warrant when it ceases to have effect—
(i) anything done before that thing could be stopped, or
(ii) anything done that it is not reasonably practicable to stop.

Further provision about warrants

93 Requirements that must be met by warrants

(1) A warrant under this Part must contain a provision stating that it is a targeted equipment interference warrant or a targeted examination warrant.

(2) A warrant under this Part must be addressed—
(a) in the case of a warrant issued under section 84 or 86, to the head of the intelligence service by whom or on whose behalf the application for the warrant was made;
(b) in the case of a warrant issued under section 87, to the Chief of Defence Intelligence;
(c) in the case of a warrant issued under section 89, to the law enforcement officer who applied for the warrant.

(3) In the case of a targeted equipment interference warrant that relates to equipment described in the first column of the Table below, the warrant must include the details specified in the second column.

Nature of warrant	*Details to be included in the warrant*
A warrant relating to equipment belonging to, used by or in the possession of a particular person or organisation	The name of the person or organisation or a description of the person or organisation
A warrant relating to equipment belonging to, used by or in the possession of persons who form a group that shares a common purpose or who carry on, or may be carrying on, a particular activity	A description of the purpose or activity and the name of, or a description of, as many of the persons as it is reasonably practicable to name or describe
A warrant relating to equipment used by or in the possession of more than one person or organisation, where the interference is for the purpose of the same investigation or operation	A description of the nature of the investigation or operation and the name of, or a description of, as many of the persons or organisations as it is reasonably practicable to name or describe
A warrant relating to equipment in a particular location	A description of the location
A warrant relating to equipment in more than one location, where the interference is for the purpose of the same investigation or operation	A description of the nature of the investigation or operation and a description of as many of the locations as it is reasonably practicable to describe
A warrant relating to equipment that is being, or may be being used, for the purposes of a particular activity or activities of a particular description	A description of the particular activity or activities
A warrant relating to equipment that is being, or may be used, to test, maintain or develop capabilities relating to interference with equipment	A description of the nature of the testing, maintenance or development of capabilities

(4) A targeted equipment interference warrant must describe—

(a) the type of equipment that is to be interfered with, and

(b) the conduct that the person to whom the warrant is addressed is authorised to take.

94 Duration of warrants

(1) A warrant issued under this Part, if it is not renewed before the end of the relevant period (see subsection (2)), ceases to have effect at the end of that period.

(2) In this section, "the relevant period"—

(a) in the case of an urgent warrant (see subsection (3)), means the period ending with the fifth working day after the day on which the warrant was issued;

(b) in any other case, means the period of 6 months beginning with—

(i) the day on which the warrant was issued, or

(ii) in the case of a warrant that has been renewed, the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed.

(3) For the purposes of subsection (2)(a) an "urgent warrant" is a warrant which—

(a) was signed by a senior official in accordance with section 88(3)(b) or (4)(b), and

(b) has not been renewed.

(4) For provision about the renewal of warrants, see section 95.

95 Renewal of warrants

(1) If the renewal conditions are met, a warrant issued under this Part may be renewed, at any time before the end of the relevant period, by an instrument issued by the appropriate person.

(2) The renewal conditions are—

(a) that the appropriate person considers that—

(i) the warrant continues to be necessary on any relevant grounds, and

(ii) the conduct authorised by the warrant continues to be proportionate to what is sought to be achieved by that conduct, and

(b) that the decision to renew the warrant has been approved by a Judicial Commissioner.

(3) The appropriate person is—

(a) in the case of a warrant issued under section 84 or 87, the Secretary of State;

(b) in the case of a warrant issued under section 86, a member of the Scottish Government;

(c) in the case of a warrant issued under section 89 to a law enforcement officer, either—

(i) a person who is the law enforcement chief in relation to that officer, or

(ii) a person who is an appropriate delegate in relation to the law enforcement chief if that person issued the warrant.

(4) In subsection (2)(a), "relevant grounds" means—

(a) in the case of a warrant issued under section 84, grounds falling within section 84(4),

(b) in the case of a warrant issued under section 86, the purpose of preventing or detecting serious crime,

(c) in the case of a warrant issued under section 87, the interests of national security, or

(d) in the case of a warrant issued under section 89, the purpose of preventing or detecting serious crime.

(5) The decision to renew a warrant issued under section 84 or 87 must be taken personally by the Secretary of State, and the instrument renewing the warrant must be signed by the Secretary of State.

(6) The decision to renew a warrant issued under section 86 must be taken personally by a member of the Scottish Government, and the instrument renewing the warrant must be signed by the person who took that decision.

(7) The instrument renewing a warrant issued under section 89 must be signed by the person who renews it.

(8) Section 85 (additional protection for Members of Parliament etc.) applies in relation to a decision to renew a warrant issued by the Secretary of State as it applies in relation to a decision to issue a warrant.

(9) Section 91 (approval of warrants by Judicial Commissioners) applies in relation to a decision to renew a warrant as it applies in relation to a decision to issue a warrant (and accordingly any reference in that section to the person who decided to issue the warrant is to be read as a reference to the person who decided to renew it).

(10) In this section, "relevant period" has the same meaning as in section 94.

96 Modification of warrants

(1) The provisions of a warrant issued under this Part may be modified at any time by an instrument issued by the person making the modification.

(2) The modifications that may be made are—

(a) adding any name or description to the names or descriptions included in the warrant in accordance with section 93(3) or (4);

(b) varying any such name or description;

(c) removing any such name or description.

(3) A modification may be made only if—

(a) the person making the modification considers that—

(i) the warrant as modified continues to be necessary on any relevant grounds (see subsection (4)), and

(ii) the conduct authorised by the warrant as so modified is proportionate to what is sought to be achieved by that conduct, and

(b) in the case of a modification of a warrant issued to a law enforcement officer under section 89, the decision to make the modification has been approved by a Judicial Commissioner.

(4) In subsection (3)(a), "relevant grounds" means—

(a) in the case of a warrant issued under section 84, grounds falling within section 84(4);
(b) in the case of a warrant issued under section 86, the purpose of preventing or detecting serious crime;
(c) in the case of a warrant issued under section 87, the interests of national security;
(d) in the case of a warrant issued under section 89, the purpose of preventing or detecting serious crime.

(5) The decision to make any modification must be taken personally by the person making the modification, and the instrument making the modification must be signed by that person.

(6) Section 90 (approval of warrants by Judicial Commissioners) applies in relation to a decision to make a modification of a warrant issued under section 89 as it applies in relation to a decision to issue such a warrant, but as if—
(a) the references in subsection (1)(a) and (b) of that section to the warrant were references to the warrant as modified, and
(b) any reference to the person who decided to issue the warrant were a reference to the person who decided to make the modification.

(7) Section 97—
(a) sets out who may make modifications of a warrant under this section, and
(b) makes other provision to supplement this section.

(8) Nothing in this section applies in relation to modifying the provisions of a warrant in a way that does not affect the conduct authorised by it.

97 Modification of warrants: supplementary provision

(1) The persons who may make modifications of a warrant under this Part are—
(a) in the case of a warrant issued by the Secretary of State under section 84 or 87—
(i) the Secretary of State, or
(ii) a senior official acting on behalf of the Secretary of State;
(b) in the case of a warrant issued by the Scottish Ministers under section 86—
(i) a member of the Scottish Government, or
(ii) a senior official acting on behalf of the Scottish Ministers;
(c) in the case of a warrant issued under section 89 to a law enforcement officer, either—
(i) a person who is the law enforcement chief in relation to that officer, or
(ii) a person who is an appropriate delegate in relation to the law enforcement chief if that person issued the warrant.

(2) Section 85 (additional protection for Members of Parliament etc.) applies in relation to a decision to make a modification of a warrant issued by the Secretary of State as it applies in relation to a decision to issue a warrant; and accordingly where that section applies only the Secretary of State may make the modification.

(3) Where a senior official has made a modification of a warrant issued under section 84 or 87, the Secretary of State must be notified personally of the modification and the reasons for making it.

(4) Where a senior official has made a modification of a warrant issued under section 86, a member of the Scottish Government must be notified personally of the modification and the reasons for making it.

98 Cancellation of warrants

(1) Any of the appropriate persons may cancel a warrant issued under this Part at any time.

(2) If any of the appropriate persons considers—

(a) that a warrant issued under this Part is no longer necessary on any relevant grounds, or

(b) that the conduct authorised by a warrant issued under this Part is no longer proportionate to what is sought to be achieved by the conduct,

the person must cancel the warrant.

(3) In subsection (2)(a), "relevant grounds" means—

(a) in the case of a warrant issued under section 84, grounds falling within section 84(4);

(b) in the case of a warrant issued under section 86, the purpose of preventing or detecting serious crime;

(c) in the case of a warrant issued under section 87, the interests of national security;

(d) in the case of a warrant issued under section 89, the purpose of preventing or detecting serious crime.

(4) For the purposes of this section, the appropriate persons are—

(a) in the case of a warrant issued by the Secretary of State under section 84 or 87, the Secretary of State or a senior official acting on behalf of the Secretary of State;

(b) in the case of a warrant issued by the Scottish Ministers under section 86, a member of the Scottish Government or a senior official acting on behalf of the Scottish Ministers;

(c) in the case of a warrant issued under section 89 to a law enforcement officer, either—

(i) a person who is a law enforcement chief in relation to that officer, or

(ii) a person who is an appropriate delegate in relation to the law enforcement chief if that person issued the warrant.

Implementation of warrants

99 Implementation of warrants

(1) In giving effect to a targeted equipment interference warrant, the person to whom it is addressed may (in addition to acting on its own) act through, or together with, such other persons as the person may require (whether under subsection (2) or otherwise) to provide it with assistance in giving effect to the warrant.

(2) For the purpose of requiring any person to provide assistance in relation to a targeted equipment interference warrant, the person to whom it is addressed may—

(a) serve a copy of the warrant on any person whom it considers may be able to provide such assistance, or

(b) make arrangements for the service of a copy of the warrant on any such person.

(3) A copy of a warrant may be served under subsection (2) on a person outside the United Kingdom for the purpose of requiring the person to provide such assistance in the form of conduct outside the United Kingdom.

(4) The references in subsections (2) and (3) to the service of a copy of a warrant include—

(a) the service of a copy of one or more schedules contained in the warrant with the omission of the remainder of the warrant, and

(b) the service of a copy of the warrant with the omission of any schedule contained in it.

100 Service of warrants

(1) This section applies to the service of warrants under section 99(2).

(2) A copy of a warrant may be served on a person outside the United Kingdom in any of the following ways (as well as by electronic or other means of service)—

(a) by serving it at the person's principal office within the United Kingdom or, if the person has no such office in the United Kingdom, at any place in the United Kingdom where the person carries on business or conducts activities;

(b) if the person has specified an address in the United Kingdom as one at which the person, or someone on the person's behalf, will accept service of documents of the same description as a copy of a warrant, by serving it at that address;

(c) by making it available for inspection (whether to the person or to someone acting on the person's behalf) at a place in the United Kingdom (but this is subject to subsection (3)).

(3) A copy of a warrant may be served on a person outside the United Kingdom in the way mentioned in subsection (2)(c) only if—

(a) it is not reasonably practicable for a copy to be served by any other means (whether as mentioned in subsection (2)(a) or (b) or otherwise), and

(b) the person to whom the warrant is addressed takes such steps as it considers appropriate for the purpose of bringing the contents of the warrant, and the availability of a copy for inspection, to the attention of the person.

(4) The steps mentioned in subsection (3)(b) must be taken as soon as reasonably practicable after the copy of the warrant is made available for inspection.

101 Duty of telecommunications providers to assist with implementation

(1) A relevant telecommunications provider that has been served with a copy of a targeted equipment interference warrant issued by the Secretary of State under section 84 or 87, or by the Scottish Ministers under section 86, must take all

steps for giving effect to the warrant that are notified to the relevant telecommunications provider by or on behalf of the person to whom the warrant is addressed.

(2) A relevant telecommunications provider that has been served with a copy of a targeted equipment interference warrant issued under section 89 and addressed to a law enforcement officer mentioned in subsection (3) must take all steps for giving effect to the warrant that—

(a) were approved by the Secretary of State before the warrant was served, and

(b) are notified to the relevant telecommunications provider by or on behalf of the law enforcement officer.

(3) The law enforcement officers mentioned in this subsection are—

(a) a National Crime Agency officer;

(b) an officer of Revenue and Customs;

(c) a constable of the Police Service of Scotland;

(d) a member of the Police Service of Northern Ireland;

(e) a member of the metropolitan police force.

(4) The Secretary of State may give approval for the purposes of subsection (2)(a) if the Secretary of State considers that—

(a) it is necessary for the relevant telecommunications provider to be required to take the steps, and

(b) the steps are proportionate to what is sought to be achieved by them.

(5) In this section, "relevant telecommunications provider" means any of the following—

(a) a person who provides a public telecommunications service;

(b) a person not falling within paragraph (a) who has control of the whole or any part of a public telecommunications system located wholly or partly in, or controlled from, the United Kingdom.

(6) A relevant telecommunications provider is not required by virtue of this section to take any steps that it is not reasonably practicable for the relevant telecommunications provider to take.

(7) The duty imposed by subsection (1) or (2) is enforceable against a person in the United Kingdom by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.

102 Offence of making unauthorised disclosure

(1) A relevant telecommunications provider who has been required under this Part to provide assistance in giving effect to a targeted equipment interference warrant, and any person employed for the purposes of the business of the relevant telecommunications provider, may not, without reasonable excuse, disclose to any person—

(a) the existence and contents of the warrant,

(b) the existence and contents of the requirement imposed on the relevant telecommunications provider to provide assistance in giving effect to it, and

(c) any steps taken in pursuance of the requirement.

(2) For the purposes of subsection (1), it is, in particular, a reasonable excuse if the disclosure is made with the permission of the person who imposed the requirement.

(3) A person who fails to comply with subsection (1) is guilty of an offence and liable—

(a) on summary conviction in England and Wales—

(i) to imprisonment for a term not exceeding 12 months (or 6 months if the offence was committed before the commencement of section 154(1) of the Criminal Justice Act 2003), or

(ii) to a fine,

or to both;

(b) on summary conviction in Scotland—

(i) to imprisonment for a term not exceeding 12 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(c) on summary conviction in Northern Ireland—

(i) to imprisonment for a term not exceeding 6 months, or

(ii) to a fine not exceeding the statutory maximum,

or to both;

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or to both.

(4) In this section, "relevant telecommunications provider" has the same meaning as in section 101.

Supplementary provision

103 Safeguards for material obtained

(1) This section applies in relation to every targeted equipment interference warrant that includes authorisation to secure the obtaining of communications, private information, equipment data or other information connected with the equipment to which the warrant relates.

(2) The Secretary of State must ensure that arrangements are in force for securing that the requirements of subsections (3) and (6) are met in relation to the material obtained under the warrant.

(3) The requirements of this subsection are met in relation to the material obtained under the warrant if each of the following is limited to the minimum that is necessary for the authorised purposes (see subsection (4))—

(a) the number of persons to whom any of the material is disclosed or otherwise made available;

(b) the extent to which any of the material is disclosed or otherwise made available;

(c) the extent to which any of the material is copied;

(d) the number of copies that are made.

(4) For the purposes of subsection (3), something is necessary for the authorised purposes if, and only if—

(a) it is, or is likely to become, necessary on any relevant grounds (see subsection (8)),

(b) it is necessary for facilitating the carrying out of any functions under this Act of the Secretary of State, the Scottish Ministers or the person to whom the warrant is addressed,

(c) it is necessary for facilitating the carrying out of any functions of the Investigatory Powers Commissioner or of the Investigatory Powers Tribunal under or in relation to this Act,

(d) it is necessary for the purpose of legal proceedings, or

(e) it is necessary for the performance of the functions of any person by or under any enactment.

(5) The arrangements for the time being in force under this section for securing that the requirements of subsection (3) are met in relation to the material obtained under the warrant must include arrangements for securing that every copy made of any of that material is stored, for so long as it is retained, in a secure manner.

(6) The requirements of this subsection are met in relation to the material obtained under the warrant if every copy made of any of that material (if not destroyed earlier) is destroyed as soon as there are no longer any grounds for retaining it (see subsection (7)).

(7) For the purposes of subsection (6), there are no longer any grounds for retaining a copy of any material if, and only if—

(a) its retention is not necessary, or not likely to become necessary, on any relevant grounds (see subsection (8)), and

(b) its retention is not necessary for any of the purposes mentioned in paragraphs (b) to (e) of subsection (4) above.

(8) In subsections (4) and (7), "relevant grounds" means—

(a) in relation to a warrant issued under section 84, grounds falling within section 84(4);

(b) in relation to a warrant issued under section 86, the purpose of preventing or detecting serious crime;

(c) in relation to a warrant issued under section 87, the interests of national security;

(d) in relation to a warrant issued under section 89, the purpose of preventing or detecting serious crime.

(9) In this section—

"appropriate authority" means—

(a) in the case of a warrant issued under section 84 or 87, the Secretary of State;

(b) in the case of a warrant issued under section 86, the Scottish Ministers;

(c) in the case of a warrant issued under section 89, the person to whom the warrant is addressed;

"copy", in relation to material, means any of the following (whether or not in documentary form)—

(a) any copy, extract or summary of the material which identifies itself as the product of a targeted equipment interference warrant, and

(b) any record which is a record of the identities of persons who owned, used or were in possession of equipment interfered with under such a warrant,

and "copied" is to be read accordingly.

104 Restriction on issue of targeted equipment interference warrants to certain law enforcement officers

(1) A targeted equipment interference warrant may not be issued under section 89 on the application of any of the following law enforcement officers unless the person who has power to issue the warrant considers that there is a British Islands connection—

(a) a member of a police force maintained under section 2 of the Police Act 1996;

(b) a member of the metropolitan police force;

(c) a member of the City of London police force;

(d) a constable of the Police Service of Scotland;

(e) a member of the Police Service of Northern Ireland.

(2) For the purpose of this section, there is a British Islands connection if—

(a) any of the conduct authorised by the warrant would take place in the British Islands (regardless of the location of the equipment that would, or may, be interfered with),

(b) any of the equipment that would, or may, be interfered with would, or may, be in the British Islands at some time while the interference is taking place, or

(c) a purpose of the interference is to facilitate the obtaining of—

(i) communications sent by, or to, a person who is, or whom the intelligence service believes to be, for the time being in the British Islands, or

(ii) private information relating to an individual who is, or whom the intelligence service believes to be, for the time being in the British Islands.

(3) A targeted equipment interference warrant may be issued under section 89 on the application of a law enforcement officer who does not fall within subsection (1)(a) to (e) whether or not the person who has power to issue the warrant considers that there is a British Islands connection.

105 Part 5: interpretation

In this Part—

"communication" includes—

(a) anything comprising speech, music, sounds, visual images or data of any description, and

(b) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus;

"equipment" means equipment producing electromagnetic, acoustic or other emissions or any device capable of being used in connection with such equipment;

"equipment data" has the meaning given by section 82;

"private information" includes information relating to a person's private or family life;

"senior official" means—

(a) in the case of a targeted equipment interference warrant issued by the Secretary of State, a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service;

(b) in the case of a targeted equipment interference warrant issued by the Scottish Ministers, a member of the staff of the Scottish Administration who is a member of the Senior Civil Service;

"targeted examination warrant" has the meaning given by section 81(9).

PART 6

BULK WARRANTS

CHAPTER 1

BULK INTERCEPTION WARRANTS

Bulk interception warrants

106 Bulk interception warrants

(1) For the purposes of this Act a "bulk interception warrant" is a warrant issued under this Chapter which meets conditions A and B.

(2) Condition A is that the main purpose of the warrant is one or more of the following—

(a) the interception of overseas-related communications (see subsection (3));

(b) the obtaining of related communications data from such communications (see subsection (6)).

(3) In this Chapter "overseas-related communications" means—

(a) communications sent by individuals who are outside the British Islands, or

(b) communications received by individuals who are outside the British Islands.

(4) Condition B is that the warrant authorises or requires the person to whom it is addressed to secure, by any conduct described in the warrant, any one or more of the following activities—

(a) the interception, in the course of their transmission by means of a telecommunication system, of communications described in the warrant;

(b) the obtaining of related communications data from communications described in the warrant;

(c) the selection for examination, in any manner described in the warrant, of intercepted material or related communications data obtained under the warrant;

(d) the disclosure, in any manner described in the warrant, of such material or data to the person to whom the warrant is addressed or to any person acting on that person's behalf.

(5) A bulk interception warrant also authorises the following conduct (in addition to the conduct described in the warrant)—

(a) any conduct which it is necessary to undertake in order to do what is expressly authorised or required by the warrant, including—

(i) the interception of communications not described in the warrant, and

(ii) conduct for obtaining related communications data from such communications;

(b) conduct by any person which is conduct in pursuance of a requirement imposed by or on behalf of the person to whom the warrant is addressed to be provided with assistance in giving effect to the warrant.

(6) In this Chapter "related communications data", in relation to a communication transmitted by means of a telecommunication system, means data falling within subsection (7) or (8).

(7) The data falling within this subsection is so much of any data as is obtained while the communication is being transmitted, or at any time when the communication is stored in or by the system (whether before or after its transmission), and—

(a) is communications data (see section 193(5)) relating to the communication or to the sender or recipient, or intended recipient, of the communication, or

(b) is comprised in, included as part of, attached to or logically associated with the communication (whether by the sender or otherwise) and enables or otherwise facilitates the functioning of—

(i) a telecommunication system (including any apparatus forming part of the system), or

(ii) any telecommunications service provided by means of a telecommunication system.

(8) The data falling within this subsection is so much of the content of the communication (see section 193(6)) as—

(a) is capable of being logically separated from the remainder of the content of the communication, and

(b) if it were so separated—

(i) would not reveal anything of what might reasonably be expected to be the meaning of the communication, disregarding any meaning arising from the fact of the communication or from any data relating to the transmission of the communication, and

(ii) would be data falling within subsection (9).

(9) The data falling within this subsection is—

(a) data which may be used to identify, or assist in identifying, any person, apparatus, telecommunication system or telecommunications service, and

(b) data which describes an event or the location of any person, event or thing.

107 Power to issue bulk interception warrants

(1) The Secretary of State may, on an application made by or on behalf of the head of an intelligence service, issue a bulk interception warrant if—

(a) the Secretary of State considers that the main purpose of the warrant is one or more of the following—

(i) the interception of overseas-related communications, and

(ii) the obtaining of related communications data from such communications,

(b) the Secretary of State considers that the warrant is necessary—

(i) in the interests of national security, or

(ii) on that ground and on any other grounds falling within subsection (2),

(c) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(d) the Secretary of State considers that—

(i) the examination of intercepted material or related communications data obtained under the warrant is necessary for one or more of the specified operational purposes (see subsection (6)), and

(ii) any examination of that material or data for those purposes is necessary as mentioned in paragraph (b),

(e) the Secretary of State considers that satisfactory arrangements made for the purposes of section 117 (general safeguards) are in force in relation to the warrant,

(f) if the Secretary of State considers that a telecommunications operator outside the United Kingdom is likely to be required to provide assistance in giving effect to the warrant if it is issued, the Secretary of State has complied with section 108, and

(g) the decision to issue the warrant has been approved by a Judicial Commissioner.

For the meaning of "head of an intelligence service", see section 195.

(2) A warrant is necessary on grounds falling within this subsection if it is necessary—

(a) for the purpose of preventing or detecting serious crime, or

(b) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security (but see subsection (3)).

(3) A warrant may be considered necessary on the ground falling within subsection (2)(b) only if the information which it is considered necessary to obtain is information relating to the acts or intentions of persons outside the British Islands.

(4) A warrant may not be considered necessary in the interests of national security or on any other grounds falling within subsection (2) if it is considered necessary only for the purpose of gathering evidence for use in any legal proceedings.

(5) The matters to be taken into account in considering whether the conditions in paragraphs (b) and (c) of subsection (1) are met include whether the information which it is considered necessary to obtain under the warrant could reasonably be obtained by other means.

(6) In subsection (1)(d) "the specified operational purposes" means the operational purposes specified in the warrant in accordance with section 111.

(7) An application for the issue of a bulk interception warrant may only be made on behalf of the head of an intelligence service by a person holding office under the Crown.

108 Additional requirements in respect of warrants affecting overseas operators

(1) This section applies where—
  (a) an application for a bulk interception warrant has been made, and
  (b) the Secretary of State considers that a telecommunications operator outside the United Kingdom is likely to be required to provide assistance in giving effect to the warrant if it is issued.

(2) Before issuing the warrant, the Secretary of State must consult the operator.

(3) Before issuing the warrant, the Secretary of State must, among other things, take into account—
  (a) the likely benefits of the warrant,
  (b) the likely number of users (if known) of any telecommunications service which is provided by the operator and to which the warrant relates,
  (c) the technical feasibility of complying with any requirement that may be imposed on the operator to provide assistance in giving effect to the warrant,
  (d) the likely cost of complying with any such requirement, and
  (e) any other effect of the warrant on the operator.

109 Approval of warrants by Judicial Commissioners

(1) In deciding whether to approve a decision to issue a warrant under section 107, a Judicial Commissioner must review the Secretary of State's conclusions as to the following matters—
  (a) whether the warrant is necessary as mentioned in subsection (1)(b) of that section,
  (b) whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct,
  (c) whether—
    (i) the examination of intercepted material or related communications data obtained under the warrant is necessary for one or more of the specified operational purposes, and
    (ii) any examination of that material or data for those purposes is necessary as mentioned in subsection (1)(b) of that section, and
  (d) any matters taken into account in accordance with section 108.

(2) In doing so, the Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review.

(3) Where a Judicial Commissioner refuses to approve a decision to issue a warrant under section 107, the Judicial Commissioner must give the Secretary of State written reasons for the refusal.

(4) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to issue a warrant under section 107, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant.

(5) In this section "the specified operational purposes" has the same meaning as in section 107.

110 Decisions to issue warrants to be taken personally by Secretary of State

(1) The decision to issue a bulk interception warrant must be taken personally by the Secretary of State.

(2) Before a bulk interception warrant is issued, it must be signed by the Secretary of State.

111 Requirements that must be met by warrants

(1) A bulk interception warrant must contain a provision stating that it is a bulk interception warrant.

(2) A bulk interception warrant must be addressed to the head of the intelligence service by whom, or on whose behalf, the application for the warrant was made.

(3) A bulk interception warrant must specify the operational purposes for which any intercepted material or related communications data obtained under the warrant may be selected for examination.

(4) In specifying any operational purposes, it is not sufficient simply to use the descriptions contained in section 107(1)(b) or (2), but the purposes may still be general purposes.

Duration, modification and cancellation of warrants

112 Duration of warrants

(1) A bulk interception warrant ceases to have effect at the end of the period of 6 months beginning with—

(a) the day on which the warrant was issued, or

(b) in the case of a warrant that has been renewed, the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed.

(2) For provision about the renewal of warrants, see section 113.

113 Renewal of warrants

(1) If the renewal conditions are met, a bulk interception warrant may be renewed, at any time before it would otherwise cease to have effect, by an instrument issued by the Secretary of State.

(2) The renewal conditions are—

(a) that the Secretary of State considers that the warrant continues to be necessary—

(i) in the interests of national security, or

(ii) on that ground and on any other grounds falling within section 107(2),

(b) that the Secretary of State considers that the conduct that would be authorised by the renewed warrant continues to be proportionate to what is sought to be achieved by that conduct,

(c) that the Secretary of State considers that—

(i) the examination of intercepted material or related communications data obtained under the warrant continues to be necessary for one or more of the specified operational purposes, and

(ii) any examination of that material or data for those purposes continues to be necessary as mentioned in paragraph (a), and

(d) that the decision to renew the warrant has been approved by a Judicial Commissioner.

(3) The decision to renew a bulk interception warrant must be taken personally by the Secretary of State, and the instrument renewing the warrant must be signed by the Secretary of State.

(4) Section 109 (approval of warrants by Judicial Commissioners) applies in relation to a decision to renew a bulk interception warrant as it applies in relation to a decision to issue a bulk interception warrant.

(5) In this section "the specified operational purposes" has the same meaning as in section 107.

114 Modification of warrants

(1) The provisions of a bulk interception warrant may be modified at any time by an instrument issued by the person making the modification.

(2) The only modifications that may be made under this section are adding, varying or removing any operational purpose specified in the warrant as a purpose for which any intercepted material or related communications data obtained under the warrant may be selected for examination.

(3) The decision to modify the provisions of a warrant must be taken personally by the person making the modification, and the instrument making the modification must be signed by that person.

(4) A modification adding or varying any operational purpose as mentioned in subsection (2)—

(a) must be made by the Secretary of State, and

(b) has effect only if the decision to make the modification is approved by a Judicial Commissioner.

(5) Section 109 (approval of warrants by Judicial Commissioners) applies in relation to a decision to modify a bulk interception warrant as mentioned in subsection (4) as it applies in relation to the decision to issue a bulk interception warrant.

(6) A modification removing any operational purpose may be made by—

(a) the Secretary of State, or

(b) a senior official acting on behalf of the Secretary of State.

(7) The Secretary of State may make a modification of a bulk interception warrant adding or varying any operational purpose as mentioned in subsection (2) only if the Secretary of State considers that the modification is necessary—

(a) in the interests of national security, or
(b) on that ground and on any other grounds falling within section 107(2).

(8) Where a modification of a bulk interception warrant is made by a senior official, the Secretary of State must be notified personally of the modification and the reasons for making it.

(9) Nothing in this section applies in relation to modifying the provisions of a warrant in a way which does not affect the conduct authorised or required by it.

115 Cancellation of warrants

(1) The Secretary of State, or a senior official acting on behalf of the Secretary of State, may cancel a bulk interception warrant at any time.

(2) If the Secretary of State, or a senior official acting on behalf of the Secretary of State, considers—
(a) that a bulk interception warrant is no longer necessary in the interests of national security, or
(b) that the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved by that conduct,
the person must cancel the warrant.

Implementation of warrants

116 Implementation of warrants

(1) In giving effect to a bulk interception warrant, the person to whom it is addressed ("the implementing authority") may (in addition to acting alone) act through, or together with, such other persons as the implementing authority may require (whether under subsection (2) or otherwise) to provide the authority with assistance in giving effect to the warrant.

(2) For the purpose of requiring any person to provide assistance in relation to a bulk interception warrant, the implementing authority may—
(a) serve a copy of the warrant on any person who the implementing authority considers may be able to provide such assistance, or
(b) make arrangements for the service of a copy of the warrant on any such person.

(3) A copy of a warrant may be served under subsection (2) on a person outside the United Kingdom for the purpose of requiring the person to provide such assistance in the form of conduct outside the United Kingdom.

(4) For the purposes of this Act, the provision of assistance in giving effect to a bulk interception warrant includes any disclosure to the implementing authority, or to persons acting on behalf of the implementing authority, of intercepted material or related communications data obtained under the warrant.

(5) Sections 30 (service of warrants) and 31 (duty of operators to assist with implementation) apply in relation to a bulk interception warrant as they apply in relation to a targeted interception warrant.

(6) References in this section (and in sections 30 and 31 as they apply in relation to bulk interception warrants) to the service of a copy of a warrant include—

(a) the service of a copy of one or more schedules contained in the warrant with the omission of the remainder of the warrant, and

(b) the service of a copy of the warrant with the omission of any schedule contained in the warrant.

Restrictions on use of intercepted material etc.

117 General safeguards

(1) The Secretary of State must ensure, in relation to every bulk interception warrant, that arrangements are in force for securing—

(a) that the requirements of subsections (2) and (5) are met in relation to the intercepted material and related communications data obtained under the warrant, and

(b) that the requirements of section 119 are met in relation to that material and data.

This is subject to subsection (8).

(2) The requirements of this subsection are met in relation to the intercepted material and related communications data obtained under a warrant if each of the following is limited to the minimum that is necessary for the authorised purposes (see subsection (3))—

(a) the number of persons to whom any of the material or data is disclosed or otherwise made available;

(b) the extent to which any of the material or data is disclosed or otherwise made available;

(c) the extent to which any of the material or data is copied;

(d) the number of copies that are made.

(3) For the purposes of subsection (2) something is necessary for the authorised purposes if, and only if—

(a) it is, or is likely to become, necessary in the interests of national security or on any other grounds falling within section 107(2),

(b) it is necessary for facilitating the carrying out of any functions under this Act of the Secretary of State, the Scottish Ministers or the head of the intelligence service to whom the warrant is addressed,

(c) it is necessary for facilitating the carrying out of any functions of the Judicial Commissioners or the Investigatory Powers Tribunal under or in relation to this Act,

(d) it is necessary to ensure that a person ("P") who is conducting a criminal prosecution has the information P needs to determine what is required of P by P's duty to secure the fairness of the prosecution, or

(e) it is necessary for the performance of any duty imposed on any person by the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923.

(4) The arrangements for the time being in force under this section for securing that the requirements of subsection (2) are met in relation to the intercepted material and related communications data obtained under the warrant must include arrangements for securing that every copy made of any of that material or data is stored, for so long as it is retained, in a secure manner.

(5) The requirements of this subsection are met in relation to the intercepted material and related communications data obtained under a warrant if every copy made of any of that material or data (if not destroyed earlier) is destroyed as soon there are no longer any relevant grounds for retaining it (see subsection (6)).

(6) For the purposes of subsection (5), there are no longer any relevant grounds for retaining a copy of any material or data if, and only if—

(a) its retention is not necessary, or not likely to become necessary, in the interests of national security or on any other grounds falling within section 107(2), and

(b) its retention is not necessary for any of the purposes mentioned in paragraphs (b) to (e) of subsection (3) above.

(7) Subsection (8) applies if—

(a) any intercepted material or related communications data obtained under the warrant has been handed over to any overseas authorities, or

(b) a copy of any such material or data has been given to any overseas authorities.

(8) To the extent that the requirements of subsections (2) and (5) relate to any of the material or data mentioned in subsection (7)(a), or to the copy mentioned in subsection (7)(b), the arrangements made for the purposes of this section are not required to secure that those requirements are met (see instead section 118).

(9) In this section—

"copy", in relation to intercepted material or related communications data obtained under a bulk interception warrant, means any of the following (whether or not in documentary form)—

(a) any copy, extract or summary of the material or data which identifies itself as having been obtained under the warrant, and

(b) any record referring to any interception or to the obtaining of any related communications data which is a record of the identities of the persons to or by whom the material was sent, or to whom the data relates,

and "copied" is to be read accordingly;

"overseas authorities" means authorities of a country or territory outside the United Kingdom.

118 Safeguards relating to disclosure of material or data overseas

(1) The Secretary of State must ensure, in relation to every bulk interception warrant, that arrangements are in force for securing that—

(a) any of the intercepted material or related communications data obtained under the warrant is handed over to overseas authorities only if the requirements of subsection (2) are met, and

(b) copies of any of that material or data are given to overseas authorities only if those requirements are met.

(2) The requirements of this subsection are met in the case of a warrant if it appears to the Secretary of State—

(a) that requirements corresponding to the requirements of section 117(2) and (5) ("the relevant requirements") will apply, to such extent (if any) as the Secretary of State considers appropriate, in relation to any of the

intercepted material or related communications data which is handed over, or any copy of which is given, to the authorities in question, and

(b) that restrictions are in force which would prevent, to such extent (if any) as the Secretary of State considers appropriate, the doing of anything in, for the purposes of or in connection with any proceedings outside the United Kingdom which would result in an unauthorised disclosure.

(3) In subsection (2)(b) "unauthorised disclosure" means a disclosure which, by virtue of section 42, could not be made in the United Kingdom.

(4) In this section—

"copy" has the same meaning as in section 117;

"overseas authorities" means authorities of a country or territory outside the United Kingdom.

119 Safeguards relating to examination of material or data

(1) For the purposes of section 117 the requirements of this section are met in relation to the intercepted material and related communications data obtained under a warrant if—

(a) any examination of the intercepted material or related communications data is carried out only for the specified purposes (see subsection (2)),

(b) the selection of any of the intercepted material or related communications data for examination is necessary and proportionate in all the circumstances, and

(c) the selection of any of the intercepted material for examination meets any of the selection conditions (see subsection (3)).

(2) Examination of intercepted material or related communications data is carried out only for the specified purposes if the material or data is examined only so far as is necessary for the operational purposes specified in the warrant in accordance with section 111.

In this subsection "specified in the warrant" means specified in the warrant at the time of the selection of the material or data for examination.

(3) The selection conditions referred to in subsection (1)(c) are—

(a) that the selection of the intercepted material for examination does not breach the prohibition in subsection (4);

(b) that the person to whom the warrant is addressed considers that the selection of the intercepted material for examination would not breach that prohibition;

(c) that the selection of the intercepted material for examination in breach of that prohibition is authorised by subsection (5);

(d) that a targeted examination warrant has been issued under Chapter 1 of Part 2 authorising the examination of the intercepted material.

(4) The prohibition referred to in subsection (3)(a) is that intercepted material may not at any time be selected for examination if—

(a) any criteria used for the selection of the material for examination are referable to an individual known to be in the British Islands at that time, and

(b) the purpose of using those criteria is to identify the content of communications sent by, or intended for, that individual.

It does not matter for the purposes of this subsection whether the identity of the individual is known.

(5) The selection of intercepted material ("the relevant material") for examination is authorised by this subsection if—

(a) criteria referable to an individual have been, or are being, used for the selection of material for examination in circumstances falling within subsection (3)(a) or (b),

(b) at any time it appears to the person to whom the warrant is addressed that there has been a relevant change of circumstances in relation to the individual (see subsection (6)) which would mean that the selection of the relevant material for examination would breach the prohibition in subsection (4),

(c) since that time, a written authorisation to examine the relevant material using those criteria has been given by a senior official, and

(d) the selection of the relevant material for examination is made before the end of the permitted period (see subsection (7)).

(6) For the purposes of subsection (5)(b) there is a relevant change of circumstances in relation to an individual if—

(a) the individual has entered the British Islands, or

(b) a belief by the person to whom the warrant is addressed that the individual was outside the British Islands was in fact mistaken.

(7) In subsection (5) "the permitted period" means the period ending with the fifth working day after the time mentioned in subsection (5)(b).

120 Application of other restrictions in relation to warrants

(1) Section 42 and Schedule 3 (exclusion of matters from legal proceedings) apply in relation to bulk interception warrants as they apply in relation to targeted interception warrants.

(2) Sections 43 and 44 (duty not to make unauthorised disclosures) apply in relation to bulk interception warrants as they apply in relation to targeted interception warrants, but as if the reference in section 43(5)(d) to a disclosure authorised by section 29(5) included a reference to a disclosure authorised by section 116(4).

Interpretation

121 Chapter 1: interpretation

(1) In this Chapter—

"intercepted material", in relation to a bulk interception warrant, means the content of any communications intercepted by an interception authorised or required by the warrant;

"interception" is to be read in accordance with section 3;

"related communications data" has the meaning given by section 106(6);

"senior official" means a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service.

(2) References in this Chapter to the examination of intercepted material are references to the material being read, looked at or listened to by the persons to whom it becomes available as a result of the warrant.

CHAPTER 2

BULK ACQUISITION WARRANTS

Bulk acquisition warrants

122 Power to issue bulk acquisition warrants

(1) The Secretary of State may, on an application made by or on behalf of the head of an intelligence service, issue a bulk acquisition warrant if—

(a) the Secretary of State considers that the warrant is necessary—

(i) in the interests of national security, or

(ii) on that ground and on any other grounds falling within subsection (2),

(b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(c) the Secretary of State considers that—

(i) the examination of communications data obtained under the warrant is necessary for one or more of the specified operational purposes (see subsection (9)), and

(ii) any examination of that data for those purposes is necessary as mentioned in paragraph (a),

(d) the Secretary of State considers that satisfactory arrangements made for the purposes of section 131 (general safeguards) are in force in relation to the warrant, and

(e) the decision to issue the warrant has been approved by a Judicial Commissioner.

(2) A warrant is necessary on grounds falling within this subsection if it is necessary—

(a) for the purpose of preventing or detecting serious crime, or

(b) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security.

(3) A warrant may be considered necessary on the ground falling within subsection (2)(b) only if the communications data which it is considered necessary to obtain is communications data relating to the acts or intentions of persons outside the British Islands.

(4) The matters to be taken into account in considering whether the conditions in paragraphs (a) and (b) of subsection (1) are met include whether the communications data which it is thought necessary to obtain under the warrant could reasonably be obtained by other means.

(5) A bulk acquisition warrant is a warrant which authorises or requires the person to whom it is addressed to secure, by any conduct described in the warrant, any one or more of the activities in subsection (6).

(6) The activities are—

(a) requiring a telecommunications operator specified in the warrant—

(i) to disclose to a person specified in the warrant any communications data which is specified in the warrant and is in the possession of the operator,

(ii) to obtain any communications data specified in the warrant which is not in the possession of the operator but which the operator is capable of obtaining, and

(iii) to disclose to a person specified in the warrant any data obtained as mentioned in sub-paragraph (ii),

(b) the selection for examination, in any manner specified in the warrant, of communications data obtained under the warrant,

(c) the disclosure, in any manner specified in the warrant, of such data to the person to whom the warrant is addressed or to any person acting on that person's behalf.

(7) A bulk acquisition warrant also authorises the following conduct (in addition to the conduct specified in the warrant)—

(a) any conduct which it is necessary to undertake in order to do what is expressly authorised or required by the warrant, and

(b) conduct by any person which is conduct in pursuance of a requirement imposed by or on behalf of the person to whom the warrant is addressed to be provided with assistance in giving effect to the warrant.

(8) A bulk acquisition warrant may relate to data whether or not in existence at the time of the issuing of the warrant.

(9) An application for the issue of a bulk acquisition warrant may only be made on behalf of the head of an intelligence service by a person holding office under the Crown.

(10) In this section—

"specified operational purposes" means the operational purposes specified in the warrant in accordance with section 125,

and for the meaning of "head of an intelligence service" see section 195.

123 Approval of warrants by Judicial Commissioners

(1) In deciding whether to approve a decision to issue a warrant under section 122, a Judicial Commissioner must review the Secretary of State's conclusions as to the following matters—

(a) whether the warrant is necessary as mentioned in subsection (1)(a) of that section,

(b) whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct, and

(c) whether—

(i) the examination of communications data obtained under the warrant is necessary for one or more of the specified operational purposes, and

(ii) any examination of that data for those purposes is necessary as mentioned in subsection (1)(a) of that section.

(2) In doing so, the Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review.

(3) Where a Judicial Commissioner refuses to approve a decision to issue a warrant under section 122, the Judicial Commissioner must give the Secretary of State written reasons for the refusal.

(4) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to issue a warrant under section 122, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant.

(5) In this section "specified operational purposes" has the same meaning as in section 122.

124 Decisions to issue warrants to be taken personally by Secretary of State

(1) The decision to issue a bulk acquisition warrant must be taken personally by the Secretary of State.

(2) Before a bulk acquisition warrant is issued, it must be signed by the Secretary of State.

125 Requirements that must be met by warrants

(1) A bulk acquisition warrant must contain a provision stating that it is a bulk acquisition warrant.

(2) A bulk acquisition warrant must be addressed to the head of the intelligence service by whom, or on whose behalf, the application for the warrant was made.

(3) A bulk acquisition warrant must specify the operational purposes for which any communications data obtained under the warrant may be selected for examination.

(4) In specifying any operational purposes, it is not sufficient simply to use the descriptions contained in section 122(1)(a) or (2), but the purposes may still be general purposes.

Duration, modification and cancellation of warrants

126 Duration of warrants

(1) A bulk acquisition warrant ceases to have effect at the end of the period of 6 months beginning with—

(a) the day on which the warrant was issued, or

(b) in the case of a warrant that has been renewed, the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed.

(2) For provision about the renewal of warrants, see section 127.

127 Renewal of warrants

(1) If the renewal conditions are met, a bulk acquisition warrant may be renewed, at any time before it would otherwise cease to have effect, by an instrument issued by the Secretary of State.

(2) The renewal conditions are—

(a) that the Secretary of State considers that the warrant continues to be necessary—

(i) in the interests of national security, or

(ii) on that ground and on any other grounds falling within section 122(2),

(b) that the Secretary of State considers that the conduct that would be authorised by the renewed warrant continues to be proportionate to what is sought to be achieved by that conduct,

(c) that the Secretary of State considers that—

(i) the examination of communications data obtained under the warrant continues to be necessary for one or more of the specified operational purposes, and

(ii) any examination of that data for those purposes continues to be necessary as mentioned in paragraph (a), and

(d) that the decision to renew the warrant has been approved by a Judicial Commissioner.

(3) The decision to renew a bulk acquisition warrant must be taken personally by the Secretary of State and the instrument renewing the warrant must be signed by the Secretary of State.

(4) Section 123 (approval of warrants by Judicial Commissioners) applies in relation to a decision to renew a bulk acquisition warrant as it applies in relation to a decision to issue a bulk acquisition warrant.

(5) In this section "specified operational purposes" has the same meaning as in section 122.

128 Modification of warrants

(1) The provisions of a bulk acquisition warrant may be modified at any time by an instrument issued by the person making the modification.

(2) The only modifications that may be made under this section are adding, varying or removing any operational purpose specified in the warrant as a purpose for which any communications data obtained under the warrant may be selected for examination.

(3) The decision to modify the provisions of a warrant must be taken personally by the person making the modification, and the instrument making the modification must be signed by that person.

(4) A modification adding or varying any operational purpose as mentioned in subsection (2)—

(a) must be made by the Secretary of State, and

(b) has effect only if the decision to make the modification is approved by a Judicial Commissioner.

(5) Section 123 (approval of warrants by Judicial Commissioners) applies in relation to a decision to modify a bulk acquisition warrant as mentioned in subsection (4) as it applies in relation to the decision to issue a bulk acquisition warrant.

(6) A modification removing any operational purpose may be made by—
  (a) the Secretary of State, or
  (b) a senior official acting on behalf of the Secretary of State.

(7) The Secretary of State may make a modification of a bulk acquisition warrant adding or varying any operational purpose as mentioned in subsection (2) only if the Secretary of State considers that the modification is necessary—
  (a) in the interests of national security, or
  (b) on that ground and on any other grounds falling within section 122(2).

(8) Where a modification of a bulk acquisition warrant is made by a senior official, the Secretary of State must be notified personally of the modification and the reasons for making it.

(9) Nothing in this section applies in relation to modifying the provisions of a warrant in a way which does not affect the conduct authorised or required by it.

129 Cancellation of warrants

(1) The Secretary of State, or a senior official acting on behalf of the Secretary of State, may cancel a bulk acquisition warrant at any time.

(2) If the Secretary of State, or a senior official acting on behalf of the Secretary of State, considers—
  (a) that a bulk acquisition warrant is no longer necessary in the interests of national security, or
  (b) that the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved by that conduct,

the person must cancel the warrant.

Implementation of warrants

130 Implementation of warrants

(1) In giving effect to a bulk acquisition warrant, the person to whom it is addressed ("the implementing authority") may (in addition to acting alone) act through, or together with, such other persons as the implementing authority may require (whether under subsection (2) or otherwise) to provide the authority with assistance in giving effect to the warrant.

(2) For the purpose of requiring any person to provide assistance in relation to a bulk acquisition warrant, the implementing authority may—
  (a) serve a copy of the warrant on any person whom the implementing authority considers may be able to provide such assistance, or
  (b) make arrangements for the service of a copy of the warrant on any such person.

(3) A copy of a warrant may be served under subsection (2) on a person outside the United Kingdom for the purpose of requiring the person to provide such assistance in the form of conduct outside the United Kingdom.

(4) For the purposes of this Act, the provision of assistance in giving effect to a bulk acquisition warrant includes any disclosure to the implementing authority, or to persons acting on behalf of the implementing authority, of communications data obtained under the warrant.

(5) Sections 30 (service of warrants) and 31(1) to (6) (duty of operators to assist with implementation) apply in relation to a bulk acquisition warrant as they apply in relation to a targeted interception warrant but as if only a telecommunications operator were a relevant operator for the purposes of section 31(1) to (6).

(6) The duty imposed by virtue of subsection (5) above and section 31(1) is enforceable against a person in the United Kingdom by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.

(7) References in this section (and in sections 30 and 31(1) to (6) as they apply in relation to bulk acquisition warrants) to the service of a copy of a warrant include—

(a) the service of a copy of one or more schedules contained in the warrant with the omission of the remainder of the warrant, and

(b) the service of a copy of the warrant with the omission of any schedule contained in the warrant.

Restrictions on use of data obtained etc.

131 General safeguards

(1) The Secretary of State must ensure, in relation to every bulk acquisition warrant, that arrangements are in force for securing—

(a) that the requirements of subsections (2) and (5) are met in relation to the communications data obtained under the warrant, and

(b) that the requirements of section 132 are met in relation to that data.

This is subject to subsection (8).

(2) The requirements of this subsection are met in relation to the communications data obtained under a warrant if each of the following is limited to the minimum that is necessary for the authorised purposes (see subsection (3))—

(a) the number of persons to whom any of the data is disclosed or otherwise made available,

(b) the extent to which any of the data is disclosed or otherwise made available,

(c) the extent to which any of the data is copied,

(d) the number of copies that are made.

(3) For the purposes of subsection (2) something is necessary for the authorised purposes if, and only if—

(a) it is, or is likely to become, necessary in the interests of national security or on any other grounds falling within section 122(2),

(b) it is necessary for facilitating the carrying out of any functions under this Act of the Secretary of State, the Scottish Ministers or the head of the intelligence service to whom the warrant is addressed,

(c) it is necessary for facilitating the carrying out of any functions of the Judicial Commissioners or the Investigatory Powers Tribunal under or in relation to this Act,

(d) it is necessary to ensure that a person ("P") who is conducting a criminal prosecution has the information P needs to determine what is required of P by P's duty to secure the fairness of the prosecution,

(e) it is necessary for use as evidence in legal proceedings, or

(f) it is necessary for the performance of any duty imposed on any person by the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923.

(4) The arrangements for the time being in force under this section for securing that the requirements of subsection (2) are met in relation to the communications data obtained under the warrant must include arrangements for securing that every copy made of any of that data is stored, for so long as it is retained, in a secure manner.

(5) The requirements of this subsection are met in relation to the communications data obtained under the warrant if every copy made of any of that data (if not destroyed earlier) is destroyed as soon there are no longer any relevant grounds for retaining it (see subsection (6)).

(6) For the purposes of subsection (5), there are no longer any relevant grounds for retaining a copy of any data if, and only if—

(a) its retention is not necessary, or not likely to become necessary, in the interests of national security or on any other grounds falling within section 122(2), and

(b) its retention is not necessary for any of the purposes mentioned in paragraphs (b) to (f) of subsection (3) above.

(7) Subsection (8) applies if—

(a) any communications data obtained under the warrant has been handed over to any overseas authorities, or

(b) a copy of any such data has been given to any overseas authorities.

(8) To the extent that the requirements of subsections (2) and (5) relate to any of the data mentioned in subsection (7)(a), or to the copy mentioned in subsection (7)(b), the arrangements made for the purposes of this section are not required to secure that those requirements are met.

(9) But the person to whom the warrant is addressed must ensure that arrangements are in force for securing that communications data obtained under the warrant, or any copy of the data, is handed over or given to an overseas authority only if that person considers that arrangements corresponding to those mentioned in this section will apply, to such extent (if any) as that person considers appropriate, in relation to the data or copy.

(10) In this section—

"copy", in relation to communications data obtained under a bulk acquisition warrant, means any of the following (whether or not in documentary form)—

(a) any copy, extract or summary of the data which identifies itself as having been obtained under the warrant, and

(b) any record referring to the obtaining of the data which is a record of the identities of the persons to whom the data relates,

and "copied" is to be read accordingly,

"overseas authorities" means authorities of a country or territory outside the United Kingdom.

132 Safeguards relating to examination of data

(1) For the purposes of section 131 the requirements of this section are met in relation to the communications data obtained under a warrant if—

(a) any examination of the data is carried out only for the specified purposes (see subsection (2)), and

(b) the selection of any of the data for examination is necessary and proportionate in all the circumstances.

(2) Examination of communications data is carried out only for the specified purposes if the data is examined only so far as is necessary for the operational purposes specified in the warrant in accordance with section 125.

(3) In subsection (2) "specified in the warrant" means specified in the warrant at the time of the selection of the data for examination.

Supplementary provision

133 Offence of making unauthorised disclosure

(1) It is an offence for—

(a) a telecommunications operator who is under a duty by virtue of section 130 to assist in giving effect to a bulk acquisition warrant, or

(b) any person employed for the purposes of the business of such an operator,

to disclose to any person, without reasonable excuse, the existence or contents of the warrant.

(2) For the purposes of subsection (1), it is, in particular, a reasonable excuse if the disclosure is made with the permission of the Secretary of State.

(3) A person guilty of an offence under this section is liable—

(a) on summary conviction in England and Wales—

(i) to imprisonment for a term not exceeding 12 months (or 6 months, if the offence was committed before the commencement of section 154(1) of the Criminal Justice Act 2003), or

(ii) to a fine,

or both;

(b) on summary conviction in Scotland—

(i) to imprisonment for a term not exceeding 12 months, or

(ii) to a fine not exceeding the statutory maximum,

or both;

(c) on summary conviction in Northern Ireland—

(i) to imprisonment for a term not exceeding 6 months, or

(ii) to a fine not exceeding the statutory maximum,

or both;

(d) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine, or both.

134 Chapter 2: interpretation

In this Chapter—

"communications data" does not include communications data within the meaning given by section 194(3),

"senior official" means—

(a) a member of the Senior Civil Service, or

(b) a member of the Senior Management Structure of Her Majesty's Diplomatic Service.

CHAPTER 3

BULK EQUIPMENT INTERFERENCE WARRANTS

Bulk equipment interference warrants

135 Bulk equipment interference warrants: general

(1) For the purposes of this Act, a warrant is "bulk equipment interference warrant" if—

(a) it is issued under this Chapter,

(b) it authorises the person to whom it is addressed to secure interference with any equipment for the purpose of facilitating the obtaining of one or more of the following—

(i) communications (see section 149);

(ii) private information (see section 149);

(iii) equipment data (see section 136); and

(c) the main purpose of the warrant is facilitating the obtaining of one or more of the following—

(i) overseas-related communications;

(ii) overseas-related private information;

(iii) overseas-related equipment data.

(2) In this Chapter —

"overseas-related communications" means—

(a) communications sent by individuals who are outside the British Islands, or

(b) communications received by individuals who are outside the British Islands;

"overseas-related private information" means private information of individuals who are outside the British Islands;

"overseas-related equipment data" means equipment data that forms part of, or is connected with, overseas-related communications or overseas-related private information.

(3) A bulk equipment interference warrant may also authorise the person to whom it is addressed to secure—

(a) the obtaining of any communications, private information or equipment data to which the purpose of the warrant relates;

(b) the obtaining of any information that does not fall within paragraph (a) but is connected with the equipment to which the warrant relates;

(c) the selection for examination, in any manner described in the warrant, of any material obtained under the warrant by virtue of paragraph (a) or (b);

(d) the disclosure, in any manner described in the warrant, of any such material to the person to whom the warrant is addressed or to any person acting on that person's behalf.

(4) A bulk equipment interference warrant also authorises the following conduct (in addition to the conduct described in the warrant)—

(a) any conduct which it is necessary to undertake in order to do what is expressly authorised by the warrant, including conduct for securing the obtaining of—

(i) communications;

(ii) private information;

(iii) equipment data;

(iv) information that does not fall within sub-paragraphs (i) to (iii) but is connected with the equipment to which the warrant relates; and

(b) any conduct by any person which is conduct in pursuance of a requirement imposed by or on behalf of the person to whom the warrant is addressed to be provided with assistance in giving effect to the warrant.

(5) A bulk equipment interference warrant may not, by virtue of subsection (3)(a), authorise a person to engage in conduct, in relation to a communication other than a stored communication, that would (unless done with lawful authority) constitute an offence under section 2(1) (unlawful interception).

(6) Subsection (4)(a) does not authorise a person to engage in conduct that could not be expressly authorised under the warrant because of the restriction imposed by subsection (5).

(7) In subsection (5), "stored communication" means a communication stored in or by a telecommunication system.

136 Meaning of "equipment data"

(1) In this Chapter, "equipment data" means—

(a) communications data (see section 193(5));

(b) data that falls within subsection (2) or (4).

(2) Data falls within this subsection if it identifies or describes anything connected with enabling or otherwise facilitating the functioning of a relevant system (including any apparatus in it) or of any service provided by means of the system.

(3) For the purposes of subsection (2), a system is a relevant system if any communications or private information are held on or by means of the system.

(4) Data falls within this subsection if, for the purposes of a relevant system, it is comprised in, included as part of, attached to or logically associated with a communication or an item of private information and either—

(a) it does not form part of the content of the communication or the item of private information (see subsection (8)), or

(b) if it does, it is capable of being logically separated from the remainder of the content in such a way that (after being separated)—

(i) it would not reveal anything of what might reasonably be expected to be the meaning of the communication or item of information, disregarding any meaning arising from the fact of the communication or the existence of the item of information or from any data relating to that fact, and

(ii) it would be data falling within subsection (5).

(5) The data falling within this subsection is—

(a) data which may be used to identify, or assist in identifying, any person, apparatus, system or service;

(b) data which may be used to identify any event;

(c) data which may be used to identify the location of any person, event or thing.

(6) For the purposes of subsection (5), the reference to data that may be used to identify any event includes—

(a) data relating to the fact of the event;

(b) data relating to the type, method or pattern of event;

(c) data relating to the time or duration of the event.

(7) In subsection (4), "relevant system" means any system on or by means of which the data is held.

(8) For the purposes of this section, the content of a communication or an item of private information is the elements of the communication or item, and any data attached to or logically associated with it, which reveal anything of what might reasonably be expected to be the meaning of the communication or item, disregarding any meaning arising from the fact of the communication or the existence of the item or from any data relating to that fact.

137 Power to issue bulk warrants

(1) The Secretary of State may, on an application made by or on behalf of the head of an intelligence service, issue a bulk equipment interference warrant if—

(a) the Secretary of State considers that the main purpose of the warrant is to facilitate the obtaining of overseas-related communications, overseas-related private information or overseas-related equipment data;

(b) the Secretary of State considers that the warrant is necessary—

(i) in the interests of national security, or

(ii) on that ground and on any other grounds falling within subsection (2),

(c) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct,

(d) where the warrant includes provision by virtue of section 135(3), the Secretary of State considers that—

(i) the examination of any material obtained under the warrant is necessary for one or more of the specified operational purposes, and

(ii) any examination of that material for those purposes is necessary as mentioned in paragraph (b),

(e) where the warrant includes provision by virtue of section 135(3), the Secretary of State considers that satisfactory arrangements made for the purposes of section 146 (general safeguards) are in force in relation to the warrant, and

(f) the decision to issue the warrant has been approved by a Judicial Commissioner.

For the meaning of "head of an intelligence service", see section 195.

(2) A warrant is necessary on grounds falling within this subsection if it is necessary—

(a) for the purpose of preventing or detecting serious crime, or

(b) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security.

(3) A warrant may be considered necessary on the ground falling within subsection (2)(b) only if the interference with equipment that would be authorised by the warrant is considered necessary to facilitate the obtaining of material relating to the acts or intentions of persons outside the British Islands.

(4) The matters to be taken into account in considering whether the conditions in paragraphs (a) and (b) of subsection (1) are met include whether what could be achieved under the warrant could reasonably be achieved by other means.

(5) In subsection 1(d)(i), "specified operational purposes" means the operational purposes specified in the warrant in accordance with section 140(4).

(6) An application for the issue of a bulk equipment interference warrant may only be made on behalf of the head of an intelligence service by a person holding office under the Crown.

138 Approval of warrants by Judicial Commissioners

(1) In deciding whether to approve a decision to issue a warrant under section 137, a Judicial Commissioner must review the Secretary of State's conclusions on the following matters—

(a) whether the warrant is necessary as mentioned in subsection (1)(b) of that section,

(b) whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct, and

(c) where the warrant includes provision by virtue of section 135(3), whether—

(i) the examination of any material obtained under the warrant is necessary for one or more of the specified operational purposes, and

(ii) any examination of that material for those purposes is necessary as mentioned in subsection (1)(b) of section 137.

(2) In doing so, the Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review.

(3) Where a Judicial Commissioner refuses to approve a decision to issue a warrant under section 137, the Judicial Commissioner must give the Secretary of State written reasons for the refusal.

(4) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to issue a warrant, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant.

(5) In this section, "specified operational purposes" has the same meaning as in section 137(5).

139 Decisions to issue warrants to be taken personally by Secretary of State

(1) The decision to issue a bulk equipment interference warrant must be taken personally by the Secretary of State.

(2) Before a bulk equipment interference warrant is issued, it must be signed by the Secretary of State.

140 Requirements that must be met by warrants

(1) A bulk equipment interference warrant must contain a provision stating that it is a bulk equipment interference warrant.

(2) A bulk equipment interference warrant must be addressed to the head of the intelligence service by whom, or on whose behalf, the application for the warrant was made.

(3) A bulk equipment interference warrant must describe the conduct that is authorised by the warrant.

(4) A bulk equipment interference warrant must specify the operational purposes for which any material obtained under the warrant may be selected for examination.

(5) In specifying any operational purposes, it is not sufficient simply to use the descriptions contained in section 137(1)(b) or (2), but the purposes may still be general purposes.

Duration, modification and cancellation of warrants

141 Duration of warrants

(1) A bulk equipment interference warrant ceases to have effect at the end of the period of 6 months beginning with—

(a) the day on which the warrant was issued, or

(b) in the case of a warrant that has been renewed, the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed.

(2) For provision about the renewal of warrants, see section 142.

142 Renewal of warrants

(1) If the renewal conditions are met, a bulk equipment interference warrant may be renewed, at any time before it would otherwise cease to have effect, by an instrument issued by the Secretary of State.

(2) The renewal conditions are—

(a) that the Secretary of State considers that the warrant continues to be necessary—

(i) in the interests of national security, or

(ii) on that ground and on any other grounds falling within section 137(2),

(b) that the Secretary of State considers that the conduct that would be authorised by the renewed warrant continues to be proportionate to what is sought to be achieved by that conduct,

(c) where the warrant includes provision by virtue of section 135(3), that the Secretary of State considers that—

(i) the examination of any material obtained under the warrant continues to be necessary for one or more of the specified operational purposes, and

(ii) any examination of that material for those purposes continues to be necessary as mentioned in paragraph (a), and

(d) that the decision to renew the warrant has been approved by a Judicial Commissioner.

(3) The decision to renew a bulk equipment interference warrant must be taken personally by the Secretary of State, and the instrument renewing the warrant must be signed by the Secretary of State.

(4) Section 138 (approval of warrants by Judicial Commissioners) applies in relation to a decision to renew a bulk equipment interference warrant as it applies in relation to a decision to issue a bulk equipment interference warrant.

(5) In this section, "the specified operational purposes" has the same meaning as in section 137(5).

143 Modification of warrants

(1) The provisions of a bulk equipment interference warrant may be modified at any time by an instrument issued by the person making the modification.

(2) The only modifications that may be made under this section are adding, varying or removing any operational purpose specified in the warrant as a purpose for which any material obtained under the warrant may be selected for examination.

(3) The decision to modify the provisions of a warrant must be taken personally by the person making the modification, and the instrument making the modification must be signed by that person.

(4) A modification adding or varying any operational purpose as mentioned in subsection (2)—

(a) must be made by the Secretary of State, and

(b) has effect only if the decision to make the modification is approved by a Judicial Commissioner.

(5) Section 138 (approval of warrants by Judicial Commissioners) applies in relation to a decision to modify a bulk equipment interference warrant as mentioned in subsection (4) as it applies in relation to the decision to issue a bulk equipment interference warrant.

(6) A modification removing any operational purpose may be made by—
(a) the Secretary of State, or
(b) a senior official acting on behalf of the Secretary of State.

(7) The Secretary of State may make a modification of a bulk equipment interference warrant adding or varying any operational purpose as mentioned in subsection (2) only if the Secretary of State considers that the modification is necessary—
(a) in the interests of national security, or
(b) on that ground and on any other grounds falling within section 137(2).

(8) Where a modification of a bulk equipment interference warrant is made by a senior official, the Secretary of State must be notified personally of the modification and the reasons for making it.

(9) Nothing in this section applies in relation to modifying the provisions of a warrant in a way which does not affect the conduct authorised by it.

144 Cancellation of warrants

(1) The Secretary of State, or a senior official acting on behalf of the Secretary of State, may cancel a bulk equipment interference warrant at any time.

(2) If the Secretary of State, or a senior official acting on behalf of the Secretary of State, considers—
(a) that a bulk equipment interference warrant is no longer necessary in the interests of national security, or
(b) that the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved by that conduct,
the person must cancel the warrant.

Implementation of warrants

145 Implementation of warrants

(1) In giving effect to a bulk equipment interference warrant, the person to whom it is addressed ("the implementing authority") may (in addition to acting alone) act through, or together with, such other persons as the implementing authority may require (whether under subsection (2) or otherwise) to provide the authority with assistance in giving effect to the warrant.

(2) For the purpose of requiring any person to provide assistance in relation to a bulk equipment interference warrant, the implementing authority may—
(a) serve a copy of the warrant on any person who the implementing authority considers may be able to provide such assistance, or
(b) make arrangements for the service of a copy of the warrant on any such person.

(3) A copy of a warrant may be served under subsection (2) on a person outside the United Kingdom for the purpose of requiring the person to provide such assistance in the form of conduct outside the United Kingdom.

(4) Sections 100 (service of warrants) and 101 (duty of telecommunications providers to assist with implementation) apply in relation to a bulk equipment interference warrant as they apply in relation to a targeted equipment interference warrant issued under section 84 by the Secretary of State.

(5) References in this section (and in sections 100 and 101 as they apply in relation to bulk equipment interference warrants) to the service of a copy of a warrant include—

(a) the service of a copy of one or more schedules contained in the warrant with the omission of the remainder of the warrant, and

(b) the service of a copy of the warrant with the omission of any schedule contained in the warrant.

Restrictions on use of material etc.

146 General safeguards

(1) This section applies in relation to every bulk equipment interference warrant that includes authorisation to secure the obtaining of communications, private information, equipment data or other information connected with the equipment to which the warrant relates.

(2) The Secretary of State must ensure that arrangements are in force for securing—

(a) that the requirements of subsections (3) and (6) are met in relation to the material obtained under the warrant, and

(b) that the requirements of section 147 are met in relation to that material.

This is subject to subsection (8).

(3) The requirements of this subsection are met in relation to the material obtained under the warrant if each of the following is limited to the minimum that is necessary for the authorised purposes (see subsection (4))—

(a) the number of persons to whom any of the material is disclosed or otherwise made available;

(b) the extent to which any of the material is disclosed or otherwise made available;

(c) the extent to which any of the material is copied;

(d) the number of copies that are made.

(4) For the purposes of subsection (3) something is necessary for the authorised purposes if, and only if—

(a) it is, or is likely to become, necessary in the interests of national security or on any other grounds falling within section 137(2),

(b) it is necessary for facilitating the carrying out of any functions under this Act of the Secretary of State, the Scottish Ministers or the head of the intelligence service to whom the warrant is addressed,

(c) it is necessary for facilitating the carrying out of any functions of the Investigatory Powers Commissioner or of the Investigatory Powers Tribunal under or in relation to this Act,

(d) it is necessary for the purpose of legal proceedings, or

(e) it is necessary for the performance of the functions of any person by or under any enactment.

(5) The arrangements for the time being in force under this section for securing that the requirements of subsection (3) are met in relation to the material obtained under the warrant must include arrangements for securing that every copy made of any of that material is stored, for so long as it is retained, in a secure manner.

(6) The requirements of this subsection are met in relation to the material obtained under the warrant if every copy made of any of that material (if not destroyed earlier) is destroyed as soon as there are no longer any relevant grounds for retaining it (see subsection (7)).

(7) For the purposes of subsection (6), there are no longer any relevant grounds for retaining a copy of any material if, and only if—

(a) its retention is not necessary, or not likely to become necessary, in the interests of national security or on any other grounds falling within section 137(2), and

(b) its retention is not necessary for any of the purposes mentioned in paragraphs (b) to (e) of subsection (4) above.

(8) Subsections (3) and (6) do not apply so far as possession of the material or any copy of it has been handed over to any authorities of a country or territory outside the United Kingdom.

(9) But the Secretary of State must ensure that arrangements are in force for securing that possession of the material or any copy of it is handed over to authorities of a country or territory outside the United Kingdom only if the intelligence service considers that arrangements corresponding to those mentioned in subsections (3) and (6) will apply, to such extent (if any) as the intelligence service considers appropriate, in relation to the material or copy.

(10) In this section "copy", in relation to material, means any of the following (whether or not in documentary form)—

(a) any copy, extract or summary of the material which identifies itself as the product of a bulk equipment interference warrant, and

(b) any record which is a record of the identities of persons who owned, used or were in possession of equipment interfered with under such a warrant,

and "copied" is to be read accordingly.

147 Safeguards relating to examination of material etc.

(1) For the purposes of section 146, the requirements of this section are met in relation to the material obtained under a warrant if—

(a) any examination of the material obtained under the warrant is carried out only for the specified purposes (see subsection (2)),

(b) the selection of any of the material for examination is necessary and proportionate in all the circumstances, and

(c) where any such material is protected material, the selection of the material for examination meets any of the selection conditions (see subsection (3)).

(2) Examination of the material is carried out only for the specified purposes if the material is examined only so far as is necessary for the operational purposes specified in the warrant in accordance with section 140(4).
In this subsection "specified" means specified at the time of the selection of the material for examination.

(3) The selection conditions referred to in subsection (1)(c) are—
(a) that the selection of the protected material for examination does not breach the prohibition in subsection (4);
(b) that the person to whom the warrant is addressed reasonably considers that the selection of the protected material for examination would not breach that prohibition;
(c) that the selection of the protected material for examination in breach of that prohibition is authorised by subsection (5);
(d) that a targeted examination warrant has been issued under Part 5 authorising the examination of the protected material.

(4) The prohibition referred to in subsection (3)(a) is that the protected material may not at any time be selected for examination if—
(a) any criteria used for the selection of the material for examination are referable to an individual known to be in the British Islands at that time, and
(b) the purpose of using those criteria is to identify the content of communications sent by, or intended for, that individual or the content of private information relating to that individual.
It does not matter for the purposes of this subsection whether the identity of the individual is known.

(5) The selection of protected material ("the relevant material") for examination is authorised by this subsection if—
(a) criteria referable to an individual have been, or are being, used for the selection of material for examination in circumstances falling within subsection (3)(a) or (b),
(b) at any time it appears to the person to whom the warrant is addressed that there has been a relevant change of circumstances in relation to the individual (see subsection (6)) which would mean that the selection of the relevant material for examination would breach the prohibition in subsection (4),
(c) since that time, a written authorisation to examine the relevant material using those criteria has been given by a senior official, and
(d) the selection of the relevant material for examination is made before the end of the permitted period (see subsection (7)).

(6) For the purposes of subsection (5)(b) there is a relevant change of circumstances in relation to an individual if—
(a) the individual has entered the British Islands, or
(b) a belief by the person to whom the warrant is addressed that the individual was outside the British Islands was in fact mistaken.

(7) In subsection (5), "the permitted period" means the period ending with the fifth working day after the time mentioned in subsection (5)(b).

(8) In this section, "protected material" means any material obtained under the warrant other than—
(a) equipment data, or

(b) information connected with the equipment to which the warrant relates but that is not a communication, private information or equipment data.

148 Application of other restrictions in relation to warrants under this Chapter

Section 102 (offence of making unauthorised disclosure) applies in relation to bulk equipment interference warrants as it applies in relation to targeted equipment interference warrants.

Interpretation

149 Chapter 3: interpretation

(1) In this Chapter—

"communication" includes—

(a) anything comprising speech, music, sounds, visual images or data of any description, and

(b) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus;

"equipment" means equipment producing electromagnetic, acoustic or other emissions or any device capable of being used in connection with such equipment;

"equipment data" has the meaning given by section 136;

"private information" includes information relating to a person's private or family life;

"senior official" means a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service.

(2) References in this Chapter to the content of a communication or an item of private information are to be read in accordance with section 136(8).

(3) References in this Chapter to the examination of material are references to the material being read, looked at or listened to by the persons to whom it becomes available as a result of the warrant.

PART 7

BULK PERSONAL DATASET WARRANTS

Bulk personal datasets: interpretation

150 Bulk personal datasets: interpretation

(1) For the purposes of this Part, an intelligence service obtains a bulk personal dataset if—

(a) it obtains a set of information that includes personal data relating to a number of individuals,

(b) the nature of the set is such that it is likely that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service in the exercise of its functions, and

(c) if (after any initial examination of the contents) the intelligence service were to decide to retain the set for the purpose of the exercise of its functions, the set would be held electronically for analysis in the exercise of those functions.

(2) For the purposes of this Part, an intelligence service retains a bulk personal dataset if—

(a) it obtains a set of information that includes personal data relating to a number of individuals,

(b) the nature of the set is such that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service in the exercise of its functions,

(c) after any initial examination of the contents, the intelligence service decides to retain the set for the purpose of the exercise of its functions, and

(d) the set is held, or is to be held, electronically for analysis in the exercise of those functions.

(3) In this section, "personal data" has the same meaning as in the Data Protection Act 1998 except that it also includes data relating to a deceased individual where the data would be personal data within the meaning of that Act if it related to a living individual.

Requirement for warrant

151 Requirement for authorisation by warrant: general

(1) An intelligence service may not exercise a power for the purpose of obtaining a bulk personal dataset unless the obtaining of the dataset is authorised by a warrant under this Part.

(2) An intelligence service may not exercise a power to retain a bulk personal dataset unless the retention of the dataset is authorised by a warrant under this Part.

(3) An intelligence service may not exercise a power to examine a bulk personal dataset retained by it unless the examination is authorised by a warrant under this Part.

(4) For the purposes of this Part, there are two kinds of warrant—

(a) a warrant, referred to in this Part as "a class BPD warrant", authorising an intelligence service to obtain, retain or examine bulk personal datasets that fall within a class described in the warrant;

(b) a warrant, referred to in this Part as "a specific BPD warrant", authorising an intelligence service—

(i) to obtain, retain and examine a bulk personal dataset described in the warrant;

(ii) to retain and examine a bulk personal dataset described in the warrant.

(5) Section 152 sets out exceptions to the restrictions imposed by subsections (1) to (3) of this section.

152 Exceptions to section 151(1) to (3)

(1) Section 151(1) to (3) does not apply to the exercise of a power conferred on an intelligence service by a warrant or other authorisation issued or given under this Act.

(2) Section 151(2) does not apply at any time when a bulk personal dataset is being retained for the purpose of enabling an application for a specific BPD warrant relating to the dataset to be made and determined.

(3) Section 151(2) or (3) does not apply at any time when a bulk personal dataset is being retained or (as the case may be) examined for the purpose of enabling any of the information contained in it to be deleted.

Issue of warrants

153 Class BPD warrants

(1) The head of an intelligence service, or a person acting on his or her behalf, may apply to the Secretary of State for a class BPD warrant.

(2) The application must include—
- (a) a description of the class of bulk personal datasets to which the application relates, and
- (b) an explanation of the operational purposes for which the applicant wishes to examine bulk personal datasets of that class.

(3) The Secretary of State may issue the warrant if—
- (a) the Secretary of State considers that the warrant is necessary—
  - (i) in the interests of national security,
  - (ii) for the purposes of preventing or detecting serious crime, or
  - (iii) in the interests of the economic well-being of the United Kingdom, so far as those interests are also relevant to the interests of national security,
- (b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by the conduct,
- (c) the Secretary of State considers that—
  - (i) the examination of bulk personal datasets of the class to which the application relates is necessary for one or more operational purposes specified in the warrant (see subsection (4)), and
  - (ii) any examination of datasets of that class for those purposes is necessary as mentioned in paragraph (a),
- (d) the Secretary of State considers that the arrangements made by the intelligence service for storing bulk personal datasets of the class to which the application relates and for protecting them from unauthorised disclosure are satisfactory, and
- (e) the decision to issue the warrant has been approved by a Judicial Commissioner.

(4) A class BPD warrant must—
- (a) include a description of the class of bulk personal datasets to which the warrant relates, and

(b) specify the operational purposes for which bulk personal datasets of that class may be examined.

(5) An examination that is not for an operational purpose specified in the warrant is not authorised by the warrant.

(6) An application for a class BPD warrant may only be made on behalf of the head of an intelligence service by a person holding office under the Crown.

154 Specific BPD warrants

(1) The head of an intelligence service, or a person acting on his or her behalf, may apply to the Secretary of State for a specific BPD warrant in the following cases.

(2) Case 1 is where —
(a) the intelligence service wishes to obtain, retain and examine, or to retain and examine, a bulk personal dataset, and
(b) the bulk personal dataset does not fall within a class described in a class BPD warrant.

(3) Case 2 is where —
(a) the intelligence service wishes to obtain, retain and examine, or to retain and examine, a bulk personal dataset, and
(b) the bulk personal dataset falls within a class described in a class BPD warrant but the intelligence service at any time considers that it would be appropriate to seek a specific BPD warrant.

(4) The application must include—
(a) a description of the bulk personal dataset to which the application relates, and
(b) an explanation of the operational purposes for which the intelligence service wishes to examine the bulk personal dataset.

(5) The Secretary of State may issue the warrant if—
(a) the Secretary of State considers that the warrant is necessary—
(i) in the interests of national security,
(ii) for the purposes of preventing or detecting serious crime, or
(iii) in the interests of the economic well-being of the United Kingdom, so far as those interests are also relevant to the interests of national security,
(b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by the conduct,
(c) the Secretary of State considers that—
(i) the examination of the bulk personal dataset to which the application relates is necessary for one or more operational purposes specified in the warrant (see subsection (7)(c)), and
(ii) any examination of the bulk personal dataset for those purposes is necessary as mentioned in paragraph (a),
(d) the Secretary of State considers that the arrangements made by the intelligence service for storing the bulk personal dataset and for protecting it from unauthorised disclosure are satisfactory, and

(e) except where the Secretary of State considers that there is an urgent need to issue the warrant, the decision to issue it has been approved by a Judicial Commissioner.

(6) A specific BPD warrant relating to a bulk personal dataset ("dataset A") may also authorise the obtaining, retention and examination, or the retention and examination, of other bulk personal datasets ("replacement datasets") that do not exist at the time of the issue of the warrant but may reasonably be regarded as replacements for dataset A.

(7) A specific BPD warrant must—
(a) describe the bulk personal dataset to which the warrant relates,
(b) where the warrant authorises the obtaining, retention and examination, or the retention and examination, of replacement datasets, include a description that will enable those datasets to be identified, and
(c) specify the operational purposes for which the bulk personal dataset and any replacement datasets may be examined.

(8) An examination that is not for an operational purpose specified in the warrant is not authorised by the warrant.

(9) An application for a specific BPD warrant may only be made on behalf of the head of an intelligence service by a person holding office under the Crown.

155 Approval of warrants by Judicial Commissioners

(1) In deciding whether to approve the Secretary of State's decision to issue a class BPD warrant or a specific BPD warrant, a Judicial Commissioner must review the Secretary of State's conclusions on the following matters—
(a) whether the warrant is necessary on grounds falling within section 153(3)(a) or (as the case may be) section 154(5)(a),
(b) whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved by that conduct, and
(c) whether—
(i) the examination that would be authorised by the warrant is necessary for one or more operational purposes specified in it in accordance with section 153(4)(b) or (as the case may be) 154(7)(c), and
(ii) any examination for those purposes is necessary as mentioned in paragraph (a).

(2) In doing so, the Judicial Commissioner must apply the same principles as would be applied by a court on an application for judicial review.

(3) Where a Judicial Commissioner refuses to approve a decision to issue a warrant, the Judicial Commissioner must give the Secretary of State written reasons for the refusal.

156 Approval of warrants issued in urgent cases

(1) This section applies where—
(a) a specific BPD warrant is issued without the approval of a Judicial Commissioner, and
(b) the Secretary of State believed that there was an urgent need to issue it.

(2) The Secretary of State must inform a Judicial Commissioner that it has been issued.

(3) The Judicial Commissioner must, before the end of the relevant period—
  (a) decide whether to approve the decision to issue the warrant, and
  (b) notify the Secretary of State of the Judicial Commissioner's decision.

"The relevant period" means the period ending with the fifth working day after the day on which the warrant was issued.

(4) But subsection (3) does not apply if the Judicial Commissioner is notified that the warrant is to be renewed under section 161 before the end of the relevant period.

(5) If a Judicial Commissioner refuses to approve the decision to issue a warrant, the warrant ceases to have effect.

(6) Section 157 contains further provision about what happens when a warrant ceases to have effect as a result of this section.

157 Warrants ceasing to have effect under section 156

(1) This section applies where a warrant ceases to have effect as a result of section 156.

(2) The head of the intelligence service to whom the warrant is addressed must, so far as is reasonably practicable, secure that anything in the process of being done in reliance on the warrant stops as soon as possible.

(3) The Judicial Commissioner who refused to approve the warrant may—
  (a) direct that any bulk personal datasets obtained or retained in reliance on the warrant be destroyed;
  (b) impose conditions as to the use or retention of any such datasets.

(4) The Judicial Commissioner—
  (a) may require an affected party to make representations about how the Judicial Commissioner should exercise any function under subsection (3), and
  (b) must have regard to any such representations made by an affected party (whether or not as a result of a requirement imposed under paragraph (a)).

(5) Each of the following is an "affected party" for the purposes of subsection (4)—
  (a) the Secretary of State;
  (b) the head of the intelligence service to whom the warrant is addressed.

(6) The Secretary of State may ask the Investigatory Powers Commissioner to review a decision made by any other Judicial Commissioner under subsection (3).

(7) On a review under subsection (6), the Investigatory Powers Commissioner may—
  (a) confirm the Judicial Commissioner's decision, or
  (b) make a fresh determination.

(8) Nothing in this section or section 156 affects the lawfulness of—
  (a) anything done in reliance on the warrant before it ceases to have effect;

(b) if anything is in the process of being done in reliance on the warrant when it ceases to have effect—

(i) anything done before that thing could be stopped, or

(ii) anything done that it is not reasonably practicable to stop.

158 Decisions to issue warrants to be taken personally by Secretary of State

(1) The decision to issue a class BPD warrant or a specific BPD warrant must be taken personally by the Secretary of State.

(2) Before a class BPD warrant is issued, it must be signed by the Secretary of State.

(3) Before a specific BPD warrant is issued, it must be signed by the Secretary of State except that, in an urgent case, it may be signed instead by a senior official designated by the Secretary of State for that purpose.

(4) Where a warrant is signed by a senior official, the warrant must contain a statement that the case is an urgent case in which the Secretary of State has personally expressly authorised the issue of the warrant.

159 Requirements that must be met by warrants

(1) A class BPD warrant or a specific BPD warrant must contain a provision stating that it is a class BPD warrant or (as the case may be) a specific BPD warrant.

(2) A class BPD warrant or a specific BPD warrant must be addressed to the head of the intelligence service by whom or on whose behalf the application for the warrant was made.

Duration, modification and cancellation

160 Duration of warrants

(1) A class BPD warrant or a specific BPD warrant, if it is not renewed before the end of the relevant period (see subsection (2)), ceases to have effect at the end of that period.

(2) In this section, "the relevant period"—

(a) in the case of an urgent specific BPD warrant, means the period ending with the fifth working day after the day on which the warrant was issued;

(b) in any other case, means the period of 6 months beginning with—

(i) the day on which the warrant was issued, or

(ii) in the case of a warrant that has been renewed, the day after the day at the end of which the warrant would have ceased to have effect if it had not been renewed.

(3) For the purposes of subsection (2)(a) an "urgent specific BPD warrant" is a warrant which—

(a) was signed by a senior official in accordance with section 158(3), and

(b) has not been renewed.

(4) For provision about the renewal of warrants, see section 161.

161 Renewal of warrants

(1) If the renewal conditions are met, a class BPD warrant or a specific BPD warrant may be renewed, at any time before the end of the relevant period, by an instrument issued by the Secretary of State.

(2) The renewal conditions are—

(a) the Secretary of State considers that the warrant continues to be necessary on grounds falling within section 153(3)(a) or (as the case may be) section 154(5)(a),

(b) the conduct that would be authorised by the warrant continues to be proportionate to what is sought to be achieved by the conduct,

(c) the Secretary of State considers that—

(i) the examination that would be authorised by the warrant continues to be necessary for one or more operational purposes specified in it in accordance with section 153(4)(b) or (as the case may be) section 154(7)(c), and

(ii) any examination for those purposes continues to be necessary as mentioned in paragraph (a), and

(d) the decision to renew the warrant has been approved by a Judicial Commissioner.

(3) The decision to renew a class BPD warrant or a specific BPD warrant must be taken personally by the Secretary of State, and the instrument renewing the warrant must be signed by the Secretary of State.

(4) Section 155 (approval of warrants by Judicial Commissioner) applies in relation to a decision to renew a warrant as it applies in relation to a decision to issue a warrant.

162 Modification of warrants

(1) The provisions of a class BPD warrant or a specific BPD warrant may be modified at any time by an instrument issued by the person making the modification.

(2) There are two kinds of modifications—

(a) major modifications, and

(b) minor modifications.

(3) The major modifications that may be made are adding or varying any operational purpose specified in the warrant in accordance with section 153(4)(b) or 154(7)(c).

(4) The minor modifications that may be made are removing any operational purpose specified in the warrant in accordance with section 153(4)(b) or 154(7)(c).

(5) A major modification may be made by—

(a) the Secretary of State, or

(b) a senior official acting on behalf of the Secretary of State.

(6) A minor modification may be made by—

(a) the Secretary of State,

(b) a senior official acting on behalf of the Secretary of State,

(c) the head of the intelligence service to whom the warrant is addressed, or

(d) a person who holds a senior position in that intelligence service.

(7) For the purposes of subsection (6)(d), a person holds a senior position in an intelligence service if the person is a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service.

(8) A person may make a major modification only if—

(a) the person considers that—

(i) the modification is necessary on grounds falling within section 153(3)(a) or (as the case may be) section 154(5)(a), and

(ii) the conduct that would be authorised by the modification is proportionate to what is sought to be achieved by the conduct, and

(b) the decision to renew the warrant has been approved by a Judicial Commissioner.

(9) Section 155 (approval of warrants by Judicial Commissioners) applies in relation to a decision to make a major modification to a warrant as it applies in relation to a decision to issue such a warrant.

(10) Where a major modification of a class BPD warrant or a specific BPD warrant is made by a senior official, the Secretary of State must be notified personally of the modification and the reasons for making it.

(11) Nothing in this section applies in relation to modifying the provisions of a warrant in a way that does not affect what is authorised by it.

163 Cancellation of warrants

(1) Any of the appropriate persons may cancel a class BPD warrant or a specific BPD warrant at any time.

(2) If any of the appropriate persons considers—

(a) that a class BPD warrant or a specific BPD warrant is no longer necessary on grounds falling within section 153(3)(3)(a) or (as the case may be) section 154(5)(a), or

(b) that the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved by it,

the person must cancel the warrant.

(3) For the purposes of this section, "the appropriate persons" are—

(a) the Secretary of State, or

(b) a senior official acting on behalf of the Secretary of State.

164 Non-renewal or cancellation of class BPD warrants

(1) This section applies where a class BPD warrant is not renewed or is cancelled.

(2) The head of the intelligence service to whom the warrant is addressed may apply to the Secretary for directions as to what may be done in relation to any material obtained or retained in reliance on the warrant.

(3) The Secretary of State may—

(a) direct that any of the material be destroyed;
(b) with the approval of a Judicial Commissioner, authorise the retention or examination of any of the material, subject to such conditions as the Secretary of State considers appropriate.

(4) If the Judicial Commissioner refuses to approve a decision by the Secretary of State to authorise the retention or examination of any of the material, the Judicial Commissioner must give the Secretary of State written reasons for the refusal.

(5) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve such a decision, the Secretary of State may ask the Investigatory Powers Commissioner to decide whether to approve the decision.

Further and supplementary provision

165 Duty to have regard to code of practice

In carrying out its functions under this Part, an intelligence service must have regard to any code of practice issued under section 179.

166 Interpretation of Part

In this Part—

"class BPD warrant" has the meaning given by section 151(4)(a);

"specific BPD warrant" has the meaning given by section 151(4)(b);

"senior official" means a member of the Senior Civil Service or a member of the Senior Management Structure of Her Majesty's Diplomatic Service.

PART 8

OVERSIGHT ARRANGEMENTS

CHAPTER 1

INVESTIGATORY POWERS COMMISSIONER AND OTHER JUDICIAL COMMISSIONERS

The Commissioners

167 Investigatory Powers Commissioner and other Judicial Commissioners

(1) The Prime Minister must appoint—
(a) the Investigatory Powers Commissioner, and
(b) such number of other Judicial Commissioners as the Prime Minister considers necessary for the carrying out of the functions of the Judicial Commissioners.

(2) A person is not to be appointed as the Investigatory Powers Commissioner or another Judicial Commissioner unless the person holds or has held a high judicial office (within the meaning of Part 3 of the Constitutional Reform Act 2005).

(3) Before appointing any person under subsection (1), the Prime Minister must consult—
  (a) the Scottish Ministers, and
  (b) the First Minister and deputy First Minister in Northern Ireland.

(4) Before appointing a Judicial Commissioner under subsection (1)(b), the Prime Minister must also consult the Investigatory Powers Commissioner.

(5) The Prime Minister must inform the Scottish Ministers and the First Minister and deputy First Minister in Northern Ireland of an appointment under subsection (1).

(6) The Investigatory Powers Commissioner is a Judicial Commissioner and the Investigatory Powers Commissioner and the other Judicial Commissioners are to be known, collectively, as the Judicial Commissioners.

(7) The Investigatory Powers Commissioner may, to such extent as the Investigatory Powers Commissioner may decide, delegate the exercise of functions of the Investigatory Powers Commissioner to any other Judicial Commissioner.

(8) References in any enactment—
  (a) to a Judicial Commissioner are to be read as including the Investigatory Powers Commissioner, and
  (b) to the Investigatory Powers Commissioner are to be read, so far as necessary for the purposes of subsection (7), as references to the Investigatory Powers Commissioner or any other Judicial Commissioner.

168 Terms and conditions of appointment

(1) Subject as follows, each Judicial Commissioner holds and vacates office in accordance with their terms and conditions of appointment.

(2) Each Judicial Commissioner is to be appointed for a term of three years.

(3) A person who ceases to be a Judicial Commissioner (otherwise than under subsection (5) or (6)) may be re-appointed under section 167(1).

(4) A Judicial Commissioner may not, subject to subsections (5) and (6), be removed from office before the end of the term for which the Commissioner is appointed unless a resolution approving the removal has been passed by each House of Parliament.

(5) A Judicial Commissioner may be removed from office by the Prime Minister if, after the appointment of the Commissioner—
  (a) a bankruptcy order is made against the Commissioner or the Commissioner's estate is sequestrated or the Commissioner makes a composition or arrangement with, or grants a trust deed for, the Commissioner's creditors,
  (b) any of the following orders is made against the Commissioner—
    (i) a disqualification order under the Company Directors Disqualification Act 1986 or the Company Directors Disqualification (Northern Ireland) Order 2002,
    (ii) an order under section 429(2)(b) of the Insolvency Act 1986 (failure to pay under county court administration order),

(iii) an order under section 429(2) of the Insolvency Act 1986 (disabilities on revocation of county court administration order),

(c) the Commissioner's disqualification undertaking is accepted under section 7 or 8 of the Company Directors Disqualification Act 1986 or under the Company Directors Disqualification (Northern Ireland) Order 2002, or

(d) the Commissioner is convicted in the United Kingdom, the Channel Islands or the Isle of Man of an offence and receives a sentence of imprisonment (whether suspended or not).

(6) A Judicial Commissioner who is not the Investigatory Powers Commissioner may be removed from office by the Investigatory Powers Commissioner on—

(a) the ground of inability or misbehaviour, or

(b) a ground specified in the Judicial Commissioner's terms and conditions of appointment.

(7) The Investigatory Powers Commissioner must consult the Prime Minister before removing a Judicial Commissioner from office under subsection (6).

Main functions of Commissioners

169 Main oversight functions

(1) The Investigatory Powers Commissioner must keep under review (including by way of audit, inspection and investigation) the exercise by public authorities of statutory functions relating to—

(a) the interception of communications,

(b) the acquisition or retention of communications data, or

(c) equipment interference.

(2) Such statutory functions include, in particular, functions relating to the disclosure, retention or other use of—

(a) intercepted material,

(b) acquired or retained communications data, or

(c) communications, private information or equipment data obtained by means of equipment interference.

(3) The Investigatory Powers Commissioner must keep under review—

(a) the acquisition, retention, use or disclosure of bulk personal datasets by an intelligence service,

(b) the giving and operation of notices under section 188 (national security notices),

(c) the exercise of functions by virtue of Part 2 or 3 of the Regulation of Investigatory Powers Act 2000 (surveillance, covert human intelligence sources and investigation of electronic data protected by encryption etc.),

(d) the adequacy of the arrangements by virtue of which the duties imposed by section 55 of that Act are sought to be discharged,

(e) the exercise of functions by virtue of the Regulation of Investigatory Powers (Scotland) Act 2000 (surveillance and covert human intelligence sources),

(f) the exercise of functions under Part 3 of the Police Act 1997 (authorisation of action in respect of property),

(g) the exercise by the Secretary of State of functions under sections 5 to 7 of the Intelligence Services Act 1994 (warrants for interference with wireless telegraphy, entry and interference with property etc.), and

(h) the exercise by the Scottish Ministers (by virtue of provision made under section 63 of the Scotland Act 1998) of functions under sections 5 and 6(3) and (4) of the Act of 1994.

(4) But the Investigatory Powers Commissioner is not to keep under review—

(a) the exercise of any function of a relevant Minister to make or modify subordinate legislation,

(b) the exercise of any function by a judicial authority,

(c) the exercise of any function by virtue of Part 3 of the Regulation of Investigatory Powers Act 2000 which is exercisable with the permission of a judicial authority,

(d) the exercise of any function in pursuance of a search warrant or production order, or

(e) the exercise of any function which is subject to review by the Information Commissioner.

(5) In exercising functions under this Act, a Judicial Commissioner must not act in a way which is contrary to the public interest or prejudicial to—

(a) national security,

(b) the prevention or detection of serious crime, or

(c) the economic well-being of the United Kingdom.

(6) A Judicial Commissioner must, in particular, ensure that the Commissioner does not—

(a) jeopardise the success of an intelligence or security operation or a law enforcement operation,

(b) compromise the safety or security of those involved, or

(c) unduly impede the operational effectiveness of an intelligence service, a police force, a government department or Her Majesty's forces.

(7) Subsections (5) and (6) do not apply in relation to the functions of a Judicial Commissioner of—

(a) deciding whether to approve the issue, modification or renewal of a warrant or authorisation,

(b) deciding what may be done with data or other material when a warrant issued for what was considered to be an urgent need is cancelled, or

(c) reviewing any decision of the kind mentioned in paragraph (a) or (b).

(8) In this section—

"judicial authority" means—

(a) any judge of the High Court or of the Crown Court or any Circuit Judge,

(b) any judge of the High Court of Justiciary or any sheriff,

(c) any justice of the peace,

(d) any county court judge or resident magistrate in Northern Ireland, or

(e) any person holding any such judicial office as entitles the person to exercise the jurisdiction of a judge of the Crown Court or of a justice of the peace,

"police force" has the same meaning as in Part 2 (see section 45(1)),

"relevant Minister" means a Minister of the Crown or government department, the Scottish Ministers, the Welsh Ministers or a Northern Ireland department,

"statutory function" means any function conferred by virtue of this Act or any other enactment.

170 Additional directed oversight functions

(1) So far as directed to do so by the Prime Minister and subject to subsection (2), the Investigatory Powers Commissioner must keep under review the carrying out of any aspect of the functions of—

(a) an intelligence service,

(b) a head of an intelligence service, or

(c) any part of Her Majesty's forces, or of the Ministry of Defence, so far as engaging in intelligence activities.

(2) Subsection (1) does not apply in relation to anything which is required to be kept under review by the Investigatory Powers Commissioner under section 169.

(3) The Prime Minister may give a direction under this section at the request of the Investigatory Powers Commissioner or otherwise.

(4) The Prime Minister must publish, in a manner which the Prime Minister considers appropriate, any direction under this section (and any revocation of such a direction) except so far as it appears to the Prime Minister that such publication would be contrary to the public interest or prejudicial to—

(a) national security,

(b) the prevention or detection of serious crime,

(c) the economic well-being of the United Kingdom, or

(d) the continued discharge of the functions of any public authority whose activities include activities that are subject to review by the Investigatory Powers Commissioner.

171 Error reporting

(1) The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person of which the Commissioner is aware and which meets the conditions in subsection (2).

(2) The conditions are that—

(a) the Investigatory Powers Commissioner considers that the error is a serious error, and

(b) the Investigatory Powers Tribunal—

(i) agrees that the error is a serious error, and

(ii) considers that it is in the public interest for the person concerned to be informed of the error.

(3) The Commissioner or Tribunal may not decide for the purposes of subsection (2)(a) or (b)(i) that an error is a serious error unless the Commissioner or

Tribunal considers that the error has caused significant prejudice or harm to the person concerned.

(4) Accordingly, the fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

(5) In making its decision for the purposes of subsection (2)(b)(ii), the Tribunal must, in particular, consider—

(a) the seriousness of the error and its effect on the person concerned, and

(b) the extent to which disclosing the error would be contrary to the public interest or prejudicial to—

(i) national security,

(ii) the prevention or detection of serious crime,

(iii) the economic well-being of the United Kingdom, or

(iv) the continued discharge of the functions of any of the intelligence services.

(6) The Investigatory Powers Commissioner must—

(a) consider whether any relevant error of which the Commissioner becomes aware is a serious error for the purposes of subsection (2)(a), and

(b) must refer any error which the Commissioner has decided is a serious error to the Tribunal for decisions for the purposes of subsection (2)(b).

(7) Before making such decisions, the Tribunal must ask (but may not require) the public authority which has made the error to make submissions to the Tribunal about the matters in subsection (2)(b).

(8) When informing a person under subsection (1) of an error, the Investigatory Powers Commissioner must—

(a) inform the person of any rights that the person may have to apply to the Tribunal, and

(b) provide such details of the error as the Commissioner considers to be necessary for the exercise of those rights, having regard in particular to the extent to which disclosing the details would be contrary to the public interest or prejudicial to anything falling within subsection (5)(b)(i) to (iv).

(9) The Investigatory Powers Commissioner may not inform the person to whom it relates of a relevant error except as provided by this section.

(10) A report under section 174(1) must include information about—

(a) the number of relevant errors of which the Investigatory Powers Commissioner has become aware during the year to which the report relates,

(b) the number of references under subsection (6)(b) during that year, and

(c) the number of persons informed under subsection (1) during that year.

(11) In this section "relevant error" means an error—

(a) by a public authority in complying with any requirements which are imposed on it by virtue of this Act or any other enactment and which are subject to review by a Judicial Commissioner, and

(b) of a description identified for this purpose in a code of practice under Schedule 6,

and the Investigatory Powers Commissioner must keep under review the definition of "relevant error".

172 Additional functions under this Part

(1) A Judicial Commissioner must give the Investigatory Powers Tribunal all such assistance (including the Commissioner's opinion as to any issue falling to be determined by the Tribunal) as the Tribunal may require—

(a) in connection with the investigation of any matter by the Tribunal, or

(b) otherwise for the purposes of the Tribunal's consideration or determination of any matter.

(2) A Judicial Commissioner may provide advice or information to any public authority or other person in relation to matters for which the Judicial Commissioners are responsible.

(3) But a Judicial Commissioner must consult the Secretary of State before providing any advice or information under subsection (2) if it appears to the Commissioner that providing the advice or information might be contrary to the public interest or prejudicial to—

(a) national security,

(b) the prevention or detection of serious crime,

(c) the economic well-being of the United Kingdom, or

(d) the continued discharge of the functions of any public authority whose activities include activities that are subject to review by the Investigatory Powers Commissioner.

173 Functions under other enactments

(1) The Investigatory Powers Commissioner and the other Judicial Commissioners have the functions that are exercisable by them by virtue of any other Part of this Act or by virtue of any other enactment.

(2) In Part 3 of the Police Act 1997 (authorisations of action in respect of property: approval by Commissioners)—

(a) in sections 96(1), 103(7)(b) and (8), 104(3) to (8) and 105(1) and (2) for "Chief Commissioner" substitute "Investigatory Powers Commissioner",

(b) in sections 96(1), 97(1)(a) and 103(1), (2), (4) and (5)(b) for "a Commissioner appointed under section 91(1)(b)" substitute "a Judicial Commissioner",

(c) in sections 96(4), 97(4) and (6) and 103(3) and (6) for "a Commissioner" substitute "a Judicial Commissioner",

(d) in section 103(7) for "a Commissioner" substitute "a Judicial Commissioner (other than the Investigatory Powers Commissioner)",

(e) in section 104(1) for ""Chief Commissioner" substitute "Investigatory Powers Commissioner (except where the original decision was made by that Commissioner)",

(f) in section 104(3) and (8)(a) for "the Commissioner" substitute "the Judicial Commissioner concerned",

(g) in section 105(1)(b)(ii) for "the Commissioner" substitute "the Judicial Commissioner", and

(h) in sections 97(5) and 103(9) for "A Commissioner" substitute "A Judicial Commissioner".

(3) In Part 2 of the Regulation of Investigatory Powers Act 2000 (surveillance and covert human intelligence sources: approval by Commissioners)—

(a) in sections 35(1) and (4), 36(2)(a) and (5) and 37(2) to (6) and (8) for "an ordinary Surveillance Commissioner", wherever it appears, substitute "a Judicial Commissioner",

(b) in sections 35(2)(b), 36(6)(g), 37(8)(b) and (9)(b), 38(1) and (4) to (6) and 39(1), (2) and (4) and in the heading to section 39 for "Chief Surveillance Commissioner", wherever it appears, substitute "Investigatory Powers Commissioner",

(c) in sections 35(3)(a), 36(4)(a) and (b) and 40 for "Surveillance Commissioner" substitute "Judicial Commissioner",

(d) in section 38(1)(a) for "an ordinary Surveillance Commissioner" substitute "a Judicial Commissioner (other than the Investigatory Powers Commissioner)",

(e) in sections 38(5) and 39(1)(b) for "ordinary Surveillance Commissioner" substitute "Judicial Commissioner", and

(f) in the headings to sections 38 and 40 for "Surveillance Commissioners" substitute "Judicial Commissioners".

(4) In Part 2 of the Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013 (notification of certain authorisations to, and approval of certain authorisations by, ordinary Surveillance Commissioner)—

(a) in article 4(1), for "an ordinary Surveillance Commissioner" substitute "a Judicial Commissioner",

(b) in article 5(8) and the heading to Part 2, for "ordinary Surveillance Commissioner" substitute "Judicial Commissioner",

(c) in article 6(1) and (3) for "Chief Surveillance Commissioner" substitute "Investigatory Powers Commissioner",

(d) in article 6(1) for "an ordinary Surveillance Commissioner" substitute "a Judicial Commissioner (other than the Investigatory Powers Commissioner)", and

(e) in the heading to article 6 for "Surveillance Commissioners" substitute "Judicial Commissioners".

Reports and information and inspection powers

174 Annual and other reports

(1) The Investigatory Powers Commissioner must, as soon as reasonably practicable after the end of each calendar year, make a report to the Prime Minister about the carrying out of the functions of the Judicial Commissioners.

(2) A report under subsection (1) must, in particular, include—

(a) statistics on the use of the investigatory powers which are subject to review by the Investigatory Powers Commissioner (including the number of warrants or authorisations issued, given, considered or approved during the year),

(b) the information on errors required by virtue of section 171(10),

(c) information about the funding, staffing and other resources of the Judicial Commissioners, and

(d) details of public engagements undertaken by the Judicial Commissioners or their staff.

(3) The Investigatory Powers Commissioner must, at any time, make any report to the Prime Minister which has been requested by the Prime Minister.

(4) The Investigatory Powers Commissioner may, at any time, make any such report to the Prime Minister, on any matter relating to the functions of the Judicial Commissioners, as the Investigatory Powers Commissioner considers appropriate.

(5) A report under subsection (1) or (4) may, in particular, include such recommendations as the Investigatory Powers Commissioner considers appropriate about any matter relating to the functions of the Judicial Commissioners.

(6) On receiving a report from the Investigatory Powers Commissioner under subsection (1), the Prime Minister must—

(a) publish the report, and

(b) lay a copy of the published report before Parliament together with a statement as to whether any part of the report has been excluded from publication under subsection (7).

(7) The Prime Minister may, after consultation with the Investigatory Powers Commissioner, exclude from publication any part of a report under subsection (1) if, in the opinion of the Prime Minister, the publication of that part would be contrary to the public interest or prejudicial to—

(a) national security,

(b) the prevention or detection of serious crime,

(c) the economic well-being of the United Kingdom, or

(d) the continued discharge of the functions of any public authority whose activities include activities that are subject to review by the Investigatory Powers Commissioner.

(8) The Prime Minister must send a copy of every report and statement as laid before Parliament under subsection (6)(b) to—

(a) the Scottish Ministers, and

(b) the First Minister and the deputy First Minister in Northern Ireland.

(9) They must lay that copy report and statement before—

(a) in the case of the Scottish Ministers, the Scottish Parliament, and

(b) in the case of the First Minister and the deputy First Minister in Northern Ireland, the Northern Ireland Assembly.

(10) The Investigatory Powers Commissioner may publish any report under subsection (3) or (4), or any part of such a report, if requested to do so by the Prime Minister.

175 Information and inspection powers

(1) Every relevant person must disclose or provide to a Judicial Commissioner all such documents and information as the Commissioner may require for the purposes of the Commissioner's functions.

(2) Every relevant person must provide a Judicial Commissioner with such assistance as the Commissioner may require in carrying out any inspection for the purposes of the Commissioner's functions.

(3) A public authority may report to the Investigatory Powers Commissioner any refusal by a telecommunications operator or postal operator to comply with any requirements imposed by virtue of this Act.

(4) A public authority, telecommunications operator or postal operator must report to the Investigatory Powers Commissioner any relevant error (within the meaning given by section 171(11)) of which it is aware.

(5) In this section "relevant person" means—

(a) any member of a public authority,

(b) any telecommunications operator or postal operator who is, has been or may become subject to a requirement imposed by virtue of this Act, or

(c) any person who is, has been or may become subject to a requirement to provide assistance by virtue of section 29, 31, 99, 101, 116, 130 or 145.

Supplementary provision

176 Funding, staff and facilities

(1) There is to be paid to the Judicial Commissioners out of money provided by Parliament such remuneration and allowances as the Treasury may determine.

(2) The Secretary of State must, after consultation with the Investigatory Powers Commissioner and subject to the approval of the Treasury as to numbers of staff, provide the Judicial Commissioners with—

(a) such staff, and

(b) such accommodation, equipment and other facilities,

as the Secretary of State considers necessary for the carrying out of the Commissioners' functions.

177 Power to modify functions

(1) The Secretary of State may by regulations modify the functions of the Investigatory Powers Commissioner or any other Judicial Commissioner.

(2) The power to make regulations under this section (including that power as extended by section 197(1)(c)) may, in particular, be exercised by modifying any provision made by or under an enactment (including this Act).

178 Abolition of existing oversight bodies

(1) The offices of—

(a) the Interception of Communications Commissioner,

(b) the Intelligence Services Commissioner,

(c) the Investigatory Powers Commissioner for Northern Ireland,

(d) the Chief Surveillance Commissioner,

(e) the other Surveillance Commissioners,

(f) the Scottish Chief Surveillance Commissioner, and

(g) the other Scottish Surveillance Commissioners,

are abolished.

(2) Accordingly, the following enactments are repealed—

(a) sections 57 and 58 of the Regulation of Investigatory Powers Act 2000 (the Interception of Communications Commissioner),

(b) sections 59, 59A and 60 of that Act (the Intelligence Services Commissioner),

(c) section 61 of that Act (the Investigatory Powers Commissioner for Northern Ireland),

(d) sections 62 and 63 of that Act and sections 91 and 107 of the Police Act 1997 (the Surveillance Commissioners),

(e) section 64 of the Regulation of Investigatory Powers Act 2000 (delegation of Commissioners' functions), and

(f) sections 2 to 4 of the Regulation of Investigatory Powers Act (Scotland) 2000 (the Scottish Surveillance Commissioners).

(3) In this section—

"the other Scottish Surveillance Commissioners" means—

(a) the Surveillance Commissioners appointed under section 2(1)(b) of the Regulation of Investigatory Powers (Scotland) Act 2000, and

(b) the Assistant Surveillance Commissioners appointed under section 3 of that Act,

"the Scottish Chief Surveillance Commissioner" means the Chief Surveillance Commissioner appointed under section 2(1)(a) of that Act.

CHAPTER 2

OTHER ARRANGEMENTS

Codes of practice

179 Codes of practice

Schedule 6 (codes of practice) has effect.

Investigatory Powers Tribunal

180 Right of appeal from Tribunal

(1) After section 67 of the Regulation of Investigatory Powers Act 2000 insert—

"67A Appeals from the Tribunal

(1) A relevant person may appeal on a point of law against any determination of the Tribunal of a kind mentioned in section 68(4) (other than a determination on a reference made to them by virtue of section 65(2)(ca)).

(2) An appeal is to be heard—

(a) in cases falling within any description specified in regulations made by the Secretary of State, by such court in Scotland or Northern Ireland as may be so specified, and

(b) in any other case, by the Court of Appeal in England and Wales.

(3) An appeal may not be made without the leave of the Tribunal or, if that is refused, of the court which would have jurisdiction to hear it.

(4) The Tribunal or court must not grant leave to appeal unless it considers that—

(a) the appeal would raise an important point of principle or practice, or

(b) there is another compelling reason for granting leave.

(5) If the Tribunal refuses leave to appeal, it must at the same time inform the relevant person of the identity of the court which would have jurisdiction to hear the appeal.

(6) In this section "relevant person", in relation to any proceedings, complaint or reference, means the complainant or—

(a) in the case of proceedings, the respondent,

(b) in the case of a complaint, the person complained against, and

(c) in the case of a reference, any public authority to whom the reference relates."

(2) In section 67 of that Act (no appeal from the Investigatory Powers Tribunal except as provided by order of the Secretary of State)—

(a) in subsection (8) for "Except to such extent as the Secretary of State may by order otherwise provide," substitute "Except as provided in section 67A,", and

(b) omit subsections (9) to (12).

(3) In section 69(2) of that Act (Tribunal rules)—

(a) in paragraph (i) after "in addition to" insert "the requirements of section 67A and", and

(b) after paragraph (i) insert ";

(j) make provision about the making and determination of applications to the Tribunal for permission to appeal".

181 Functions of Tribunal in relation to Part 4

(1) In section 65 of the Regulation of Investigatory Powers Act 2000 (the Investigatory Powers Tribunal)—

(a) in subsection (5) (conduct in relation to which the Tribunal has jurisdiction), after paragraph (f), insert ";

(g) the giving or varying of a retention notice under Part 4 of the Investigatory Powers Act 2016;

(h) conduct required or permitted by a retention notice under that Part of that Act (other than conduct which is subject to review by the Information Commissioner)",

(b) after subsection (7ZA) insert—

"(7ZB) For the purposes of this section conduct also takes place in challengeable circumstances if it is, or purports to be, conduct falling within subsection (5)(g).", and

(c) in subsection (8) (matters that may be challenged before the Tribunal), the word "or" at the end of paragraph (e) is omitted and, after

paragraph (f), insert "; or

(g) a retention notice under Part 4 of the Investigatory Powers Act 2016".

(2) In section 67(7) of the Act of 2000 (powers of the Tribunal) after paragraph (aa) (and before the word "and" at the end of it) insert—

"(ab) an order quashing a retention notice under Part 4 of the Investigatory Powers Act 2016;".

(3) In section 68(7) of the Act of 2000 (persons subject to duty to co-operate with the Tribunal)—

(a) after paragraph (m) (and before the word "and" at the end of it) insert—

"(ma) every person who is subject to a retention notice under Part 4 of the Investigatory Powers Act 2016;", and

(b) in paragraph (n) for "or (m)" substitute ", (m) or (ma)".

Information Commissioner

182 Oversight by Information Commissioner in relation to Part 4

The Information Commissioner must audit compliance with requirements or restrictions imposed by virtue of Part 4 in relation to the integrity, security or destruction of data retained by virtue of that Part.

Technical Advisory Board

183 Technical Advisory Board

(1) There is to continue to be a Technical Advisory Board consisting of such number of persons appointed by the Secretary of State as the Secretary of State may by regulations provide.

(2) The regulations providing for the membership of the Technical Advisory Board must also make provision which is calculated to ensure—

(a) that the membership of the Board includes persons likely effectively to represent the interests of the persons on whom obligations may be imposed under this Act and in relation to whom the Board has functions under this Act;

(b) that the membership of the Board includes persons likely effectively to represent the interests of the persons by or on whose behalf applications for warrants or authorisations under this Act may be made and in relation to whom the Board has functions under this Act;

(c) that such other persons (if any) as the Secretary of State considers appropriate may be appointed to be members of the Board; and

(d) that the Board is so constituted as to produce a balance between the representation of the interests mentioned in paragraph (a) and the representation of those mentioned in paragraph (b).

PART 9

MISCELLANEOUS AND GENERAL PROVISIONS

CHAPTER 1

MISCELLANEOUS

Combined warrants and authorisations

184 Combination of warrants and authorisations

Schedule 7 (which makes provision for the combination of targeted interception warrants or targeted equipment interference warrants with other warrants or authorisations) has effect.

Compliance with Act

185 Payments towards certain compliance costs

(1) The Secretary of State must ensure that arrangements are in force for securing that telecommunications operators and postal operators receive an appropriate contribution in respect of such of their relevant costs as the Secretary of State considers appropriate.

(2) In subsection (1) "relevant costs" means costs incurred, or likely to be incurred, by telecommunications operators and postal operators in complying with this Act.

(3) The arrangements may provide for payment of a contribution to be subject to terms and conditions determined by the Secretary of State.

(4) Such terms and conditions may, in particular, include a condition on the operator concerned to comply with any audit that may reasonably be required to monitor the claim for costs.

(5) The arrangements may provide for the Secretary of State to determine—

(a) the scope and extent of the arrangements, and

(b) the appropriate level of contribution which should be made in each case.

(6) Different levels of contribution may apply for different cases or descriptions of case but the appropriate contribution must never be nil.

(7) A retention notice under Part 4 given to a telecommunications operator or a postal operator, or a national security notice under section 188 given to a telecommunications operator, must specify the level or levels of contribution which the Secretary of State has determined should be made in respect of the costs incurred, or likely to be incurred, by the operator as a result of the notice in complying with that Part or (as the case may be) with the national security notice.

(8) For the purpose of complying with this section the Secretary of State may make, or arrange for the making of, payments out of money provided by Parliament.

186 Power to develop compliance systems etc.

(1) The Secretary of State may—

(a) develop, provide, maintain or improve, or

(b) enter into financial or other arrangements with any person for the development, provision, maintenance or improvement of,

such apparatus, software, systems or other facilities or services as the Secretary of State considers appropriate for enabling or otherwise facilitating compliance by the Secretary of State, another public authority or any other person with this Act.

(2) Arrangements falling within subsection (1)(b) may, in particular, include arrangements consisting of the giving of financial assistance by the Secretary of State.

(3) Such financial assistance—

(a) may, in particular, be given by way of—

(i) grant,

(ii) loan,

(iii) guarantee or indemnity,

(iv) investment, or

(v) incurring expenditure for the benefit of the person assisted, and

(b) may be given subject to terms and conditions determined by the Secretary of State,

but any financial assistance other than a grant requires the consent of the Treasury.

(4) Terms and conditions imposed by virtue of subsection (3)(b) may include terms and conditions as to repayment with or without interest.

Additional powers

187 Amendments of the Intelligence Services Act 1994

(1) The Intelligence Services Act 1994 is amended as follows.

(2) In section 3 (the Government Communications Headquarters)—

(a) in subsection (1)(a), after "monitor" insert ", make use of", and

(b) in the words following subsection (1)(b)(ii), for the words from "or to any other organisation" to the end substitute "or, in such cases as it considers appropriate, to other organisations (whether or not in the United Kingdom) or to members of the public.".

(3) In section 5 (warrants: general)—

(a) in subsection (2), omit ", subject to subsection (3) below,", and

(b) omit subsection (3).

188 National security notices

(1) The Secretary of State may give any telecommunications operator in the United Kingdom a notice ("a national security notice") requiring the operator to take such specified steps as the Secretary of State considers necessary in the interests of national security.

(2) The Secretary of State may give a national security notice only if the Secretary of State considers that the conduct required by the notice is proportionate to what is sought to be achieved by that conduct.

(3) A national security notice may, in particular, require the operator to whom it is given—

(a) to carry out any conduct, including the provision of services or facilities, for the purpose of—

(i) facilitating anything done by an intelligence service under any enactment other than this Act, or

(ii) dealing with an emergency (within the meaning of Part 1 of the Civil Contingencies Act 2004);

(b) to provide services or facilities for the purpose of assisting an intelligence service to carry out its functions more securely or more effectively.

(4) But a national security notice may not require the taking of any steps the main purpose of which is to do something for which a warrant or authorisation is required under this Act.

(5) Sections 190 and 191 contain further provision about national security notices.

189 Maintenance of technical capability

(1) The Secretary of State may make regulations imposing specified obligations on relevant operators, or relevant operators of a specified description.

(2) In this section "relevant operator" means any person who provides, or is proposing to provide—

(a) public postal services, or

(b) telecommunications services.

(3) Regulations under this section may impose an obligation on any relevant operators only if the Secretary of State considers it is reasonable to do so for the purpose of securing—

(a) that it is (and remains) practicable to impose requirements on those relevant operators to provide assistance in relation to relevant authorisations (see subsection (9)), and

(b) that it is (and remains) practicable for those relevant operators to comply with those requirements.

(4) The obligations that may be imposed by regulations under this section include, among other things—

(a) obligations to provide facilities or services of a specified description;

(b) obligations relating to apparatus owned or operated by a relevant operator;

(c) obligations relating to the removal of electronic protection applied by a relevant operator to any communications or data;

(d) obligations relating to the security of any postal or telecommunications services provided by a relevant operator;

(e) obligations relating to the handling or disclosure of any material or data.

(5) Before making any regulations under this section, the Secretary of State must consult the following persons—

(a) the Technical Advisory Board,
(b) persons appearing to the Secretary of State to be likely to be subject to the obligations specified in the regulations,
(c) persons representing persons falling within paragraph (b), and
(d) persons with statutory functions in relation to persons falling within that paragraph.

(6) The Secretary of State may give any person, or any person of a specified description, on whom obligations are imposed under this section a notice (a "technical capability notice") requiring the person to take all the steps specified in the notice for the purpose of complying with those obligations.

(7) The only steps that may be specified in a technical capability notice given to a person are steps which the Secretary of State considers to be necessary for securing that the person has the practical capability of providing any assistance which the person may be required to provide in relation to any relevant authorisation.

(8) An obligation specified in regulations under this section may be imposed on, and a technical capability notice given to, persons outside the United Kingdom (and may require things to be done, or not to be done, outside the United Kingdom).

(9) In this section "relevant authorisation" means—
(a) any warrant issued under Part 2, 5 or 6, or
(b) any authorisation or notice given under Part 3.

(10) Sections 190 and 191 contain further provision about technical capability notices.

190 Further provision about notices under section 188 or 189

(1) In this section "relevant notice" means—
(a) a national security notice under section 188, or
(b) a technical capability notice under section 189.

(2) Before giving a relevant notice to a person, the Secretary of State must consult that person.

(3) Before giving a relevant notice, the Secretary of State must, among other things, take into account—
(a) the likely benefits of the notice,
(b) the likely number of users (if known) of any postal or telecommunications service to which the notice relates,
(c) the technical feasibility of complying with the notice,
(d) the likely cost of complying with the notice, and
(e) any other effect of the notice on the person (or description of person) to whom it relates.

(4) A relevant notice must specify such period as appears to the Secretary of State to be reasonable as the period within which the steps specified in the notice are to be taken.

(5) A technical capability notice may be given to a person outside the United Kingdom in any of the following ways (as well as by electronic or other means of giving a notice)—

(a) by delivering it to the person's principal office within the United Kingdom or, if the person has no such office in the United Kingdom, to any place in the United Kingdom where the person carries on business or conducts activities;

(b) if the person has specified an address in the United Kingdom as one at which the person, or someone on the person's behalf, will accept documents of the same description as a notice, by delivering it to that address.

(6) The Secretary of State may by regulations make further provision about the giving of relevant notices.

(7) The Secretary of State must keep each relevant notice under review.

(8) A person to whom a relevant notice is given, or any person employed or engaged for the purposes of that person's business, must not disclose the existence and contents of the notice to any other person.

(9) A person to whom a relevant notice is given must comply with the notice.

(10) The duty imposed by subsection (9) is enforceable—

(a) in relation to a person in the United Kingdom, and

(b) so far as relating to a technical capability notice within subsection (11), in relation to a person outside the United Kingdom,

by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.

(11) A technical capability notice is within this subsection if it relates to any of the following—

(a) a targeted interception warrant or mutual assistance warrant under Chapter 1 of Part 2;

(b) a bulk interception warrant;

(c) an authorisation or notice given under Part 3.

191 Review by the Secretary of State

(1) A person who is given a notice under section 188 or 189 may, within such period or circumstances as may be provided for in regulations made by the Secretary of State, refer the notice back to the Secretary of State.

(2) Such a reference may be in relation to the whole of a notice or any aspect of it.

(3) There is no requirement for a person who has referred a notice under subsection (1) to comply with the notice, so far as referred, until the Secretary of State has reviewed the notice in accordance with subsection (4).

(4) The Secretary of State must review any notice so far as referred to the Secretary of State under subsection (1).

(5) Before deciding the review, the Secretary of State must consult—

(a) the Technical Advisory Board, and

(b) the Investigatory Powers Commissioner.

(6) The Board must consider the technical requirements and the financial consequences, for the person who has made the reference, of the notice so far as referred.

(7) The Commissioner must consider whether the notice so far as referred is proportionate.

(8) The Board and the Commissioner must—

(a) give the person concerned the opportunity to provide evidence to them before reaching their conclusions,

(b) give the Secretary of State the opportunity to make representations to them before reaching their conclusions, and

(c) report their conclusions to—

(i) the person, and

(ii) the Secretary of State.

(9) The Secretary of State may, after considering the conclusions of the Board and the Commissioner—

(a) vary or withdraw the notice, or

(b) give a notice under this section to the person confirming its effect.

(10) Subsections (5), (6) and (8) of section 190 apply in relation to a notice under subsection (9)(b) above as they apply in relation to a notice under section 188 or 189.

Wireless telegraphy

192 Amendments of the Wireless Telegraphy Act 2006

(1) The Wireless Telegraphy Act 2006 is amended as follows.

(2) Section 48 (interception and disclosure of messages) is amended as follows.

(3) In subsection (1), for "otherwise than under the authority of a designated person" substitute "without lawful authority".

(4) After subsection (3) insert—

"(3A) A person does not commit an offence under this section consisting in any conduct if the conduct—

(a) constitutes an offence under section 2 of the Investigatory Powers Act 2016 (offence of unlawful interception), or

(b) would do so in the absence of any lawful authority (within the meaning of section 5 of that Act)."

(5) Omit subsection (5).

(6) Omit section 49 (interception authorities).

(7) In consequence of the repeal made by subsection (6)—

(a) in sections 50(5) and 119(2)(a), for "49" substitute "48";

(b) in section 121(2), omit paragraph (b).

CHAPTER 2

GENERAL

Interpretation

193 Telecommunications definitions

(1) The definitions in this section have effect for the purposes of this Act.

Communication

(2) "Communication", in relation to a telecommunications operator, telecommunications service or telecommunication system, includes—

(a) anything comprising speech, music, sounds, visual images or data of any description, and

(b) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus.

Entity data

(3) "Entity data" means any data which—

(a) is about—

(i) an entity,

(ii) an association between a telecommunications service and an entity, or

(iii) an association between any part of a telecommunication system and an entity,

(b) consists of, or includes, data which identifies or describes the entity (whether or not by reference to the entity's location), and

(c) is not events data.

Events data

(4) "Events data" means any data which identifies or describes an event (whether or not by reference to its location) on, in or by means of a telecommunication system where the event consists of one or more entities engaging in a specific activity at a specific time.

Communications data

(5) "Communications data", in relation to a telecommunications operator, telecommunications service or telecommunication system, means entity data or events data—

(a) which is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator and—

(i) is about an entity to which a telecommunications service is provided and relates to the provision of the service,

(ii) is comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of a telecommunication system by means of which the communication is being or may be transmitted, or

(iii) does not fall within sub-paragraph (i) or (ii) but does relate to the use of a telecommunications service or a telecommunication system,

(b) which is available directly from a telecommunication system and falls within sub-paragraph (i), (ii) or (iii) of paragraph (a), or

(c) which—

(i) is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator,

(ii) is about the architecture of a telecommunication system, and

(iii) is not about a specific person,

but does not include the content of a communication.

Content of a communication

(6) The content of a communication is the elements of the communication, and any data attached to or logically associated with the communication, which reveal anything of what might reasonably be expected to be the meaning of the communication but—

(a) anything in the context of web browsing which identifies the telecommunications service concerned is not content, and

(b) any meaning arising from the fact of the communication or from any data relating to the transmission of the communication is to be disregarded.

Other definitions

(7) "Entity" means a person or thing.

(8) "Public telecommunications service" means any telecommunications service which is offered or provided to the public, or a substantial section of the public, in any one or more parts of the United Kingdom.

(9) "Public telecommunication system" means any parts of a telecommunication system by means of which any public telecommunications service is provided which are located in the United Kingdom.

(10) "Telecommunications operator" means a person who—

(a) offers or provides a telecommunications service to persons in the United Kingdom, or

(b) controls or provides a telecommunication system which is (wholly or partly)—

(i) in the United Kingdom, or

(ii) controlled from the United Kingdom.

(11) "Telecommunications service" means any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service).

(12) For the purposes of subsection (11), the cases in which a service is to be taken to consist in the provision of access to, and of facilities for making use of, a telecommunication system include any case where a service consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system.

(13) "Telecommunication system" means a system (including the apparatus comprised in it) that exists (whether wholly or partly in the United Kingdom

or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy.

(14) "Private telecommunication system" means any telecommunication system which—

(a) is not a public telecommunication system,

(b) is attached, directly or indirectly, to a public telecommunication system (whether or not for the purposes of the communication in question), and

(c) includes apparatus which is both located in the United Kingdom and used (with or without other apparatus) for making the attachment to that public telecommunication system.

194 Postal definitions

(1) The definitions in this section have effect for the purposes of this Act.

Communication

(2) "Communication", in relation to a postal operator or postal service (but not in the definition of "postal service" in this section), includes anything transmitted by a postal service.

Communications data

(3) "Communications data", in relation to a postal operator or postal service, means—

(a) postal data comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of a postal service by means of which it is being or may be transmitted,

(b) information about the use made by any person of a postal service (but excluding the content of a communication (apart from information within paragraph (a)), or

(c) information not within paragraph (a) or (b) that is (or is to be) held or obtained by a person providing a postal service, is about those to whom the service is provided by that person and relates to the service so provided.

Postal data

(4) "Postal data" means data which—

(a) identifies, or purports to identify, a person, apparatus or location to or from which a communication is or may be transmitted,

(b) identifies or selects, or purports to identify or select, apparatus through which, or by means of which, a communication is or may be transmitted,

(c) identifies, or purports to identify, the time at which an event relating to a communication occurs, or

(d) identifies the data or other data as data comprised in, included as part of, attached to or logically associated with a particular communication.

For the purposes of this definition "data", in relation to a postal item, includes anything written on the outside of the item.

Other definitions

(5) "Postal item" means—

(a) any letter, postcard or other such thing in writing as may be used by the sender for imparting information to the recipient, or

(b) any packet or parcel.

(6) "Postal operator" means a person providing a postal service to persons in the United Kingdom.

(7) "Postal service" means a service that—

(a) consists in the following, or in any one or more of them, namely, the collection, sorting, conveyance, distribution and delivery (whether in the United Kingdom or elsewhere) of postal items, and

(b) has as its main purpose, or one of its main purposes, to make available, or to facilitate, a means of transmission from place to place of postal items containing communications.

(8) "Public postal operator" means a person providing a public postal service.

(9) "Public postal service" means a postal service that is offered or provided to the public, or a substantial section of the public, in any one or more parts of the United Kingdom.

195 General definitions

(1) In this Act—

"apparatus" includes any equipment, machinery or device (whether physical or logical) and any wire or cable,

"bulk acquisition warrant" has the meaning given by section 122(5),

"bulk equipment interference warrant" has the meaning given by section 135(1),

"bulk interception warrant" has the meaning given by section 106(1),

"civil proceedings" means any proceedings in or before any court or tribunal that are not criminal proceedings,

"crime" means conduct which—

(a) constitutes one or more criminal offences, or

(b) is, or corresponds to, any conduct which, if it all took place in any one part of the United Kingdom, would constitute one or more criminal offences,

"criminal proceedings" includes proceedings before a court in respect of a service offence within the meaning of the Armed Forces Act 2006 (and references to criminal prosecutions are to be read accordingly),

"data" includes any information which is not data,

"enactment" means an enactment whenever passed or made; and includes—

(a) an enactment contained in subordinate legislation within the meaning of the Interpretation Act 1978,

(b) an enactment contained in, or in an instrument made under, an Act of the Scottish Parliament,

(c) an enactment contained in, or in an instrument made under, Northern Ireland legislation, and

(d) an enactment contained in, or in an instrument made under, a Measure or Act of the National Assembly for Wales,

"enhanced affirmative procedure" has the meaning given by section 198,

"functions" includes powers and duties,

"GCHQ" has the same meaning as in the Intelligence Services Act 1994,

"head", in relation to an intelligence service, means—

(a) in relation to the Security Service, the Director-General,

(b) in relation to the Secret Intelligence Service, the Chief, and

(c) in relation to GCHQ, the Director,

"Her Majesty's forces" has the same meaning as in the Armed Forces Act 2006,

"intelligence service" means the Security Service, the Secret Intelligence Service or GCHQ,

"the Investigatory Powers Tribunal" means the tribunal established under section 65 of the Regulation of Investigatory Powers Act 2000,

"legal proceedings" means—

(a) civil or criminal proceedings in or before a court or tribunal, or

(b) proceedings before an officer in respect of a service offence within the meaning of the Armed Forces Act 2006,

"modify" includes amend, repeal or revoke (and related expressions are to be read accordingly),

"person" (other than in Part 2) includes an organisation and any association or combination of persons,

"person holding office under the Crown" includes any servant of the Crown and any member of Her Majesty's forces,

"primary legislation" means—

(a) an Act of Parliament,

(b) an Act of the Scottish Parliament,

(c) a Measure or Act of the National Assembly for Wales, or

(d) Northern Ireland legislation,

"public authority" means a public authority within the meaning of section 6 of the Human Rights Act 1998, other than a court or tribunal,

"serious crime" means crime where—

(a) the offence, or one of the offences, which is or would be constituted by the conduct concerned is an offence for which a person who has reached the age of 18 (or, in relation to Scotland or Northern Ireland, 21) and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of 3 years or more, or

(b) the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose,

"source of journalistic information" has the meaning given by section 61(7),

"specified", in relation to an authorisation, warrant, notice or regulations, means specified or described in the authorisation, warrant, notice or (as the case may be) regulations (and "specify" is to be read accordingly),

"subordinate legislation" means—

(a) subordinate legislation within the meaning of the Interpretation Act 1978, or

(b) an instrument made under an Act of the Scottish Parliament, Northern Ireland legislation or a Measure or Act of the National Assembly for Wales,

"targeted equipment interference warrant" has the meaning given by section 81,

"targeted interception warrant" has the meaning given by section 12,

"the Technical Advisory Board" means the Board provided for by section 183,

"working day" means a day other than a Saturday, a Sunday, Christmas Day, Good Friday or a bank holiday under the Banking and Financial Dealings Act 1971 in any part of the United Kingdom.

(2) For the purposes of this Act detecting crime is to be taken to include—

(a) establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, and

(b) the apprehension of the person by whom any crime was committed,

and any reference in this Act to preventing or detecting serious crime is to be read accordingly.

Supplementary provision

196 Offences by bodies corporate etc.

(1) This section applies if an offence under this Act is committed by a body corporate or a Scottish partnership.

(2) If the offence is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of—

(a) a senior officer of the body corporate or Scottish partnership, or

(b) a person purporting to act in such a capacity,

the senior officer or person (as well as the body corporate or partnership) is guilty of the offence and liable to be proceeded against and punished accordingly.

(3) In this section—

"director", in relation to a body corporate whose affairs are managed by its members, means a member of the body corporate,

"senior officer" means—

(a) in relation to a body corporate, a director, manager, secretary or other similar officer of the body corporate, and

(b) in relation to a Scottish partnership, a partner in the partnership.

197 Regulations

(1) Any power of the Secretary of State or the Treasury to make regulations under this Act—

(a) is exercisable by statutory instrument,

(b) may be exercised so as to make different provision for different cases or descriptions of case, different circumstances, different purposes or different areas, and

(c) includes power to make supplementary, incidental, consequential, transitional, transitory or saving provision.

(2) A statutory instrument containing regulations under section 55 to which section 56 applies may not be made except in accordance with the enhanced affirmative procedure.

(3) A statutory instrument containing regulations under—

(a) section 9 or 201 which amend or repeal any provision of primary legislation,
(b) section 34,
(c) section 39,
(d) section 67,
(e) section 73(1),
(f) section 177,
(g) section 183,
(h) section 189, or
(i) section 191(1),

may not be made unless a draft of the instrument has been laid before, and approved by a resolution of, each House of Parliament.

(4) A statutory instrument containing—

(a) regulations under section 9 or 201 to which subsection (3) does not apply,
(b) regulations under section 49, or
(c) regulations under paragraph 2(1)(b) of Schedule 5,

is (if a draft of the instrument has not been laid before, and approved by a resolution of, each House of Parliament) subject to annulment in pursuance of a resolution of either House of Parliament.

(5) A statutory instrument containing—

(a) regulations under section 7,
(b) regulations under section 55 to which section 56 does not apply,
(c) regulations under section 57(4), or
(d) regulations under section 190(6),

is subject to annulment in pursuance of a resolution of either House of Parliament.

(6) A statutory instrument containing regulations under paragraph 4 of Schedule 5 is subject to annulment in pursuance of a resolution of the House of Commons.

(7) See paragraphs 5(4) and 6(5) of Schedule 6 for the procedure for a statutory instrument containing regulations about the coming into force of a code of practice under that Schedule or of any revisions to such a code of practice.

(8) Provision is not prevented from being included in regulations made under a particular power conferred by this Act merely because the provision could be included in regulations made under a different power conferred by this Act and subject to a different or no parliamentary procedure.

198 Enhanced affirmative procedure

(1) For the purposes of regulations under section 55 to which section 56 applies, the enhanced affirmative procedure is as follows.

(2) Subsection (3) applies if—

(a) the Secretary of State has consulted under section 56(2) in relation to making such regulations,

(b) a period of at least 12 weeks, beginning with the day on which any such consultation first began, has elapsed, and

(c) the Secretary of State considers it appropriate to proceed with making such regulations.

(3) The Secretary of State must lay before Parliament—

(a) draft regulations, and

(b) a document which explains the regulations.

(4) The Secretary of State may make regulations in the terms of the draft regulations laid under subsection (3) if, after the end of the 40-day period, the draft regulations are approved by a resolution of each House of Parliament.

(5) But subsections (6) to (9) apply instead of subsection (4) if—

(a) either House of Parliament so resolves within the 30-day period, or

(b) a committee of either House charged with reporting on the draft regulations so recommends within the 30-day period and the House to which the recommendation is made does not by resolution reject the recommendation within that period.

(6) The Secretary of State must have regard to—

(a) any representations,

(b) any resolution of either House of Parliament, and

(c) any recommendations of a committee of either House of Parliament charged with reporting on the draft regulations,

made during the 60-day period with regard to the draft regulations.

(7) If after the end of the 60-day period the draft regulations are approved by a resolution of each House of Parliament, the Secretary of State may make regulations in the terms of the draft regulations.

(8) If after the end of the 60-day period the Secretary of State wishes to proceed with the draft regulations but with material changes, the Secretary of State may lay before Parliament—

(a) revised draft regulations, and

(b) a statement giving a summary of the changes proposed.

(9) If the revised draft regulations are approved by a resolution of each House of Parliament, the Secretary of State may make regulations in the terms of the revised draft regulations.

(10) For the purposes of this section regulations are made in the terms of draft regulations or revised draft regulations if they contain no material changes to the provisions of the draft, or revised draft, regulations.

(11) References in this section to the "30-day", "40-day" and "60-day" periods in relation to any draft regulations are to the periods of 30, 40 and 60 days beginning with the day on which the draft regulations were laid before Parliament; and, for this purpose, no account is to be taken of any time during

which Parliament is dissolved or prorogued or during which either House is adjourned for more than four days.

199 Financial provisions

(1) There is to be paid out of money provided by Parliament—

(a) any expenditure incurred by the Secretary of State by virtue of this Act, and

(b) any increase attributable to this Act in the sums payable by virtue of any other Act out of money so provided.

(2) There is to be paid into the Consolidated Fund any sums received by the Secretary of State by virtue of this Act.

200 Transitional, transitory or saving provision

(1) Schedule 8 (transitional, transitory and saving provision) has effect.

(2) The Secretary of State may by regulations make such transitional, transitory or saving provision as the Secretary of State considers appropriate in connection with the coming into force of any provision of this Act.

201 Minor and consequential provision

(1) Schedule 9 (minor and consequential provision) has effect.

(2) The Secretary of State may by regulations make such provision as the Secretary of State considers appropriate in consequence of this Act.

(3) The power to make regulations under this section may, in particular, be exercised by modifying any provision made by or under an enactment.

Final provision

202 Commencement, extent and short title

(1) Subject to subsection (2), this Act comes into force on such day as the Secretary of State may by regulations appoint; and different days may be appointed for different purposes.

(2) Sections 193 to 199, 200(2), 201(2) and (3) and this section come into force on the day on which this Act is passed.

(3) Subject to subsections (4) and (5), this Act extends to England and Wales, Scotland and Northern Ireland.

(4) An amendment, repeal or revocation of an enactment has the same extent as the enactment amended, repealed or revoked.

(5) Her Majesty may by Order in Council provide for any of the provisions of this Act to extend, with or without modifications, to any of the British overseas territories.

(6) This Act may be cited as the Investigatory Powers Act 2016.

SCHEDULES

SCHEDULE 1

Section 6

MONETARY PENALTY NOTICES

PART 1

MONETARY PENALTY NOTICES

Payment of monetary penalties

1 (1) A monetary penalty imposed by a monetary penalty notice must be paid to the Commissioner within the period specified in the notice.

(2) The period specified under sub-paragraph (1) must not be less than 28 days beginning with the day after the day on which the notice is served.

(3) Any sum received by the Commissioner by virtue of a monetary penalty notice must be paid into the Consolidated Fund.

Contents of monetary penalty notices

2 A monetary penalty notice must, in particular—

(a) state the name and address of the person on whom it is to be served,

(b) provide details of the notice of intent served on that person (see paragraph 4),

(c) state whether the Commissioner has received written representations in accordance with that notice of intent,

(d) state the grounds on which the Commissioner serves the monetary penalty notice,

(e) state the grounds on which the Commissioner decided the amount of the monetary penalty imposed by the monetary penalty notice,

(f) state the details of how the monetary penalty is to be paid,

(g) provide details of the person's rights of appeal under paragraph 8 in respect of the monetary penalty notice,

(h) provide details of the Commissioner's rights of enforcement under paragraph 9 in respect of the monetary penalty notice.

Enforcement obligations

3 (1) The Commissioner may include an enforcement obligation, or enforcement obligations, in a monetary penalty notice if the Commissioner considers that the interception to which the notice relates is continuing.

(2) Each of the following is an enforcement obligation—

(a) a requirement on the person on whom the notice is served to cease the interception on a specified day or within a specified period;

(b) (where appropriate for achieving such a cessation) a requirement on the person to take specified steps within a specified period, or to refrain from taking specified steps after the end of a specified period.

"Specified" means specified in the notice.

(3) An enforcement obligation may not have effect before the end of the period of 7 days beginning with the day after the day on which the notice is served.

(4) Where an enforcement obligation is included in a monetary penalty notice under this paragraph, the notice must state what the obligation is and the grounds for including it.

Consultation requirements before service of monetary penalty notices

4 (1) The Commissioner must proceed in accordance with sub-paragraphs (2) to (7) before serving a monetary penalty notice on a person.

(2) The Commissioner must serve a notice of intent on the person.

(3) A notice of intent is a notice that the Commissioner proposes to serve a monetary penalty notice on the person.

(4) A notice of intent served on a person must, in particular—

(a) state the name and address of the person,

(b) state the grounds on which the Commissioner proposes to serve the monetary penalty notice,

(c) provide an indication of the amount of the monetary penalty that the Commissioner proposes to impose and the Commissioner's grounds for deciding that amount,

(d) state whether the monetary penalty notice is to include any enforcement obligation and, if so, what the obligation is and the grounds for including it,

(e) state the date on which the Commissioner proposes to serve the monetary penalty notice,

(f) inform the person that the person may make written representations in relation to the Commissioner's proposal within a period specified in the notice, and

(g) inform the person that the person may, within a period specified in the notice, request an oral hearing before the Commissioner in order to make representations of the kind mentioned in sub-paragraph (6)(b).

(5) No period specified as mentioned in sub-paragraph (4)(f) or (g) may be less than 21 days beginning with the day after the day on which the notice is served.

(6) Where the person has requested an oral hearing within the period specified for the purpose in the notice—

(a) the Commissioner must arrange such a hearing, and

(b) the person may make representations at the hearing about—

(i) any matter falling within section 6(3)(c), or

(ii) any other matter relating to the Commissioner's proposal which, by virtue of section 42, the person would be unable to raise on an appeal under paragraph 8.

(7) The Commissioner must consider any representations which have been made by the person in accordance with the notice or sub-paragraph (6).

(8) If the Commissioner decides not to serve a monetary penalty notice on a person as a result of any representations which have been made by the person in accordance with a notice of intent or sub-paragraph (6), the Commissioner must inform the person of that fact.

5 (1) The Commissioner may not vary a notice of intent except as set out in sub-paragraph (2).

(2) The Commissioner may vary a notice of intent by extending the period mentioned in paragraph 4(4)(f) or (g).

(3) Sub-paragraph (1) does not prevent the Commissioner from serving a new notice of intent instead of varying such a notice.

(4) The Commissioner may cancel a notice of intent.

(5) A variation or cancellation of a notice of intent is effected by serving on the person on whom the notice was served a notice setting out the variation or cancellation.

6 (1) The Commissioner must not serve a monetary penalty notice on a person in respect of an interception if any notice of intent in respect of that interception was served on the person more than 3 months earlier.

(2) But the Commissioner may serve a monetary penalty notice on a person where the service of the notice would otherwise be prevented by sub-paragraph (1) if the Commissioner—

(a) considers it reasonable to do so, and

(b) includes the reasons for doing so in the monetary penalty notice.

Variation or cancellation of monetary penalty notices

7 (1) The Commissioner may vary or cancel a monetary penalty notice.

(2) But the Commissioner may not vary a monetary penalty notice in a way that is detrimental to the person on whom it was served (whether by increasing the amount of the monetary penalty, by reducing the period specified in the notice as the period within which the penalty must be paid, by imposing a new enforcement obligation or making an existing enforcement obligation effective earlier or otherwise more onerous, or otherwise).

(3) The Commissioner must—

(a) in the case of a variation which reduces the amount of a monetary penalty, repay any excess already paid in accordance with the notice, and

(b) in the case of a cancellation, repay any amount already paid in accordance with the notice.

(4) A variation or cancellation of a monetary penalty notice is effected by serving on the person on whom the monetary penalty notice was served a notice setting out the variation or cancellation.

(5) The Commissioner may not serve another monetary penalty notice on a person in respect of an interception if the Commissioner has cancelled a previous notice served on the person in respect of the same interception.

(6) If the Commissioner refuses a request by a person to vary or cancel a monetary penalty notice which has been served on the person, the Commissioner must inform the person of that fact.

Appeals in relation to monetary penalty notices

8 (1) A person on whom a monetary penalty notice is served may appeal to the First-tier Tribunal against—

(a) the monetary penalty notice or any provision of it, or

(b) any refusal of a request by the person to serve a notice of variation or cancellation in relation to the monetary penalty notice.

(2) Where there is an appeal under sub-paragraph (1)(a) in relation to a monetary penalty notice or any provision of it, any requirement in the notice or (as the case may be) provision which does not relate to the imposition of an enforcement obligation need not be complied with until the appeal is withdrawn or finally determined.

(3) Sub-paragraphs (4) to (6) apply in relation to an appeal under sub-paragraph (1)(a).

(4) The First-tier Tribunal must allow the appeal or substitute such other monetary penalty notice as could have been served by the Commissioner if the Tribunal considers—

(a) that the notice to which the appeal relates is not in accordance with the law, or

(b) to the extent that the notice involved an exercise of discretion by the Commissioner, that the Commissioner ought to have exercised the discretion differently.

(5) In any other case, the First-tier Tribunal must dismiss the appeal.

(6) The First-tier Tribunal may review any determination of fact on which the notice was based.

(7) Sub-paragraphs (8) to (10) apply in relation to an appeal under sub-paragraph (1)(b).

(8) The First-tier Tribunal must direct the Commissioner to serve, on such terms as the Tribunal considers appropriate, a notice of variation or cancellation in relation to the monetary penalty notice if the Tribunal considers that the monetary penalty notice ought to be varied or cancelled on those terms.

(9) In any other case, the First-tier Tribunal must dismiss the appeal.

(10) The First-tier Tribunal may review any determination of fact on which the refusal to serve the notice of variation or cancellation was based.

Enforcement of monetary penalty notices

9 (1) This paragraph applies in relation to any penalty payable to the Commissioner by virtue of a monetary penalty notice.

(2) In England and Wales or Northern Ireland, the penalty is recoverable—

(a) if the county court in England and Wales or a county court in Northern Ireland so orders, as if it were payable under an order of that court, and

(b) if the High Court so orders, as if it were payable under an order of that court.

(3) In Scotland, the penalty is recoverable as if it were payable under an extract registered decree arbitral bearing a warrant for execution issued by the sheriff for any sheriffdom in Scotland.

10 (1) A person on whom a monetary penalty notice containing an enforcement obligation is served must comply with the obligation.

(2) The duty imposed by sub-paragraph (1) is enforceable by civil proceedings by the Commissioner for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.

Guidance

11 (1) The Commissioner must prepare and issue guidance on how the Commissioner proposes to exercise the Commissioner's functions under section 6 and this Schedule.

(2) The guidance must, in particular, deal with—

(a) the manner in which the Commissioner is to deal with claims of a description specified in the guidance which may give rise to grounds for serving a monetary penalty notice,

(b) the circumstances in which the Commissioner would consider it appropriate to serve a monetary penalty notice,

(c) how the Commissioner will determine the amount of the penalty, and

(d) the circumstances in which the Commissioner would consider it appropriate to impose an enforcement obligation.

(3) The Commissioner may alter or replace the guidance.

(4) If the guidance is altered or replaced, the Commissioner must issue the altered or replacement guidance.

(5) The Commissioner must arrange for the publication, in such form and manner as the Commissioner considers appropriate, of any guidance issued under this paragraph.

Interpretation of Part 1

12 In this Part of this Schedule—

"address" means—

(a) in the case of a registered company, the address of its registered office,

(b) in the case of a person (other than a registered company) carrying on a business, the address of the person's principal place of business in the United Kingdom, and

(c) in any other case, the person's last known address;

"business" includes any trade or profession;

"the Commissioner" means the Investigatory Powers Commissioner;

"enforcement obligation" has the meaning given by paragraph 3(2);

"monetary penalty notice" means a monetary penalty notice under section 6;

"notice" means notice in writing;

"notice of intent" has the meaning given by paragraph 4(3);

"registered company" means a company registered under the enactments relating to companies for the time being in force in the United Kingdom.

PART 2

INFORMATION PROVISIONS

Information notices

13 (1) The Commissioner may by notice (an "information notice") request any person on whom the Commissioner is considering whether to serve a Part 1 notice of intent or a Part 1 monetary penalty notice to provide such information as the Commissioner reasonably requires for the purpose of deciding whether to serve it.

(2) Where the Commissioner requests that documents be produced, the Commissioner may take copies of, or extracts from, any document so produced.

(3) An information notice must—

(a) specify or describe the information to be provided,

(b) specify the manner in which, and the period within which, the information is to be provided,

(c) state that the Commissioner considers that the information is information which the Commissioner reasonably requires for the purpose of deciding whether to serve a Part 1 notice of intent or (as the case may be) a Part 1 monetary penalty notice,

(d) state the Commissioner's grounds for this view, and

(e) provide details of the rights of appeal under paragraph 15 in respect of the information notice.

(4) For the purposes of sub-paragraph (3)(b)—

(a) specifying the manner in which the information is to be provided may include specifying the form in which it is to be provided, and

(b) the specified period within which the information is to be provided must not be less than 28 days beginning with the day after the day on which the information notice is served.

14 (1) The Commissioner may not vary an information notice except as set out in sub-paragraph (2).

(2) The Commissioner may vary an information notice by extending the period within which the information is to be provided if the person on whom the notice is served appeals under paragraph 15 in relation to the notice.

(3) Sub-paragraph (1) does not prevent the Commissioner from serving a new information notice instead of varying such a notice.

(4) The Commissioner may cancel an information notice.

(5) A variation or cancellation of an information notice is effected by serving on the person on whom the notice was served a notice setting out the variation or cancellation.

Appeals in relation to information notices

15 (1) A person on whom an information notice is served may appeal to the First-tier Tribunal against—

(a) the information notice or any provision of it, or

(b) any refusal of a request by the person to serve a notice of variation or cancellation in relation to the information notice.

(2) Subject to paragraph 14(2), an appeal under this paragraph does not affect the need to comply with the information notice while the appeal is not finally determined.

(3) Sub-paragraphs (4) to (6) apply in relation to an appeal under sub-paragraph (1)(a).

(4) The First-tier Tribunal must allow the appeal or substitute such other information notice as could have been served by the Commissioner if the Tribunal considers—

(a) that the notice to which the appeal relates is not in accordance with the law, or

(b) to the extent that the notice involved an exercise of discretion by the Commissioner, that the Commissioner ought to have exercised the discretion differently.

(5) In any other case, the First-tier Tribunal must dismiss the appeal.

(6) The First-tier Tribunal may review any determination of fact on which the notice was based.

(7) Sub-paragraphs (8) to (10) apply in relation to an appeal under sub-paragraph (1)(b).

(8) The First-tier Tribunal must direct the Commissioner to issue, on such terms as the Tribunal considers appropriate, a notice of variation or cancellation in relation to the information notice if the Tribunal considers that the information notice ought to be varied or cancelled on those terms.

(9) In any other case, the First-tier Tribunal must dismiss the appeal.

(10) The First-tier Tribunal may review any determination of fact on which the refusal to serve the notice of variation or cancellation was based.

Enforcement of information notices

16 (1) The Commissioner may serve a Part 2 monetary penalty notice on a person if the person—

(a) without reasonable excuse fails to comply with an information notice, or

(b) knowingly or recklessly gives any information which is false in a material particular in response to an information notice.

(2) A Part 2 monetary penalty notice is a notice requiring the person on whom it is served to pay to the Commissioner a monetary penalty of an amount determined by the Commissioner and specified in the notice.

(3) The amount of a monetary penalty determined by the Commissioner under this paragraph may be—

(a) a fixed amount,

(b) an amount calculated by reference to a daily rate, or

(c) a fixed amount and an amount calculated by reference to a daily rate.

(4) But the total amount payable must not exceed £10,000.

(5) In the case of an amount calculated by reference to a daily rate—

(a) no account is to be taken of the day on which the Part 2 monetary penalty notice is served or any day before that day, and

(b) the Part 2 monetary penalty notice must specify—

(i) the day on which the amount first starts to accumulate and the circumstances in which it is to cease to accumulate, and

(ii) the period or periods within which the amount, or any part or parts so far accumulated, must be paid to the Commissioner.

Any period falling within paragraph (b)(ii) must not be less than 28 days beginning with the day after the day on which the notice is served.

17 (1) Part 1 of this Schedule applies in relation to a Part 2 monetary penalty notice and the penalty that relates to that notice as it applies in relation to a Part 1 monetary penalty notice and the penalty that relates to that notice.

This is subject to the following modifications.

(2) The provisions in Part 1 of this Schedule so far as relating to enforcement obligations do not apply in relation to a Part 2 monetary penalty notice.

(3) Paragraph 4 has effect in relation to a Part 2 monetary penalty notice as if in sub-paragraph (6)(b) the reference to making representations about matters falling within sub-paragraph (6)(b)(i) or (ii) were a reference to making representations about matters falling within sub-paragraph (6)(b)(ii) only.

(4) Paragraph 6 has effect in relation to a Part 2 monetary penalty notice as if the references in sub-paragraph (1) to an interception were references to conduct falling within paragraph 16(1)(a) or (b).

(5) Paragraph 7(5) has effect in relation to a Part 2 monetary penalty notice as if the references to an interception were references to conduct falling within paragraph 16(1)(a) or (b).

Technical assistance for the Commissioner

18 (1) OFCOM must comply with any reasonable request made by the Commissioner, in connection with the Commissioner's functions under section 6 and this Schedule, for advice on technical and similar matters relating to electronic communications.

(2) For this purpose, the Commissioner may disclose to OFCOM any information obtained by the Commissioner under this Schedule.

(3) In this paragraph "OFCOM" means the Office of Communications established by section 1 of the Office of Communications Act 2002.

Interpretation of Part 2

19 In this Part of this Schedule—

"the Commissioner" means the Investigatory Powers Commissioner;

"enforcement obligation" has the meaning given by paragraph 3(2);

"information" includes documents; and any reference to providing or giving information includes a reference to producing a document;

"information notice" has the meaning given by paragraph 13(1);

"notice" means notice in writing;

"Part 1 monetary penalty notice" means a monetary penalty notice under section 6;

"Part 1 notice of intent" means a notice of intent (within the meaning of paragraph 4(3)) relating to a Part 1 monetary penalty notice;

"Part 2 monetary penalty notice" means a monetary penalty notice under paragraph 16.

SCHEDULE 2

Section 9(1)

ABOLITION OF DISCLOSURE POWERS

Health and Safety at Work etc. Act 1974 (c. 37)

1 In section 20 of the Health and Safety at Work etc. Act 1974 (powers of inspectors), at end, insert—

"(9) Nothing in this section is to be read as enabling an inspector to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator.

(10) In subsection (9) "communications data", "postal operator" and "telecommunications operator" have the same meanings as in the Investigatory Powers Act 2016 (see sections 193 and 194 of that Act)."

Criminal Justice Act 1987 (c. 38)

2 In section 2 of the Criminal Justice Act 1987 (investigation powers of Director of Serious Fraud Office), after subsection (10), insert—

"(10A) Nothing in this section is to be read as enabling a person to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator.

(10B) In subsection (10A) "communications data", "postal operator" and "telecommunications operator" have the same meanings as in the Investigatory Powers Act 2016 (see sections 193 and 194 of that Act)."

Consumer Protection Act 1987 (c. 43)

3 In section 29 of the Consumer Protection Act 1987 (powers of search etc.), at

end, insert—

"(8) The officer may not exercise a power under this section to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator.

(9) In subsection (8) "communications data", "postal operator" and "telecommunications operator" have the same meanings as in the Investigatory Powers Act 2016 (see sections 193 and 194 of that Act)."

Environmental Protection Act 1990 (c. 43)

4 In section 71 of the Environmental Protection Act 1990 (obtaining of information from persons and authorities), at end, insert—

"(5) Nothing in this section is to be read as enabling a person to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator.

(6) In subsection (5) "communications data", "postal operator" and "telecommunications operator" have the same meanings as in the Investigatory Powers Act 2016 (see sections 193 and 194 of that Act)."

Social Security Administration Act 1992 (c. 5)

5 In section 109B of the Social Security Administration Act 1992 (power to require information)—

(a) in subsection (2A), omit paragraph (j),

(b) in subsection (2E), for the words from "for" to the end of the subsection substitute "so as to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator.",

(c) omit subsection (2F), and

(d) in subsection (7)—

(i) after the definition of "bank" insert—

""communications data" has the same meaning as in the Investigatory Powers Act 2016 (see sections 193 and 194 of that Act);",

(ii) after the definition of "insurer" insert—

""postal operator" has the same meaning as in the Investigatory Powers Act 2016 (see section 194 of that Act);", and

(iii) for the definition of "telecommunications service" substitute—

""telecommunications operator" has the same meaning as in the Investigatory Powers Act 2016 (see section 193 of that Act).".

6 In section 109C of the Social Security Administration Act 1992 (powers of entry), for subsection (6), substitute—

"(6) Subsections (2E) and (5) of section 109B apply for the purposes of this section as they apply for the purposes of that section."

Financial Services and Markets Act 2000 (c. 8)

7 In section 175 of the Financial Services and Markets Act 2000 (information gathering and investigations: supplemental provision), after subsection (5), insert—

"(5A) Nothing in this Part is to be read as enabling a person to secure the disclosure by a telecommunications operator or postal operator of communications data without the consent of the operator.

(5B) In subsection (5A) "communications data", "postal operator" and "telecommunications operator" have the same meanings as in the Investigatory Powers Act 2016 (see sections 193 and 194 of that Act)."

Finance Act 2008 (c. 9)

8 In Schedule 36 to the Finance Act 2008 (information and inspection powers), in paragraph 19 (restrictions on powers: types of information), at end, insert—

"(4) An information notice does not require a telecommunications operator or postal operator to provide or produce communications data.

(5) In sub-paragraph (4) "communications data", "postal operator" and "telecommunications operator" have the same meanings as in the Investigatory Powers Act 2016 (see sections 193 and 194 of that Act)."

Prevention of Social Housing Fraud (Power to Require Information) (England) Regulations 2014 (S.I. 2014/899)

9 In regulation 4 of the Prevention of Social Housing Fraud (Power to Require Information) (England) Regulations 2014 (power to require information from persons who provide telecommunications services etc.)—

(a) omit sub-paragraph (f) of paragraph (3),
(b) in sub-paragraph (g) of that paragraph for "(f)" substitute "(e)", and
(c) omit paragraphs (6) and (7) and, in paragraph (11), the definition of "telecommunications service".

SCHEDULE 3

Section 42

EXCEPTIONS TO SECTION 42

Introductory

1 This Schedule contains—

(a) exceptions to the exclusion by section 42(1) of certain matters from legal proceedings, and
(b) limitations on those exceptions where that exclusion will still apply.

Disclosures of lawfully intercepted communications

2 (1) Section 42(1)(a) does not prohibit the disclosure of any of the content of a communication if the interception of that communication was lawful by virtue of section 5(1)(c) or any of sections 32 to 39.

(2) Where any disclosure is proposed to be, or has been, made on the grounds that it is authorised by sub-paragraph (1), section 42(1) does not prohibit the doing of anything in, or for the purposes of, so much of any proceedings as relates to the question whether that disclosure is or was so authorised.

Disclosures of convictions for certain offences

3 Section 42(1)(b) does not prohibit the doing of anything that discloses any conduct of a person for which that person has been convicted of—

(a) an offence under section 2(1), 31(7) or 44,

(b) an offence under section 1(1) or (2), 11(7) or 19 of the Regulation of Investigatory Powers Act 2000, or

(c) an offence under section 1 of the Interception of Communications Act 1985.

Proceedings before the Investigatory Powers Tribunal etc.

4 Section 42(1) does not apply in relation to—

(a) any proceedings before the Investigatory Powers Tribunal, or

(b) any proceedings on an appeal under section 67A of the Regulation of Investigatory Powers Act 2000 (appeal against decisions of the Tribunal etc.).

Proceedings before Special Immigration Appeals Commission

5 (1) Section 42(1) does not apply in relation to—

(a) any proceedings before the Special Immigration Appeals Commission, or

(b) any proceedings arising out of proceedings before that Commission.

(2) But nothing in sub-paragraph (1) authorises the disclosure of anything to—

(a) the appellant or (as the case may be) applicant to the Special Immigration Appeals Commission, or

(b) any person who—

(i) represents that appellant or applicant for the purposes of the proceedings, and

(ii) does so otherwise than by virtue of appointment under section 6 of the Special Immigration Appeals Commission Act 1997.

Proceedings before Proscribed Organisations Appeal Commission

6 (1) Section 42(1) does not apply in relation to—

(a) any proceedings before the Proscribed Organisations Appeal Commission, or

(b) any proceedings arising out of proceedings before that Commission.

(2) But nothing in sub-paragraph (1) authorises the disclosure of anything to any of the following—

(a) the applicant to the Commission;

(b) the organisation concerned (if different);

(c) any person designated under paragraph 6 of Schedule 3 to the Terrorism Act 2000 to conduct the proceedings on behalf of that organisation;

(d) any person who—

(i) represents that appellant or that organisation for the purposes of the proceedings, and

(ii) does so otherwise than by virtue of an appointment under paragraph 7 of that Schedule.

Closed material proceedings

7 (1) Section 42(1) does not apply in relation to any section 6 proceedings within the meaning given by section 14(1) of the Justice and Security Act 2013 (certain civil proceedings in which closed material applications may be made).

(2) But nothing in sub-paragraph (1) authorises a prohibited section 6 disclosure.

(3) In the case of section 6 proceedings where the only relevant person is the Secretary of State, a "prohibited section 6 disclosure" means a disclosure of anything to—

(a) any person, other than the Secretary of State, who is or was a party to the proceedings, or

(b) any person who—

(i) represents such a person for the purposes of the proceedings, and

(ii) does so otherwise than by virtue of appointment as a special advocate.

(4) In the case of section 6 proceedings where the Secretary of State is not the only relevant person, or is not a relevant person but is a party to the proceedings, a "prohibited section 6 disclosure" means a disclosure of anything to—

(a) any person, other than the relevant person concerned or the Secretary of State, who is or was a party to the proceedings, or

(b) any person who—

(i) represents a person within paragraph (a) for the purposes of the proceedings, and

(ii) does so otherwise than by virtue of appointment as a special advocate.

(5) In this paragraph "relevant person", in relation to section 6 proceedings, has the meaning given by section 14(1) of the Justice and Security Act 2013.

TPIM proceedings

8 (1) Section 42(1) does not apply in relation to—

(a) any TPIM proceedings, or

(b) any proceedings arising out of any TPIM proceedings.

(2) But nothing in sub-paragraph (1) authorises the disclosure of anything to—
  (a) any person, other than the Secretary of State, who is or was a party to the proceedings, or
  (b) any person who—
    (i) represents such a person for the purposes of the proceedings, and
    (ii) does so otherwise than by virtue of appointment as a special advocate under Schedule 4 to the Terrorism Prevention and Investigation Measures Act 2011.

(3) In this paragraph "TPIM proceedings" has the same meaning as in the Terrorism Prevention and Investigation Measures Act 2011.

TEO proceedings

9 (1) Section 42(1) does not apply in relation to—
  (a) any TEO proceedings, or
  (b) any proceedings arising out of any TEO proceedings.

(2) But nothing in sub-paragraph (1) authorises the disclosure of anything to—
  (a) any person, other than the Secretary of State, who is or was a party to the proceedings, or
  (b) any person who—
    (i) represents such a person for the purposes of the proceedings, and
    (ii) does so otherwise than by virtue of appointment as a special advocate under Schedule 3 to the Counter-Terrorism and Security Act 2015.

(3) In this paragraph "TEO proceedings" has the meaning given by paragraph 1 of Schedule 3 to the Counter-Terrorism and Security Act 2015 (temporary exclusion orders: proceedings).

Proceedings relating to freezing of terrorist assets etc.

10 (1) Section 42(1) does not apply in relation to—
  (a) any financial restrictions proceedings, or
  (b) any proceedings arising out of such proceedings.

(2) In this paragraph "financial restrictions proceedings" has the meaning given by section 65 of the Counter-Terrorism Act 2008.

11 Section 42(1) does not apply in relation to any proceedings—
  (a) on an appeal under section 26, or an application under section 27, of the Terrorist Asset-Freezing etc Act 2010 (appeals and reviews by the court), or
  (b) on a claim arising from any matter to which such an appeal or application relates,

or any proceedings arising out of such proceedings.

12 But nothing in paragraph 10 or 11 authorises the disclosure of anything to—
  (a) any person, other than the Treasury, who is or was a party to the proceedings, or
  (b) any person who—

(i) represents such a person for the purposes of the proceedings, and

(ii) does so otherwise than by virtue of appointment as a special advocate.

Proceedings relating to release of prisoners etc. in Northern Ireland

13 (1) Section 42(1) does not apply in relation to—

(a) any proceedings before—

(i) the Parole Commissioners for Northern Ireland, or

(ii) any Sentence Review Commissioners appointed under section 1 of the Northern Ireland (Sentences) Act 1998, or

(b) any proceedings arising out of such proceedings.

(2) But nothing in sub-paragraph (1) authorises the disclosure of anything to—

(a) any person, other than the Secretary of State, who is or was a party to the proceedings, or

(b) any person who—

(i) represents such a person for the purposes of the proceedings, and

(ii) does so otherwise than by virtue of appointment as a special advocate.

Employment or industrial tribunal proceedings

14 (1) Section 42(1) does not apply in relation to any proceedings before an employment tribunal where the applicant, or the applicant's representatives, are excluded for all or part of the proceedings pursuant to—

(a) a direction to the tribunal by virtue of section 10(5)(b) or (c) of the Employment Tribunals Act 1996 (exclusion from Crown employment proceedings by direction of Minister in interests of national security), or

(b) a determination of the tribunal by virtue of section 10(6) of that Act (determination by tribunal in interests of national security).

(2) Section 42(1) does not apply in relation to any proceedings before an industrial tribunal in Northern Ireland where the applicant, or the applicant's representatives, are excluded for all or part of the proceedings pursuant to—

(a) a direction to the tribunal by virtue of Article 12(5)(b) or (c) of the Industrial Tribunals (Northern Ireland) Order 1996 (S.I. 1996/1921 (N.I. 18)) (exclusion from Crown employment proceedings by direction of Minister in interests of national security), or

(b) a determination of the tribunal by virtue of Article 12(6) of that Order (determination by tribunal in interests of national security).

(3) Section 42(1) does not apply in relation to any proceedings arising out of proceedings within sub-paragraph (1) or (2).

15 But nothing in paragraph 14 authorises the disclosure of anything to—

(a) the person who is or was the applicant in the proceedings before the employment or industrial tribunal, or

(b) any person who—

(i) represents that person for the purposes of any proceedings within paragraph 14, and

(ii) does so otherwise than by virtue of appointment as a special advocate.

Proceedings relating to dismissal for certain offences

16 Section 42(1) does not prohibit anything done in, for the purposes of, or in connection with, so much of any legal proceedings as relates to the fairness or unfairness of a dismissal on the grounds of any conduct constituting—

(a) an offence under section 2(1), 31(7) or 44,

(b) an offence under section 1(1) or (2), 11(7) or 19 of the Regulation of Investigatory Powers Act 2000, or

(c) an offence under section 1 of the Interception of Communications Act 1985.

Proceedings on appeals relating to claims of discrimination in Northern Ireland

17 (1) Section 42(1) does not apply in relation to any proceedings on an appeal under Article 80(2) of the Fair Employment and Treatment (Northern Ireland) Order 1998 (S.I. 1998/3162 (N.I. 21)) where—

(a) the appeal relates to a claim of discrimination in contravention of Part 3 of that Order (employment cases) and to a certificate of the Secretary of State that the act concerned was justified for the purpose of safeguarding national security, and

(b) a party to the appeal, or the party's representatives, are excluded for all or part of the proceedings by virtue of section 91(4)(b) of the Northern Ireland Act 1998.

(2) Section 42(1) does not apply in relation to any proceedings arising out of proceedings within sub-paragraph (1).

18 But nothing in paragraph 17 authorises the disclosure of anything to—

(a) any person who is or was excluded from all or part of the proceedings mentioned in paragraph 17(1), or

(b) any person who—

(i) represents that person for the purposes of any proceedings within paragraph 17, and

(ii) does so otherwise than by virtue of appointment as a special advocate.

Civil proceedings under section 31

19 Section 42(1) does not apply in relation to any civil proceedings under section 31(8) (enforcement of duty of operators to assist with implementation of warrants).

Proceedings for certain offences

20 (1) Section 42(1) does not apply in relation to any proceedings for a relevant offence.

(2) "Relevant offence" means—

(a) an offence under any provision of this Act;

(b) an offence under section 1 of the Interception of Communications Act 1985;

(c) an offence under any provision of the Regulation of Investigatory Powers Act 2000;

(d) an offence under section 47 or 48 of the Wireless Telegraphy Act 2006;

(e) an offence under section 83 or 84 of the Postal Services Act 2000;

(f) an offence under section 4 of the Official Secrets Act 1989 relating to any such information, document or article as is mentioned in subsection (3)(a) of that section;

(g) an offence under section 1 or 2 of the Official Secrets Act 1911 relating to any sketch, plan, model, article, note, document or information which—

(i) incorporates, or relates to, the content of any intercepted communication or any related communications data, or

(ii) tends to suggest that any interception-related conduct has or may have occurred or may be going to occur;

(h) an offence of perjury committed in the course of any relevant proceedings;

(i) an offence of attempting or conspiring to commit an offence falling within any of paragraphs (a) to (h);

(j) an offence under Part 2 of the Serious Crime Act 2007 in relation to an offence falling within any of those paragraphs;

(k) an offence of aiding, abetting, counselling or procuring the commission of an offence falling within any of those paragraphs;

(l) contempt of court committed in the course of, or in relation to, any relevant proceedings.

(3) In this paragraph—

"intercepted communication" and "interception-related conduct" have the same meaning as in section 42;

"relevant proceedings" means any proceedings mentioned in paragraphs 4 to 19.

Disclosures to prosecutors, judges etc.

21 (1) Nothing in section 42(1) prohibits—

(a) a disclosure to a person ("P") conducting a criminal prosecution that is made for the purpose only of enabling P to determine what is required of P by P's duty to secure the fairness of the prosecution,

(b) a disclosure to a relevant judge in a case in which the judge has ordered the disclosure to be made to the judge alone, or

(c) a disclosure to the panel of an inquiry held under the Inquiries Act 2005, or to a person appointed as counsel to such an inquiry, where, in the course of the inquiry, the panel has ordered the disclosure to be made to the panel alone or (as the case may be) to the panel and the person appointed as counsel to the inquiry.

(2) A relevant judge may order a disclosure under sub-paragraph (1)(b) only if the judge considers that the exceptional circumstances of the case make the disclosure essential in the interests of justice.

(3) The panel of an inquiry may order a disclosure under sub-paragraph (1)(c) only if it considers that the exceptional circumstances of the case make the disclosure essential to enable the inquiry to fulfil its terms of reference.

(4) Where in any criminal proceedings—

(a) a relevant judge orders a disclosure under sub-paragraph (1)(b), and

(b) in consequence of that disclosure, the judge considers that there are exceptional circumstances requiring the judge to make a direction under this sub-paragraph,

the judge may direct the person conducting the prosecution to make for the purposes of the proceedings any admission of fact which the judge considers essential in the interests of justice.

(5) But nothing in any direction under sub-paragraph (4) may authorise or require anything to be done in contravention of section 42(1).

(6) In this section "relevant judge" means—

(a) any judge of the High Court or of the Crown Court or any Circuit judge,

(b) any judge of the High Court of Justiciary or any sheriff,

(c) in relation to proceedings before the Court Martial, the judge advocate for those proceedings, or

(d) any person holding a judicial office that entitles the person to exercise the jurisdiction of a judge falling within paragraph (a) or (b).

SCHEDULE 4

Section 54(1)

RELEVANT PUBLIC AUTHORITIES AND DESIGNATED SENIOR OFFICERS

PART 1

TABLE OF AUTHORITIES AND OFFICERS

Table

(1) Relevant public authority	*(2) DSO: minimum office, rank or position*	*(3) Type of communications data that may be obtained by DSO*	*(4) Paragraphs of section 46(7) specified for DSO*
Police force maintained under section 2 of the Police Act 1996	Inspector	Entity data	(a), (b), (c), (d), (e), (g) and (i)
	Superintendent	All	(a), (b), (c), (d), (e), (g) and (i)
Metropolitan police force	Inspector	Entity data	(a), (b), (c), (d), (e), (g) and (i)
	Superintendent	All	(a), (b), (c), (d), (e), (g) and (i)

(1) *Relevant public authority*	*(2)* *DSO: minimum office, rank or position*	*(3)* *Type of communications data that may be obtained by DSO*	*(4)* *Paragraphs of section 46(7) specified for DSO*
City of London police force	Inspector	Entity data	(a), (b), (c), (d), (e), (g) and (i)
	Superintendent	All	(a), (b), (c), (d), (e), (g) and (i)
Police Service of Scotland	Inspector	Entity data	(a), (b), (c), (d), (e), (g) and (i)
	Superintendent	All	(a), (b), (c), (d), (e), (g) and (i)
Police Service of Northern Ireland	Inspector	Entity data	(a), (b), (c), (d), (e), (g) and (i)
	Superintendent	All	(a), (b), (c), (d), (e), (g) and (i)
British Transport Police Force	Inspector	Entity data	(a), (b), (c), (d), (e), (g) and (i)
	Superintendent	All	(a), (b), (c), (d), (e), (g) and (i)
Ministry of Defence Police	Inspector	Entity data	(a), (b), (c) and (g)
	Superintendent	All	(a), (b), (c) and (g)
Royal Navy Police	Lieutenant Commander	Entity data	(a), (b), (c) and (g)
	Commander	All	(a), (b), (c) and (g)
Royal Military Police	Major	Entity data	(a), (b), (c) and (g)
	Lieutenant Colonel	All	(a), (b), (c) and (g)
Royal Air Force Police	Squadron Leader	Entity data	(a), (b), (c) and (g)
	Wing Commander	All	(a), (b), (c) and (g)
Security Service	General Duties 4 or any other level 4 officer	Entity data	(a), (b) and (c)
	General Duties 3 or any other level 3 officer	All	(a), (b) and (c)
Secret Intelligence Service	Grade 6	All	(a), (b) and (c)
GCHQ	GC8	All	(a), (b) and (c)
Ministry of Defence	Member of the Senior Civil Service or equivalent	All	(a)
Department of Health	Grade 7 in the Medicines and Healthcare Products Regulatory Agency	All	(b), (d) and (e)
	Grade 7 in the Anti-Fraud Unit	All	(b)

(1) *Relevant public authority*	*(2)* *DSO: minimum office, rank or position*	*(3)* *Type of communications data that may be obtained by DSO*	*(4)* *Paragraphs of section 46(7) specified for DSO*
Home Office	Immigration inspector or equivalent with responsibility for investigations or other functions relating to immigration and border security	All	(b)
	Immigration inspector or equivalent with responsibility for anti-corruption in relation to investigations or other functions relating to immigration and border security	All	(b)
	Immigration inspector or equivalent with responsibility for asylum fraud investigations	All	(b)
	Immigration inspector or equivalent with responsibility for security and intelligence in the immigration detention estate	All	(b), (d) and (i)
Ministry of Justice	Manager in the security group of the National Offender Management Service responsible for intelligence	Entity data	(b) and (d)
	Senior manager in the security group of the National Offender Management Service responsible for intelligence	All	(b) and (d)
National Crime Agency	Grade 3	Entity data	(b), (g) and (i)
	Grade 2	All	(b), (g) and (i)
Northern Ireland Office	Governor 4 in the Northern Ireland Prison Service	All	(b), (d) and (i)
Her Majesty's Revenue and Customs	Higher officer	Entity data	(b) and (f)
	Senior officer	All	(b) and (f)
Department for Transport	Enforcement Officer in Maritime and Coastguard Agency	Entity data	(b) and (d)
	Head of Enforcement in Maritime and Coastguard Agency	All	(b) and (d)
	Maritime Operations Commander (grade 7) in the Maritime and Coastguard Agency	All	(g)
	Principal Inspector in the Air Accident Investigation Branch, the Marine Accident Investigation Branch or the Rail Accident Investigation Branch	All	(d)

(1) *Relevant public authority*	*(2)* *DSO: minimum office, rank or position*	*(3)* *Type of communications data that may be obtained by DSO*	*(4)* *Paragraphs of section 46(7) specified for DSO*
Department for Work and Pensions	Senior Executive Officer in Fraud and Error Services	All	(b)
	Senior Executive Officer in the Child Maintenance Group Central Legal Services	All	(b)
Common Services Agency for the Scottish Health Service	Head of Counter Fraud Services	All	(b)
Competition and Markets Authority	Member of the Senior Civil Service with responsibility for cartels and criminal enforcement	All	(b)
Criminal Cases Review Commission	Investigations Adviser	All	(h)
Department of Enterprise, Trade and Investment in Northern Ireland	Deputy chief inspector in trading standards services	All	(b)
Financial Conduct Authority	Head of department in the Enforcement and Market Oversight Division	All	(b) and (j)
A fire and rescue authority under the Fire and Rescue Services Act 2004	Watch Manager (Control)	All	(g)
Food Standards Agency	Grade 6 in the National Food Crime Unit	All	(b)
Gambling Commission	Senior manager	All	(b)
Gangmasters Licensing Authority	Head of operations	All	(b)
Health and Safety Executive	Band 1 inspector	All	(b), (d) and (e)
Independent Police Complaints Commission	Deputy Chair or Director	All	(b) and (i)
Information Commissioner	Group Manager	Entity data	(b)
	Head of enforcement or an equivalent grade	All	(b)
National Health Service Business Services Authority	Senior manager (of pay band 8b) in the Counter Fraud and Security Management Services Division	All	(b)
A National Health Service Trust established under section 5 of the National Health Service and Community Care Act 1990 whose functions, as specified in its establishment order, include the provision of emergency ambulance services	Director of Operations or Control and Communications Manager	All	(b)
	Duty Manager of Ambulance Trust Control Rooms	All	(g)
Northern Ireland Ambulance Service Health and Social Care Trust	Watch Manager (Control)	All	(g)

(1) Relevant public authority	*(2) DSO: minimum office, rank or position*	*(3) Type of communications data that may be obtained by DSO*	*(4) Paragraphs of section 46(7) specified for DSO*
Northern Ireland Fire and Rescue Service Board	Group Manager (Control)	All	(b) and (d)
	Watch Manager (Control)	All	(g)
Northern Ireland Health and Social Care Regional Business Services Organisation	Assistant Director Counter Fraud and Probity Services	All	(b)
Office of Communications	Senior associate	All	(b)
Office of the Police Ombudsman for Northern Ireland	Senior investigating officer	All	(b)
Police Investigations and Review Commissioner	Commissioner or Director of Investigations	All	(b) and (i)
Scottish Ambulance Service Board	Watch Manager (Control)	All	(g)
Scottish Criminal Cases Review Commission	Investigations Adviser	All	(h)
Serious Fraud Office	Grade 6	All	(b)
Welsh Ambulance Services National Health Service Trust	Watch Manager (Control)	All	(g)

PART 2

INTERPRETATION OF TABLE

Interpretation

1 In the table in Part 1 of this Schedule "entity data" means any communications data which is entity data.

SCHEDULE 5

Section 67(5)

TRANSFER AND AGENCY ARRANGEMENTS WITH PUBLIC AUTHORITIES: FURTHER PROVISIONS

Particular safeguards in connection with operation of section 53

1 (1) The following provisions apply where the functions of the Secretary of State under section 51 are exercisable by a public authority by virtue of regulations under section 67(1).

(2) The measures adopted or arrangements made by the public authority for the purpose of complying with the requirements of section 53 must be such as are approved by the Secretary of State.

(3) Any report required by section 53(6)(b) or (8) must be made to the Secretary of State as well as to the Investigatory Powers Commissioner.

Requirement for public authority to provide reports to Secretary of State

2 (1) A public authority, when exercising functions by virtue of regulations under section 67(1), must at least once in each calendar year make a report to the Secretary of State on—

(a) the discharge of the functions, and

(b) such other matters as the Secretary of State may by regulations require.

(2) Regulations under section 67(1) may, in particular, modify sub-paragraph (1) as it has effect in relation to the calendar year in which the regulations come into force or are revoked.

(3) The Secretary of State may agree to a report under this paragraph being combined with any other report which the public authority concerned is required to, or may, make to the Secretary of State.

Transfer schemes in connection with transfer of functions

3 (1) The Secretary of State may, in connection with regulations under section 67(1), make a scheme for the transfer of property, rights or liabilities.

(2) The things that may be transferred under a transfer scheme include—

(a) property, rights and liabilities which could not otherwise be transferred,

(b) property acquired, and rights and liabilities arising, after the making of the scheme.

(3) A transfer scheme may make consequential, supplementary, incidental, transitional, transitory or saving provision and may, in particular—

(a) create rights, or impose liabilities, in relation to property or rights transferred,

(b) make provision about the continuing effect of things done by, on behalf of or in relation to the transferor in respect of anything transferred,

(c) make provision about the continuation of things (including legal proceedings) in the process of being done by, on behalf of or in relation to the transferor in respect of anything transferred,

(d) make provision for references to the transferor in an instrument or other document in respect of anything transferred to be treated as references to the transferee,

(e) make provision for the shared ownership or use of property,

(f) if the TUPE regulations do not apply in relation to the transfer, make provision which is the same or similar.

(4) A transfer scheme may provide—

(a) for modification by agreement,

(b) for modifications to have effect from the date when the original scheme came into effect.

(5) A transfer scheme may confer a discretion on the Secretary of State to pay compensation to any person whose interests are adversely affected by the scheme.

(6) A transfer scheme may be included in regulations under section 67(1) but, if not so included, must be laid before Parliament after being made.

(7) For the purposes of this paragraph references to rights and liabilities include references to—

(a) rights and liabilities relating to a contract of employment, and

(b) rights and liabilities of the Crown relating to the terms of employment of individuals in the civil service.

(8) Accordingly, a transfer scheme may, in particular, provide—

(a) for—

(i) an individual employed in the civil service to become an employee of the transferee, or

(ii) an employee of the transferor to become an employee of the transferee or an individual employed in the civil service,

(b) for—

(i) the individual's terms of employment in the civil service to have effect (subject to any necessary modifications) as the terms of the individual's contract of employment with the transferee, or

(ii) (as the case may be) the individual's contract of employment to have effect (subject to any necessary modifications) as the terms of the individual's contract of employment with the transferee or, where the transferee is the Secretary of State, the individual's terms of employment with the civil service,

(c) for the transfer of rights and liabilities of the Crown or another public authority under or in connection with the individual's terms of employment.

(9) In this paragraph—

"civil service" means the civil service of the State,

"TUPE regulations" means the Transfer of Undertakings (Protection of Employment) Regulations 2006 (S.I. 2006/246),

and references to the transfer of property include the grant of a lease.

Tax in connection with transfer schemes

4 (1) The Treasury may by regulations make provision varying the way in which a relevant tax has effect in relation to—

(a) anything transferred under a transfer scheme, or

(b) anything done for the purposes of, or in relation to, a transfer under a transfer scheme.

(2) The provision which may be made under sub-paragraph (1)(a) includes, in particular, provision for—

(a) a tax provision not to apply, or to apply with modifications, in relation to anything transferred,

(b) anything transferred to be treated in a specified way for the purposes of a tax provision,

(c) the Secretary of State to be required or permitted to determine, or specify the method for determining, anything which needs to be determined for the purposes of any tax provision so far as relating to anything transferred.

(3) The provision which may be made under sub-paragraph (1)(b) includes, in particular, provision for—

(a) a tax provision not to apply, or to apply with modifications, in relation to anything done for the purposes of, or in relation to, the transfer,

(b) anything done for the purposes of, or in relation to, the transfer to have or not have a specified consequence or be treated in a specified way,

(c) the Secretary of State to be required or permitted to determine, or specify the method for determining, anything which needs to be determined for the purposes of any tax provision so far as relating to anything done for the purposes of, or in relation to, the transfer.

(4) In this paragraph—

"relevant tax" means income tax, corporation tax, capital gains tax, stamp duty, stamp duty reserve tax or stamp duty land tax,

"tax provision" means any provision—

(a) about a relevant tax, and

(b) made by an enactment,

"transfer scheme" means a transfer scheme under paragraph 3,

and references to the transfer of property include the grant of a lease.

Supplementary and other general provision

5 The power to make regulations under section 67(1) includes, in particular, power to—

(a) modify any enactment about a public authority for the purpose of enabling or otherwise facilitating any function under sections 51 to 53 to be exercisable by the public authority,

(b) impose requirements or confer other functions on a public authority in connection with functions transferred by the regulations.

6 The power to make regulations under—

(a) section 67, or

(b) paragraph 4 above,

including that power as extended (whether by section 197(1) or otherwise) may, in particular, be exercised by modifying any enactment (including this Act).

SCHEDULE 6

Section 179

CODES OF PRACTICE

Scope of codes

1 (1) The Secretary of State must issue one or more codes of practice about the exercise of functions conferred by virtue of this Act.

(2) Sub-paragraph (1) does not apply in relation to any functions conferred by virtue of this Act on—

(a) the Investigatory Powers Commissioner or any other Judicial Commissioner,

(b) the Information Commissioner,
(c) the Investigatory Powers Tribunal,
(d) any other court or tribunal,
(e) the Technical Advisory Board,
(f) the Scottish Ministers, or
(g) the Secretary of State or the Treasury.

(3) A code of practice may, in particular, contain provision about the training of people who may exercise functions within sub-paragraph (1).

2 (1) A code of practice about the exercise of functions conferred by virtue of Part 2 must contain provision about the making of requests ("relevant overseas requests") for intercepted material or related communications data that has been obtained by an overseas authority by means of any interception carried out at the request of an intercepting authority.

(2) Such provision must, in particular, include provision about—
(a) the process to be followed before making a relevant overseas request;
(b) the handling of intercepted material or related communications data obtained as a result of such a request.

(3) In this paragraph—
"intercepted material", in relation to an interception, means the content of any communications intercepted by the interception;
"intercepting authority" has the same meaning as in Part 2 (see section 15);
"interception" means the interception of communications in the course of their transmission by means of a postal service or telecommunication system;
"overseas authority" means an authority of a country or territory outside the United Kingdom;
"related communications data" has the meaning given by section 12(6).

3 (1) A code of practice about the exercise of functions conferred by virtue of Part 3 must contain provision about communications data held by public authorities by virtue of that Part.

(2) Such provision must, in particular, include provision about—
(a) why, how and where the data is held,
(b) who may access the data on behalf of the authority,
(c) with whom, and under what conditions, the data may be disclosed,
(d) the processing of the data for purposes otherwise than in connection with the purposes for which it was obtained or retained,
(e) the processing of the data together with other data,
(f) the processes for determining how long the data should be held and for the destruction of the data.

4 (1) A code of practice about the obtaining or holding of communications data by virtue of Part 3 must include—
(a) provision designed to protect the public interest in the confidentiality of sources of journalistic information, and
(b) provision about particular considerations applicable to any data which relates to a member of a profession which routinely holds legally privileged information or relevant confidential information.

(2) In this paragraph—

"legally privileged information" means information with respect to which a claim to legal professional privilege (in Scotland, to confidentiality of communications) could be maintained in legal proceedings,

"relevant confidential information" means information which is held in confidence by a member of a profession and consists of—

(a) personal records or journalistic material which are (or would be if held in England and Wales) excluded material as defined by section 11 of the Police and Criminal Evidence Act 1984,

(b) banking records, or

(c) communications between Members of Parliament and their constituents,

and the references in this paragraph to a member of a profession include references to any person acting in the course of any trade, business, profession or other occupation or for the purposes of any paid or unpaid office.

Procedural requirements

5 (1) Before issuing a code the Secretary of State must—

(a) prepare and publish a draft of the code, and

(b) consider any representations made about it,

and may modify the draft.

(2) The Secretary of State must, in particular, consult the Investigatory Powers Commissioner.

(3) A code comes into force in accordance with regulations made by the Secretary of State.

(4) A statutory instrument containing such regulations may not be made unless a draft of the instrument has been laid before, and approved by a resolution of, each House.

(5) When a draft instrument is laid, the code to which it relates must also be laid.

(6) No draft instrument may be laid until the consultation required by sub-paragraphs (1) and (2) has taken place.

Revision of codes

6 (1) The Secretary of State may from time to time revise the whole or part of a code.

(2) Before issuing any revision of a code the Secretary of State must—

(a) prepare and publish a draft, and

(b) consider any representations made about it,

and may modify the draft.

(3) The Secretary of State must, in particular, consult the Investigatory Powers Commissioner.

(4) A revision of a code comes into force in accordance with regulations made by the Secretary of State.

(5) A statutory instrument containing such regulations must be laid before Parliament if the regulations have been made without a draft having been so laid and approved by a resolution of each House of Parliament.

(6) When an instrument or draft instrument is laid, the revision of a code to which it relates must also be laid.

(7) No instrument or draft instrument may be laid until the consultation required by sub-paragraphs (2) and (3) has taken place.

Effect of codes

7 (1) A person must have regard to a code when exercising any functions to which the code relates.

(2) A failure on the part of a person to comply with any provision of a code does not of itself make that person liable to criminal or civil proceedings.

(3) A code is admissible in evidence in any such proceedings.

(4) A court or tribunal may, in particular, take into account a failure by a person to have regard to a code in determining a question in any such proceedings.

(5) A supervisory authority exercising functions by virtue of this Act may take into account a failure by a person to have regard to a code in determining a question which arises in connection with the exercise of those functions.

(6) In this paragraph "supervisory authority" means—

(a) the Investigatory Powers Commissioner or any other Judicial Commissioner,

(b) the Information Commissioner, or

(c) the Investigatory Powers Tribunal.

Interpretation

8 In paragraphs 6 and 7 "a code" means a code issued under paragraph 1 (as revised from time to time).

SCHEDULE 7

Section 184

COMBINATION OF WARRANTS

PART 1

COMBINATIONS WITH TARGETED INTERCEPTION WARRANTS

The intelligence services

1 The Secretary of State may, on an application made by or on behalf of the head of an intelligence service, issue a warrant, addressed to the head of the service, that combines a targeted interception warrant that the Secretary of State has power to issue under section 14(1) with one or more of the following—

(a) a targeted equipment interference warrant that the Secretary of State has power to issue under section 84;

(b) a targeted examination warrant that the Secretary of State has power to issue under section 14(2) or 84(3);

(c) an authorisation under section 28 of the Regulation of Investigatory Powers Act 2000 (authorisation of directed surveillance);

(d) an authorisation under section 32 of that Act (authorisation of intrusive surveillance);

(e) a warrant under section 5 of the Intelligence Services Act 1994 (warrants for entry or interference with property or wireless telegraphy).

2 The Scottish Ministers may, on an application made by or on behalf of the head of an intelligence service, issue a warrant, addressed to the head of the service, that combines a targeted interception warrant that the Scottish Ministers have power to issue under section 17(1) with one or more of the following—

(a) a targeted equipment interference warrant that the Scottish Ministers have power to issue under section 86;

(b) a targeted examination warrant that the Scottish Ministers have power to issue under section 17(2);

(c) an authorisation under section 6 of the Regulation of Investigatory Powers (Scotland) Act 2000 (asp 11) (authorisation of directed surveillance);

(d) an authorisation under section 10 of that Act (authorisation of intrusive surveillance).

3 The Secretary of State may, on an application made by or on behalf of the Chief of Defence Intelligence, issue a warrant, addressed to the Chief, that combines a targeted interception warrant that the Secretary of State has power to issue under section 14(1) with a targeted equipment interference warrant that the Secretary of State has power to issue under section 87.

Law enforcement agencies

4 (1) The Secretary of State may, on an application made by or on behalf of a relevant intercepting authority, issue a warrant, addressed to the authority, that combines a targeted interception warrant that the Secretary of State has power to issue under section 14(1) with one or more of the following—

(a) a targeted equipment interference warrant that a law enforcement chief has power to issue under section 89;

(b) an authorisation under section 28 of the Regulation of Investigatory Powers Act 2000 (authorisation of directed surveillance);

(c) an authorisation under section 32 of that Act (authorisation of intrusive surveillance);

(d) an authorisation under section 93 of the Police Act 1997 (authorisations to interfere with property).

(2) For the purposes of sub-paragraph (1), each of the following is a "relevant intercepting authority"—

(a) the Director General of the National Crime Agency;

(b) the Commissioner of Police of the Metropolis;

(c) the Chief Constable of the Police Service of Northern Ireland;

(d) the chief constable of the Police Service of Scotland;

(e) the Commissioners for Her Majesty's Revenue and Customs.

PART 2

OTHER COMBINATIONS

The intelligence services

5 The Secretary of State may, on an application made by or on behalf of the head of an intelligence service, issue a warrant, addressed to the head of the service, that combines a targeted equipment interference warrant that the Secretary of State has power to issue under section 84(1) with one of more of the following—

(a) a targeted examination warrant that the Secretary of State has power to issue under section 84(3);

(b) an authorisation under section 28 of the Regulation of Investigatory Powers Act 2000 (authorisation of directed surveillance);

(c) an authorisation under section 32 of that Act (authorisation of intrusive surveillance);

(d) a warrant under section 5 of the Intelligence Services Act 1994 (warrants for entry or interference with property or wireless telegraphy).

6 The Scottish Ministers may, on an application made by or on behalf of the head of an intelligence service, issue a warrant, addressed to the head of the service, that combines a targeted equipment interference warrant that the Scottish Ministers have power to issue under section 86 with one or more of the following—

(a) an authorisation under section 6 of the Regulation of Investigatory Powers (Scotland) Act 2000 (asp 11) (authorisation of directed surveillance);

(b) an authorisation under section 10 of that Act (authorisation of intrusive surveillance).

Law enforcement agencies

7 (1) A law enforcement chief may, on the application of an appropriate law enforcement officer, issue a warrant, addressed to the officer, that combines a targeted equipment interference warrant that the law enforcement chief has power to issue under section 89 with either or both of the following—

(a) an authorisation under section 28 of the Regulation of Investigatory Powers Act 2000 (authorisation of directed surveillance);

(b) an authorisation under section 32 of that Act (authorisation of intrusive surveillance);

(c) an authorisation under section 93 of the Police Act 1997 (authorisations to interfere with property).

(2) For the purposes of this paragraph, references to a "law enforcement chief" and "appropriate law enforcement officer" are to be read in accordance with section 89(3).

PART 3

GENERAL

Interpretation of Part 3

8 In this Part of this Schedule—

a "combined warrant" means a warrant issued under Part 1 or 2 of this Schedule;

"procedural rules" (in relation to a warrant) means the law about any of the following matters—

(a) the involvement of Judicial Commissioners in decisions;

(b) delegation of decisions;

(c) the signing of warrants;

(d) urgent cases.

Rules applying separately in relation to each part of a combined warrant

9 The law about the following matters, so far as relating to a warrant or other authorisation that may be included in a combined warrant, applies in relation to the part of a combined warrant that contains the warrant or other authorisation—

(a) the grounds on which the warrant or authorisation may be issued or given;

(b) the conduct that may be authorised by the warrant or authorisation;

(c) any requirements as to what must be included in the warrant or authorisation;

(d) the grounds on which the warrant or authorisation may be renewed;

(e) the grounds on which the warrant or authorisation may be modified and the procedural rules that apply to the modification;

(f) the circumstances in which the warrant or authorisation may or must be cancelled.

Modification of rules as to who may issue etc

10 (1) Where Part 1 or 2 provides for a person to have power to issue a combined warrant, the person may issue a combined warrant containing any warrant or authorisation that may be included in it, whether or not that person would have power to issue that warrant, or to give that authorisation, as a single instrument.

(2) Where Part 1 or 2 provides for a person to have power to apply for a combined warrant, the person may apply for a combined warrant containing any warrant or authorisation that may be included in it, provided that—

(a) the person could apply for that warrant or authorisation as a single instrument, or

(b) the organisation on whose behalf the person is acting, or another person who is a member of staff or an officer of the organisation or who is otherwise acting on its behalf, could apply for that warrant or authorisation as a single instrument.

Modification of rules as to duration

11 Where a combined warrant includes warrants or authorisations which (as single instruments) would cease to have effect at the end of different periods, the combined warrant is to cease to have effect at the end of the shortest of the periods (unless renewed).

Modification of procedural rules as to issue etc

12 (1) A combined warrant under paragraph 1 or 2 addressed to the head of an intelligence service, or a combined warrant under paragraph 3 addressed to the Chief of Defence Intelligence, may only be issued, renewed or cancelled in accordance with the procedural rules that would apply to the issue, renewal or cancellation of a targeted interception warrant addressed to the head of the service or (as the case may be) to the Chief of Defence Intelligence (see Chapter 1 of Part 2).

(2) A combined warrant under paragraph 4 addressed to a relevant intercepting authority may only be issued, renewed or cancelled in accordance with the procedural rules that would apply to the issue, renewal or cancellation of a targeted interception warrant addressed to the authority (see Chapter 1 of Part 2).

(3) However, if a combined warrant under paragraph 1 includes a warrant under section 5 of the Intelligence Services Act 1994, any requirement (arising from sub-paragraph (1)) for the involvement of Judicial Commissioners in the decision whether to issue or renew the combined warrant does not apply in relation to the part of the combined warrant that contains the warrant under section 5.

13 (1) A combined warrant under paragraph 5 or 6 addressed to the head of an intelligence service, or a combined warrant under paragraph 7 addressed to the Chief of Defence Intelligence, may only be issued, renewed or cancelled in accordance with the procedural rules that would apply to the issue, renewal or cancellation of a targeted equipment interference warrant addressed to the head of the service or (as the case may be) to the Chief of Defence Intelligence (see Part 5).

(2) A combined warrant under paragraph 8 addressed to a law enforcement officer may only be issued, renewed or cancelled in accordance with the procedural rules that would apply to the issue, renewal or cancellation of a targeted equipment interference warrant addressed to the officer (see Part 5).

(3) However, if a combined warrant under paragraph 5 includes a warrant under section 5 of the Intelligence Services Act 1994, any requirement (arising from sub-paragraph (1)) for the involvement of Judicial Commissioners in the decision whether to issue or renew the combined warrant does not apply in relation to the part of the combined warrant that contains the warrant under section 5.

SCHEDULE 8

Section 200(1)

TRANSITIONAL, TRANSITORY AND SAVING PROVISION

Lawful interception of communications

1 Any agreement which, immediately before the day on which section 7 comes into force, is designated for the purposes of section 1(4) of the Regulation of Investigatory Powers Act 2000 is to be treated, on and after that day, as designated as an international mutual assistance agreement by regulations under section 7 of this Act.

The Data Retention and Investigatory Powers Act 2014

2 (1) A retention notice under section 1 of the Data Retention and Investigatory Powers Act 2014 is to be treated, during the transitional period mentioned in sub-paragraph (2), as a retention notice under section 71 of this Act; and Part 4 of this Act is to be read accordingly in relation to that period.

(2) The transitional period mentioned in this sub-paragraph is the period of six months beginning with the day on which section 1(1) of the Data Retention and Investigatory Powers Act 2014 is repealed.

(3) The repeal of section 1(7) of the Act of 2014 does not affect the continued operation, during the transitional period mentioned in sub-paragraph (4), of regulations made under section 1(7) of that Act.

(4) The transitional period mentioned in this sub-paragraph is the period of six months beginning with the day on which section 1(7) of the Act of 2014 is repealed.

(5) In their continued operation by virtue of sub-paragraph (3), the regulations made under section 1(7) of the Act of 2014 have effect subject to such modifications (if any) as may be specified in regulations under section 200(2).

(6) The power to make regulations under section 200(2) includes power to make such transitional, transitory or saving provision as the Secretary of State considers appropriate in connection with the repeal of any provision by section 8(3) of the Act of 2014.

General savings

3 Nothing in any of the provisions of this Act by virtue of which conduct of any description is or may be authorised by any warrant, authorisation or notice, or by virtue of which information may be obtained in any manner, is to be read—

(a) as making it unlawful to engage in any conduct of that description which is not otherwise unlawful under this Act and would not be unlawful apart from this Act,

(b) as otherwise requiring—

(i) the issue, grant or giving of such a warrant, authorisation or notice, or

(ii) the taking of any step for or towards obtaining the authority of such a warrant, authorisation or notice,

before any such conduct of that description is engaged in, or

(c) as prejudicing any power to obtain information by any means not involving conduct that may be authorised under this Act.

4 Nothing in Part 3 or 4 of this Act affects any power conferred on a postal operator by or under any enactment to open, detain or delay any postal packet (within the meaning given by section 125(1) of the Postal Services Act 2000) or to deliver any such packet to a person other than the person to whom it is addressed.

SCHEDULE 9

Section 201(1)

MINOR AND CONSEQUENTIAL PROVISION

PART 1

MINOR AND CONSEQUENTIAL PROVISION: GENERAL

Telecommunications Act 1984

1 Section 94 of the Telecommunications Act 1984 (directions in the interests of national security etc.) is repealed.

Regulation of Investigatory Powers Act 2000

2 Part 1 of the Regulation of Investigatory Powers Act 2000 (interception of communications and acquisition and disclosure of communications data) is repealed.

3 In section 65(2) of that Act (the jurisdiction of the Investigatory Powers Tribunal), after paragraph (c) (but before the "and" at the end of the paragraph) insert—

"(ca) to consider and determine any reference to them by the Investigatory Powers Commissioner under section 171(6)(b) of the Investigatory Powers Act 2016;".

4 In section 67(1)(b) of that Act (exercise of the Tribunal's jurisdiction) for "or (c)" substitute ", (c) or (ca)".

5 In section 68(8) of that Act (Tribunal procedure) for the words from "the Interception" to the end substitute "the Investigatory Powers Commissioner or any other Judicial Commissioner".

Anti-terrorism, Crime and Security Act 2001

6 Part 11 of the Anti-terrorism, Crime and Security Act 2001 (retention of communications data) is repealed.

Data Retention and Investigatory Powers Act 2014

7 The Data Retention and Investigatory Powers Act 2014 is repealed.

PART 2

REPEALS AND REVOCATIONS CONSEQUENTIAL ON PART 1 OF THIS SCHEDULE

Title	*Extent of repeal or revocation*
Communications Act 2003	In Schedule 17, paragraph 70.
Serious Organised Crime and Police Act 2005	In Schedule 4, paragraph 135.
Serious Crime Act 2007	In Schedule 12, paragraphs 7 and 8.
Police, Public Order and Criminal Justice (Scotland) Act 2006 (Consequential Provisions and Modifications) Order 2007 (S.I. 2007/1098)	In the Schedule, paragraph 4(5).
Policing and Crime Act 2009	Section 7. In Schedule 7, paragraphs 13 and 14.
Protection of Freedoms Act 2012	Section 37. In Schedule 9, paragraphs 7 and 8.
Crime and Courts Act 2013	In Schedule 8, paragraph 81.
Police and Fire Reform (Scotland) Act 2012 (Consequential Provisions and Modifications) Order 2013 (S.I. 2013/602)	In Schedule 2, paragraph 33(5) to (8).
Counter-Terrorism and Security Act 2015	Section 21. Section 52(3)(a).

INVESTIGATORY POWERS BILL

EXPLANATORY NOTES

What these notes do

These Explanatory Notes relate to the Investigatory Powers Bill as published in Draft on 4 November 2015 (Cm 9152).

- These Explanatory Notes have been produced by the Home Office in order to assist the reader of the Bill and to help inform debate on it. They do not form part of the Bill and have not been endorsed by Parliament.
- These Explanatory Notes explain what each part of the Bill will mean in practice; provide background information on the development of policy; and provide additional information on how the Bill will affect existing legislation in this area.
- These Explanatory Notes might best be read alongside the Bill. They are not, and are not intended to be, a comprehensive description of the Bill. So where a provision of the Bill does not seem to require any explanation or comment, the Notes simply say in relation to it that the provision is self-explanatory.

Cm 9152–EN

Table of Contents

Overview of the Bill

1 The Investigatory Powers Bill will provide a clear framework for the use (by the security and intelligence agencies, law enforcement and other public authorities) of investigatory powers. These powers cover the interception of communications, the retention and acquisition of communications data, equipment interference for obtaining (private) data, and the security and intelligence agencies' acquisition of bulk personal datasets. It will not be lawful to exercise such powers other than as provided for by the Bill.

2 Section 7 of the Data Retention and Investigatory Powers Act 2014 required David Anderson QC, in his capacity as the Independent Reviewer of Terrorism Legislation, to conduct a review of existing laws relating to investigatory powers. This Bill responds to the recommendations made by the Independent Reviewer and those of the reviews undertaken by the Intelligence and Security Committee of Parliament (ISC) and the Panel of the Independent Surveillance Review convened by the Royal United Services Institute (RUSI). All three reviews agreed that existing powers remain essential in tackling the current and evolving threats to the United Kingdom.

Policy background

3 The Government is proposing legislation to replace the emergency legislation passed in July 2014, the Data Retention and Investigatory Powers Act 2014 (DRIPA), which falls away on 31 December 2016. This Act replaced the Data Retention (EC Directive) Regulations 2009 (S.I. 2009/859) following the European Court of Justice judgment of April 2014 which declared the Data Retention Directive invalid. During the passage of DRIPA, the Government committed to bring forward new legislation to provide public authorities with the investigatory powers and capabilities they need to address evolving threats within a changing communications environment, as well as providing the public with clarity and reassurance about how those powers and capabilities are used. The Investigatory Powers Bill will therefore modernise and update the legal framework governing the state's ability to acquire communications and data about communications. It will consolidate existing legislation and ensure the powers in the Bill are fit for the digital age.

4 The purpose of the Bill is threefold. First it will replace the existing statutory scheme with one that is comprehensive and comprehensible. It will govern all of the powers available to the state to access communications to provide a new statutory basis for these powers in a way that is clear about when and how public authorities acquire, store and access information. Second, this legislation will ensure consistent, effective statutory safeguards and will clarify which powers different public authorities can use and for what purposes. It will set out the statutory tests that must be met before a power may be used and will set out in detail the authorisation regime for each investigative tool. It will remove doubt or ambiguity about the sufficiency and efficacy of checks and balances and it will provide robust oversight arrangements. Finally, it will enhance communications data powers in order to reinstate capabilities that have been lost as a result of changes in the way people communicate.

5 This Bill is in nine parts.

6 Part 1 asserts the privacy of communications and provides for related offences. It defines interception and sets out the offences of unlawful interception and unlawful acquisition of communications data and the penalties for committing such offences. It also references the use of powers to acquire stored communications such as an email stored on a web-based server or a voicemail.

7 Part 2 provides for interception: acquiring the content of communications. This power is currently provided for under the Regulation of the Investigatory Powers Act 2000 (RIPA). The Bill will repeal and replace the existing interception powers in Part 1, Chapter 1 of RIPA with a new targeted interception power. It will set out the offence of unlawful interception and provide for the targeted interception of communications by a limited number of public authorities for a limited number of purposes when a warrant is in place. It will clarify that in all circumstances, when law enforcement or the security and intelligence agencies wish to intercept the communications of a person believed to be in the UK, or examine the communications of a person believed to be in the UK that have been collected in bulk a targeted interception warrant must be sought. It also lists the other limited circumstances in which interception (not undertaken by law enforcement or security and intelligence agencies) can be lawful. It includes the interception powers previously provided for in the Wireless Telegraphy Act 2006. The Bill will address the various recommendations made in respect of interception authorisation by making the decision to issue a warrant by the Secretary of State subject to approval by a Judicial Commissioner before the warrant comes into force.

8 Part 3 concerns authorisations for acquiring communications data: the 'who', 'when', 'where' and 'how' of a communication. These powers are currently primarily provided for under RIPA. The Bill will provide powers for public authorities to acquire communications data, replacing and largely replicating the effect of Chapter 2 of Part 1 of RIPA. The classes of communications data will be redefined so that they reflect current technology. The Bill will require requests for communications data to be made on a case by case basis so that access is permitted only when authorised by designated senior officers (who will be, subject to some specific exceptions, independent from investigations), on the advice of an expert Single Point of Contact (SPoC). Minor public authorities will be required to share SPoCs. The individual requests must be in respect of the statutory purposes and must be considered necessary and proportionate by a Designated Person. The Bill will set out the public authorities that will have access to communications data in future, permitting bodies to retain powers to access to communications data only where a clear case has been made.

9 Part 4 covers the retention of communications data. The existing statutory regime by which public telecommunications operators can be required to retain communications data will be broadly replicated, replacing section 1 of DRIPA. It will provide for the Secretary of State to require communications service providers to retain relevant communications data for one or more of the statutory purposes for a period that must not exceed twelve months. It specifies a number of safeguards in respect of data retention, for example the matters that must be considered before the giving of a retention notice, oversight arrangements and means of redress. The Bill also provides a new power for the retention of, and access to, internet connection records (ICRs) (the records captured by a network access provider of the internet services with which a person or device interacts).

10 Part 5 concerns equipment interference: interfering with computer equipment to obtain communications, private information or equipment data. This is currently provided for the security and intelligence agencies under the Intelligence Services Act 1994 (ISA) and, for law enforcement agencies under the Police Act 1997. The Bill will not repeal existing legislation but will provide a bespoke statutory framework for the ability of the security and intelligence agencies, Armed Forces and law enforcement agencies to undertake equipment interference to obtain communications and other private information. Interference with equipment where the primary purpose is not to acquire communications or private information will continue to be authorised under the Intelligence Services Act 1994 and the Police Act 1997.

11 Part 6 contains powers for the security and intelligence agencies to intercept communications, conduct equipment interference and to obtain communications data in bulk. The Bill will provide for a new 'Bulk Acquisition' warrant for the security and intelligence agencies to obtain communications data. This replaces the provision at section 94 of the Telecommunications Act 1984, which will be

repealed. The Bill will allow the security and intelligence agencies to intercept communications in bulk, focusing on the communications of persons who are believed to be outside the UK. This will replace the power to intercept "external communications" in Chapter 1, Part 1 of RIPA. Where it is not necessary to obtain the content of such communications, the Bill will provide the Secretary of State with the power to issue, subject to Judicial Commissioner approval, a warrant for the acquisition of related communications data only. The warrant will also pre-authorise the purposes for which communications acquired under a bulk warrant may be examined. A bulk equipment interference power will provide the statutory basis for foreign-focused equipment interference activity undertaken by the security and intelligence agencies. All bulk powers will be underpinned by safeguards equivalent to the bulk interception regime for the handling, destruction and retention of information.

12 Part 7 provides clarity and additional safeguards for the security and intelligence agencies' acquisition and use of Bulk Personal Datasets (BPD). The security and intelligence agencies have existing statutory powers under ISA and the Security Service Act 1989 (SSA) which enable them to acquire and access datasets containing personal data about a large number of individuals, many of whom are not of interest to the agencies. The Bill will not create a new power but bring greater transparency to this important capability and provide for enhanced safeguards. Acquisition and use of bulk personal data by the security and intelligence agencies will be subject to an authorisation process where the Secretary of State will issue a either a 'class' or 'specific' warrant which must then be approved by a Judicial Commissioner before it can come into force.

13 Part 8 sets out new oversight regime arrangements which will replace the three existing commissioners (the Intelligence Services Commissioner, the Interception of Communications Commissioner and the Chief Surveillance Commissioner) with a single new commissioner, the Investigatory Powers Commissioner (IPC). The Investigatory Powers Commissioner, a senior judge, will be supported by a number of Judicial Commissioners undertaking either authorisation or oversight and inspection functions. The Investigatory Powers Commissioner will have significantly greater powers and resources compared to the current oversight regime. The IPC will be a more visible body, providing robust oversight and scrutiny of the use of investigatory powers by a wide range of public authorities. The Investigatory Powers Commissioner will be able to draw on extensive legal and technical expertise. The Investigatory Powers Commissioner will have to report annually and be able to make ad hoc reports on matters that they consider appropriate.

14 The Bill will also create a domestic right of appeal in relation to decisions of the Investigatory Powers Tribunal (IPT) to the Court of Appeal. Regulations will make provision for claims relating to a devolved matter in Northern Ireland and Scotland in cases where the IPT has made a determination and found there is a point of law at issue. The Bill will enable appeals to be heard wholly or partly in closed material proceedings (CMP), if it is necessary for the appeal court to review information which was considered by the IPT in closed session. The Bill will provide for statutory Codes of Practice providing further guidance on the powers and duties in the Bill, to which public authorities and providers must have regard when carrying out these powers and duties.

15 Part 9 contains General and Final Provisions. This includes provision relating to obligations that may be placed on communications service providers to assist in giving effect to warrants and authorisations under the Bill as well as providing a new framework for obligations previously provided for under s.94 of the Telecommunications Act 1984.

Legal background

16 The investigatory powers available to the security and intelligence agencies, law enforcement and other public authorities are currently contained in a number of pieces of legislation. These powers include the interception of communications, the retention and acquisition of communications data, equipment interference, and the acquisition of bulk data.

17 The Regulation of Investigatory Powers Act 2000 (RIPA) contains much of the current legislative scheme governing the investigatory powers used by the security and intelligence and law enforcement agencies to interfere with communications, and was intended to provide an ECHR-compliant framework. Part 1 concerns communications. Chapter 1 of Part 1 concerns the interception of communications in the course of their transmission. It provides that such interception is an offence if carried out without lawful authority, and sets out the circumstances in which interception may be lawful. It also provides for the circumstances in which the Secretary of State may issue warrants for the interception of communications, and protections for intercepted material. Chapter 2 of Part 1 concerns powers to acquire communications data (information concerning a communication, but not its content) from communications service providers. It sets out the public authorities who may acquire such data and the purposes for which they may do so, and the procedure for the authorisation of such conduct.

18 Part 4 contains oversight measures, providing for the Interception of Communications Commissioner, the Intelligence Services Commissioner and giving additional powers to the Surveillance Commissioner established under the Police Act 1997. Part 4 also establishes the Investigatory Powers Tribunal.

19 Sections 1 - 2 of the Data Retention and Investigatory Powers Act 2014 (DRIPA) and the Data Retention Regulations 2014 (DRR) contain the legislative scheme concerning the power of the Secretary of State to require communications service providers to retain communications data. DRIPA also made clear the extra-territorial extent of Part 1 of RIPA. Part 3 of the Counter-Terrorism and Security Act 2015 (CTSA) amends DRIPA so that an additional category of data - that necessary to resolve Internet Protocol addresses – can be included in a requirement to retain data. DRIPA contains a sunset clause and sections 1-7 are repealed on 31 December 2016. Part 11 of the Anti-Terrorism, Crime and Security Act 2001 provides for a voluntary code of conduct concerning the retention of communications data.

20 The Security Service Act 1989 (SSA) sets out the functions of the Security Service, and provides that the Service can only obtain or disclose information so far as is necessary for those functions.

21 The Intelligence Services Act 1994 (ISA) sets out the functions of the Secret Intelligence Service and GCHQ, and contains similar provision concerning the obtaining and disclosure of information. Section 5 provides for the Secretary of State to authorise interference with property or wireless telegraphy where necessary for assisting the carrying out of any of the three Agencies' functions. Section 7 provides for the Secretary of State to authorise activities overseas that would otherwise incur civil or criminal liability, where necessary for the proper discharge of the functions of SIS or GCHQ. These powers are currently used to authorise certain activities of the Agencies that will be included in the new legislation.

22 Part 3 of the Police Act 1997 provides for the authorisation of interference with property or with wireless telegraphy. It also provides for the appointment of Surveillance Commissioners, who are given additional powers by Part 4 of RIPA.

23 The Wireless Telegraphy Act 2006 (sections 49) provides for the authorisation of the use of wireless telegraphy equipment to obtain information about a communication, or the disclosure

of such information. Such conduct is otherwise an offence under section 48 of the Act.

24 Section 94 of the Telecommunications Act 1984 gives the Secretary of State power to issue a direction of a general character to OFCOM or to a communications provider, in the interests of national security or international relations. Such directions may be kept secret.

European law

25 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector ('the e-Privacy Directive') contains a general requirement of confidentiality of electronic communications, as well as requirements to delete traffic data when no longer needed, and other protections for electronic communications. Art 15(1) provides that Member States may derogate from certain rights in the directive (including the right to privacy) where this is a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence, public security, the prevention, detection of crime and the purposes laid down in Art 13 of the Data Protection Directive. Art 15(1) specifically provides for the retention of communications data.

26 Directive 2006/24/EC ('the Data Retention Directive') harmonised the retention of communications data. The Data Retention Directive was struck down as incompatible with Articles 7 and 8 of the Charter of Fundamental Rights in joined cases C-293/12 and C-594/12 Digital Rights Ireland & Seitlinger, on the basis that it did not contain sufficient safeguards. No replacement Directive has as yet been proposed.

Territorial extent and application

27 The provisions in this Bill extend to the whole of the United Kingdom.

Commentary on provisions of Bill

Part 1: General Protections

Clause 1: Overview of the Act

29 This clause is self-explanatory.

Clause 2: Offence of unlawful interception

30 Subsection (1) makes it an offence to intentionally intercept, in the United Kingdom, a communication in the course of its transmission without lawful authority. This applies to a public telecommunications system, private telecommunications system or a public postal service. This is the same offence which previously existed under the RIPA.

31 Subsection (2) confirms that the criminal offence in subsection (1) does not apply where a person has the right to control the operation or use of the system or has the expressed or implied consent of such a person to carry out the interception. This is relevant to computer networks in the home or workplace.

32 Subsections (3), (4) and (5) signpost the sections of the Bill which define interception and when this is understood to be taking place in the UK; definitions of public telecommunications system, private telecommunications system and public postal service; and who has the lawful authority to apply for an interception warrant. A public telecommunications system is the hardware and software used to provide a telecommunications service to the public in the United Kingdom. A private telecommunications system is one that is separate from, but connected to a public telecommunications system; this will include computer networks in the home or workplace.

33 Subsection (6) sets out the penalties for a person who is found guilty of the offence of unlawful interception under section 1. The penalty for unlawful interception replicates the penalty which existed under RIPA.

34 Subsection (7) provides that any proceedings for an offence under subsection (1) must be with the consent of the Director of Public Prosecutions (in England and Wales) or the Director of Public Prosecutions for Northern Ireland (in Northern Ireland).

Clause 3: Definition of "interception" etc

35 This clause defines interception in relation to a telecommunication system and sets out when interception is understood to take place in the United Kingdom. The intention is to make clear which actions constitute interception.

36 Subsection (1) explains that a person must undertake one or more 'relevant acts' (set out in subsection (2)) at a 'relevant time', the consequence of which is to make some or all of the content of a communication available to a person who is not the sender or intended recipient.

37 Subsection (3) gives more detail of the relevant act of modifying a telecommunications system.

38 Subsections (4) and (5) define what is meant by 'relevant time'. The intention of subsection (4)(b) is to make clear that a communication is still considered in the course of its transmission when it is stored in or by the system used to transmit it. A stored communication includes communications stored on phones, tablets and other individual devices.

> Example:
> An email which has been sent and is stored on an email server or a voicemail message which has been stored on a telecommunications system to be retrieved later.

39 Subsection (8) makes clear when interception takes place in the United Kingdom.

Clause 4: Conduct that is not interception

40 The purpose of clause 4 is to set out conduct which does not constitute interception. Subsection (1) makes clear that interception of a communication broadcast for general reception is not interception within the context of this Bill. Subsection (2) excludes conduct in relation to 'postal data' attached to the communication. Clause 194 provides provide further information on the references to postal data.

Clause 5: Definition of "lawful authority"

41 This clause sets out the circumstances in which a person has lawful authority to carry out interception, so an offence of unlawful interception is not committed. Subsection (1) sets out that lawful authority to carry out interception must be either: in accordance with a warrant; with consent or, in relation to stored communications, the exercise of any statutory power for the purpose of obtaining information or taking possession of any document or other property.

Clause 6: Monetary Penalties for certain unlawful interceptions

42 This clause provides for the Investigatory Powers Commissioner to impose fines where unlawful interception has taken place but where the person responsible was not intending to intercept a communication.

> Example:
> A company that develops and uses a piece of software to collect information about Wi-Fi hotspots but does not realise that it is also intercepting content which is being sent from non-secure Wi-Fi devices.

43 Subsections (3) and (4) set out the conditions which must be met for the Investigatory Powers Commissioner to issue a monetary penalty notice. The Investigatory Powers Commissioner may not issue a monetary penalty notice if he or she considers that the person has committed an offence of unlawful interception i.e. the interception was intentional.

44 Subsection (6) introduces Schedule 1 which makes further provision about monetary penalty notices.

Clause 7: Restrictions on requesting overseas interception

45 This clause explains that a mutual assistance warrant must be in place before a request for interception can be made to authorities outside the UK under a mutual assistance agreement. Subsection (3) sets out the meaning of "international mutual assistance agreement"and "EU mutual assistance instrument".

Clause 8: Offence of unlawfully obtaining communications data

46 Clause 8 creates a new offence of unlawfully obtaining communications data. It is intended to act as a deterrent and provide reassurance that abuse of communications data will be punished.

Clause 9: Abolition of certain powers to obtain data

47 This clause and Schedule 2 restrict general information gathering powers and certain specific pieces of legislation being used to acquire communications data. The intent of these provisions is to ensure that this Bill, with its associated safeguards, is the only route for the acquisition of communications data for the statutory purposes in this Bill.

48 Numerous pieces of legislation provide public authorities with powers to require information in certain circumstances. This clause ensures those pieces of legislation will no longer be able to be used to acquire communications data.

49 Clause 9 does not apply where the power relates to communications data or the regulation of telecommunications services. This is to allow OFCOM and the Information Commissioner's Office to carry out legitimate regulatory functions, for example ensuring the radio spectrum is used in an effective way.

50 Schedule 2 lists the powers that specifically reference communications data or telecommunications services that are being repealed.

Clause 10: Mandatory use of targeted equipment interference warrants

51 This clause sets out the conditions in which a warrant must be sought under the powers contained in the Bill before equipment interference can be carried out by a relevant service which includes the intelligence agencies and Ministry of Defence.

52 Subsections (1) (a) and (b) state that the activity must both be believed to constitute one or more offences under sections 1 to 3A of the Computer Misuse Act 1990, and have a connection to the British Islands.

53 Subsection (2) defines British Islands as either:

a. Where the proposed activity would take place in the UK (regardless of where the equipment to be interfered with is located). When the intelligence agencies or Ministry of Defence are operating from the UK, they must use this act to authorise their activity even if the equipment itself leaves or does not enter the UK;

b. or where the intelligence service or Ministry of Defence believes the equipment to be interfered with may be located in the UK at some point during the interference itself. This will include circumstances where the computer is located in the UK or is carried by someone transiting through the UK at the time the interference is taking place;

c. or where the purpose of the interference is to enable the acquisition of the private information or the communications sent to or from a person believed to be in the UK. The interference is aimed at a person in the UK.

54 Subsection (3) clarifies that where those conditions are not met, an intelligence service or Ministry of Defence may still apply for an equipment interference warrant. The circumstances in which they would do so will be set out in Codes of Practice.

Clause 11: Restriction on use of section 93 of the Police Act 1997

55 This clause confirms that applications may not be made under section 93 of the Police Act for activity that would be authorised by a targeted equipment interference warrant (in other words where the primary aim of the equipment interference is to obtain communications etc.) if the applicant believes it constitutes an offence under the Computer Misuse Act. This does not

remove or otherwise limit the ability for equipment interference to be authorised under the Police Act 1997 where the primary aim is not to obtain communications, private information or equipment data.

Part 2: Lawful Interception of Communications

Chapter 1: Interception and examination with a warrant

Clause 12: Warrants that may be issued under this Chapter

56 Subsection (1) explains that there are three types of warrants which can be issued under this chapter. Subsection (2) describes a targeted interception warrant. Subsection (3) describes a targeted examination warrant which authorises the examination of material that has been collected under a bulk interception warrant. Examination warrants must be sought whenever a member of an intelligence service wishes to look at material which relates to a person who is believed to be in the British Islands and when he or she believes that it is necessary and proportionate to select the content of that person's communications for examination.

57 Subsection (4) describes a mutual assistance warrant which would be made to EU or non-EU authorities requesting assistance in relation to the intelligence request specified in the warrant.

58 Subsection (5) confirms that a warrant authorises any conduct necessary to fulfill what is required by the warrant, including interception of communications not specifically described in the warrant or related communications data.

59 Subsections (6)-(9) define what is related communications data in relation to a targeted interception warrant. Related communications data includes:

a. Communications data (see clause 193);

b. Data obtained through a warrant which enables or otherwise facilitates the functioning of any postal service, telecommunications system or any telecommunications service provided by means of the system;

c. Data which:

i. Can be logically extracted from the content of the communication;

ii. Which does not, once extracted, reveal the meaning of the content of the communication; and

iii. Can identify, or assist in identifying, any person, apparatus, telecommunication system or telecommunications service, or which describes an event, or the location of any person, event or thing.

60 Related communications data as defined in this clause may only be obtained under a targeted interception warrant and, once the data is obtained, will be subject to the safeguards set out in Part 2.

61 Related communications data obtained under a targeted interception warrant is equivalent to related communications data obtained under a bulk interception warrant, and equipment data obtained pursuant to an equipment interference warrant.

62 This clause makes clear that the extraction of any data from the content of a communication that has been acquired during the course of its transmission can only take place under an interception warrant.

63 In addition to communications data the data falling within this category could include:

a. The version of the app sending the message;

b. Data relating to any files attached to a message such as the date and time it was created and the author;

c. Any location information related to the communication, for example the location required to enable an application;

d. Any email addresses contained within a communication

Clause 13: Subject-matter of warrants

64 Subsection (1) sets out that a warrant under this Chapter may relate to a particular person or organisation, or a single set of premises. Subsection (2) provides further detail on when a warrant may apply to a group of persons or more than one set of premises.

Clause 14: Power of Secretary of State to issue warrants

65 This clause provides a power for the Secretary of State to issue a Part 2 warrant. Subsections (1) and (2) require that the Secretary of State considers that the targeted interception, mutual assistance or examination warrant is necessary (for the purposes set out in subsection (3)) and proportionate to what is sought to be achieved. The decision of the Secretary of State to issue the warrant must then be approved by a Judicial Commissioner before the warrant comes into force.

66 Subsection (3) sets out the grounds on which a Part 2 warrant can be applied for. These are the interest of national security, preventing or detecting serious crime, safeguarding the economic well-being of the United Kingdom (in circumstances relevant to the interests of national security), or giving effect to the provisions of any international mutual assistance agreement.

67 Subsection (4) clarifies that a warrant authorised on grounds of being in the economic well-being of the UK can only be sought to obtain information relating to acts or persons outside of the UK.

68 Subsection (6) requires the Secretary of State to consider whether the information thought necessary to obtain under a warrant could be sought by other means. Subsection (7) provides the circumstances under which the Secretary of State may not issue a warrant under this section i.e. if it relates to serious crime activity in Scotland.

Clause 15: Persons who may apply for issue of a warrant

69 Clause 15 lists those persons who may apply to the Secretary of State for an interception warrant. The same people may apply for a warrant as was the case under RIPA.

Clause 16: Additional protection for Members of Parliament, etc

70 This clause requires the Secretary of State to consult the Prime Minister before deciding to issue a targeted interception or examination warrant where the purpose may be to obtain the communications of a person who is a member of a relevant legislature. Subsection (3) defines "member of a relevant legislature".

Clause 17: Power of Scottish Ministers to issue warrants

71 This clause provides a power for the Scottish Ministers to issue a Part 2 warrant. Subsections (1) and (2) require that the Scottish Ministers consider that the warrant is necessary (for the purposes set out in subsection (3)) and proportionate to what is sought to be achieved. The decision of the Scottish Ministers to issue the warrant must then be approved by a Judicial Commissioner before the warrant comes into force.

Clause 18: "Relevant Scottish applications"

72 Subsections (2) – (4) set out the conditions that need to be met for a warrant application under this Chapter to be considered as a "relevant Scottish application". These are where the application relates to a person reasonably believed to be in Scotland or premises which are in Scotland; or if the application is made by or on behalf of the Chief Constable of Police Scotland, the Commissioner of HM Revenue and Customs or the Director General of the National Crime Agency for the purpose of preventing or detecting serious crime in Scotland.

Clause 19: Approval of warrants by Judicial Commissioner

73 This clause sets out the test that the Judicial Commissioner must follow when looking at whether to approve a decision to issue a warrant. They must look at the necessity and proportionality test applied by the Secretary of State under clause 14 in relation to the same grounds that the court would apply for a judicial review.

74 Subsection (4) makes clear that where a Commissioner refuses to approve a warrant they must set out written reasons for their refusal. This may allow the agency requesting the warrant to reconsider their application and what action they are seeking to take in order to meet any concerns expressed by the Commissioner.

75 Subsection (5) sets out that a Secretary of State or Scottish Ministers may ask the Investigatory Powers Commissioner to reconsider an application that a Judicial Commissioner has refused. Should the Investigatory Powers Commissioner also refuse to approve the warrant there is no further right of appeal and the warrant cannot come into force.

Clause 20: Approval of warrants in urgent cases

76 This clause sets out the process for issuing a warrant in urgent cases. If the person issuing the warrant deems the warrant to be urgent then in extremis it can be issued without the approval of a Judicial Commissioner. Subsection (2) requires that the issuing of the warrant must be notified to the Judicial Commissioner. Subsection (3) provides that the Commissioner must decide whether to approve the decision to issue the warrant within five working days. Subsection (4) makes clear that this requirement for the Judicial Commissioner to approve the urgent warrant falls away if the warrant is to be renewed within the five working day period. In those circumstance the Judicial Commissioner will approve the warrant renewal in the usual way

77 If the Judicial Commissioner refuses to approve the urgent warrant within the five day period then subsection (5) provides that the warrant ceases to have effect. Subsection (6) refers the reader to the part of the Bill that contains further provision about what happens in these circumstances.

Clause 21: Warrants ceasing to have effect under section 20

78 If a Judicial Commissioner (or on appeal, the Investigatory Powers Commissioner), refuses to approve a warrant that has been approved under the urgency procedure then the warrant ceases to have effect. Subsection (2) outlines how those exercising powers under the warrant must, as far and as quickly as they can, stop any activity being undertaken.

79 Subsection (3) sets out how the Judicial Commissioner can determine what can happen to any material or intelligence gathered under an urgent warrant that they have declined to approve. Subsection (4) provides for representations to be made to the Judicial Commissioner from those involved in applying for the warrant or carrying out activity under the authority of the warrant.

80 Subsections (6) and (7) provide for the Secretary of State or Scottish Minister who authorised the warrant to ask the Investigatory Powers Commissioner to review a decision of a Judicial Commissioner to refuse an urgent warrant and provides that he can confirm the Judicial

Commissioner's decision or make a fresh determination.

81 Subsection (8) provides that any activity carried out before the Judicial Commissioner refused to authorise the warrant remains lawful, as is anything that cannot practically be stopped.

Clause 22: Decisions to issue warrants to be taken personally by Ministers

82 Subsection (1) requires the decision to issue a warrant under Chapter 2 to be taken personally by the Secretary of State or a member of the Scottish Government. Subsection (2) requires the warrant to be signed by the person who has taken the decision to issue the warrant (except in urgent cases). Subsections (4) to (6) provide that in urgent cases a warrant may be signed by a senior official designated by a Secretary of State or Scottish Minister.

Clause 23: Requirements that must be met by warrants

83 This clause deals with the information which needs to be contained in Part 2 warrants. Subsections (2) to (9) specify the information a warrant must contain including the intercepting authority, details of the person or group of persons, organisation or premises to which the warrant relates. In the case where the warrant relates to a group of individuals linked by an activity/investigation/operation, this must be described.

> Example:
> This involves an operation where an individual has been kidnapped. The agency may have a phone number or numbers but at the time not know who they are being used by. In these circumstances the agency could not describe the individuals (beyond kidnapper 1, kidnapper 2, driver etc.). The warrant could therefore refer to operation 'safe return' and would allow an addition if the investigation then becomes aware of 'kidnapper 3'.

Clause 24: Duration of warrants

84 This clause deals with the duration of a Part 2 warrant. An interception warrant will last for 6 months (unless it is cancelled earllier). If the warrant is not renewed it will cease to have effect after that period. Urgent warrants will last for 5 days unless renewed.

Clause 25: Renewal of warrants

85 Subsections (1) - (3) state that a warrant may be renewed by an instrument issued by the appropriate person. The appropriate person is set out at subsection (3). In order to renew the warrant the appropriate person must consider that it is still necessary. As with an application for an interception warrant, the decision to renew the warrant must also be reviewed by a Judicial Commissioner prior to the date of expiry. The clause also sets out the additional protection for Members of Parliament, etc. (see 16(3)), that apply in relation to a decision to renew a warrant as it applies in relation to a decision to issue a warrant.

Clause 26: Modification of warrants

86 This clause provides for a warrant to be modified as specified in subsection (2) by instrument. Subsection (4) explains what "major" and "minor" modifications are and subsections (5) and (6) outline who can undertake a major and minor modification. Subsections (8)-(11) restate the conditions of necessity and proportionality which must be considered before major modifications can be made. The clause also sets out the additional protection for Members of

Parliament, etc. (see 16(3)), that apply in relation to a decision to make a major modification of a warrant as it applies in relation to a decision to issue a warrant.

Clause 27: Cancellation of warrants

87 This clause provides that the Secretary of State, Scottish Ministers, a member of the Scottish Government or a senior official acting on their behalf may cancel a warrant if it is no longer necessary.

Clause 28: Special rules for certain mutual assistance warrants

88 This clause deals with the process for providing assistance in relation to a mutual assistance agreement or instrument. This applies to applications to provide assistance with intercepting the communications of an individual outside the United Kingdom or in relation to premises outside the United Kingdom.

89 Subsection (2) provides that the decision to provide assistance in such circumstances can be taken by a senior official designated by the Secretary of State. Subsection (4) makes clear that the senior official may also renew the mutual assistance warrant. Subsections (3) and (5) set out what must be included in the warrant. Subsection (7) makes clear that any warrant must be cancelled if the subject of the warrant is in the UK.

Clause 29: Implementation of warrants

90 This clause requires the person on whom a targeted interception warrant or mutual assistance warrant is served to give effect to the warrant. Subsections (3, 4 and 6) make clear that a copy of a warrant may be served on any person who the implementing authority believes may be able to provide assistance to give effect to the warrant; that a copy can be served on a person outside the UK and that copies of the warrant itself or one or more of the schedules contained in the warrant may be served. Subsection (5) defines that provision of assistance requires the disclosure of interception and related communications data authorised by the warrant.

Clause 30: Service of warrants

91 This clause sets out the process for serving an interception warrant. Subsection (2) and (3) set out how an interception warrant may be served on a person outside the UK.

Clause 31: Duty of operators to assist with implementation

92 This clause sets out the obligation placed on service providers to give effect to a warrant and makes clear the steps they must take to give effect to it. Subsection (3) requires a relevant provider to give effect to a targeted interception warrant whether or not the provider is in the UK. Subsection (4) ensures that the steps a service provider is required to make must be reasonably practicable and subsection (5) makes clear that in considering what is reasonable, any requirements or restrictions under the laws of the country in which a provider is based must be taken into account.

93 Subsection (7) sets out the offence for knowingly failing to comply with an interception warrant. Subsection (8) provides that the duty to comply with a warrant is enforceable by civil proceedings brought by the Secretary of State.

Chapter 2: Other forms of lawful interception

Clause 32: Interception with the consent of the sender or recipient

94 Subsection (1) confirms that the interception of a communication is authorised if both the person sending the communication and the intended recipient of the communication have given consent for the interception to take place.

95 Subsection (2) confirms that the interception of a communication is authorised if either the sender or the intended recipient has consented and surveillance has been authorised under Part 2 of the Regulation of Investigatory Powers Act 2000.

> Example:
> This situation might arise where a kidnapper is telephoning relatives of a hostage, and the police wish to listen to the call in order to identify or trace the kidnapper. The operation will be authorised as surveillance, rather than by means of an interception warrant, because consent can only reasonably be obtained for one end of the communications i.e. the relatives have consented.

Clause 33: Interception by providers of postal or telecommunication services

96 This clause authorises interception where it takes place for the purpose of providing or operating a postal service or telecommunications service, or where any enactment relating to the use of such a service is to be enforced. This might occur, for example, where the postal provider needs to open a postal item to determine the address of the sender because the recipient's address is unknown. A further example might be where a telecommunications service provider is delivering a service to its customers and the customer has requested that harmful, illegal or adult content is filtered (e.g. family friendly filtering).

97 Subsection (3) makes clear that telecommunication service providers can undertake activity to protect the telecommunication system through which their service is provided and any apparatus attached to that system, to maintain the integrity of their services and to ensure the security of their customers.

Clause 34: Interception by businesses, etc for monitoring and record-keeping purposes

98 This clause allows for the making of regulations by the Secretary of State to authorise legitimate practice to carry out relevant activities. This clause will allow the Secretary of State to make regulations authorising the monitoring or keeping of records of communications, where that is a legitimate business practice required for business purposes.

> Example:
> The recording of telephone conversations by businesses for training or quality control purposes.

Clause 35: Postal Services: interception for enforcement purposes

99 This clause provides for the interception of postal items by HM Revenue and Customs in carrying out their duties under clause 159 of the Customs and Excise Act 1979 or by an examining officer under paragraph 9 of Schedule 7 of the Terrorism Act 2000.

Clause 36: Interception by OFCOM in connection with wireless telegraphy

100 This clause states that the interception of communications is authorised with the authority of OFCOM under section 48 of the Wireless Telegraphy Act 2006 in their efforts to maintain the security of the radio frequency network.

101 Subsection (3) sets out the purposes for which OFCOM can use wireless telegraphy to intercept communications.

Clause 37: Interception in prisons

102 Subsection (1) makes clear that it is lawful to intercept communications in a prison if it is in the exercise of any power conferred under prison rules and subsections (2 and 3) sets out what is meant by "prison rules" and "prisons".

Clause 38: Interception in psychiatric hospitals

103 This clause sets out the circumstances in which interception can be carried out in psychiatric hospitals.

Clause 39: Interception in accordance with overseas requests

104 This clause deals with the issue of interception when a request is made from overseas.

105 Subsections (2) – (5) sets out the conditions which need to be met in order that a communications provider may intercept the communications of an individual outside the UK at the request of another country. Further conditions may be contained in regulations made by the Secretary of State.

Chapter 3 – Other provisions about interception

Clause 40: General safeguards

106 This clause sets out that the issuing authority must ensure that arrangements are in force for safeguarding material obtained under an interception warrant.

107 Subsection (2) sets out the requirements to keep to a minimum the number of persons who see material and to limit the disclosure and number of copies made of any material to the minimum necessary for the authorised purposes. Subsection (3) sets out the circumstances in which something is necessary for the authorised purposes.

108 Subsections (4) to (6) require that material is kept in a secure manner and that it must be destroyed as soon as it is no longer required for any authorised purpose.

Clause 41: Safeguards relating to disclosure of material or data overseas

109 This clause sets out the safeguards which apply when disclosing intercept material and related communications data to an overseas authority. These include that material is not disclosed in a way which would constitute unlawful disclosure in the United Kingdom.

Clause 42: Exclusion of matters from legal proceedings

110 This clause prevents intercept material being used or disclosed in legal proceedings or Inquiries Act proceedings. This includes adducing it in evidence, asking questions about it, disclosing it, or doing anything from which it could be inferred that the material came from interception or which suggests that interception may have occurred. Subsection (2) defines "interception related conduct" and the other statutes that apply

111 The exceptions to this prohibition are set out in Schedule 2.

Clause 43: Duty not to make unauthorised disclosures

112 This clause places a duty on those persons listed in subsection (3) not to disclose the existence or details of a warrant or any intercepted material. Subsection (4) sets out the matters which, if disclosed, would constitute unauthorised disclosure. Subsection (5) sets out the circumstances in which disclosure would be authorised. It also makes clear that operators may disclose information relating to the number of warrants they have given effect to and subsection (7)

provides for the Secretary of State to issue directions relating that disclosure.

Clause 44: Offence of making unauthorised disclosures

113 This clause provides that it is an offence to fail to comply with the duty in clause 43 and sets out the penalty for unlawful disclosure of intercept material.

Clause 45: Part 2: interpretation

114 This clause sets out definitions for a number of terms used throughout this clause.

Part 3: Authorisations for obtaining communications data

Clause 46: Power to grant authorisations

115 This clause provides the power for relevant public authorities to acquire communications data. An authorisation can be granted where a designated person in a relevant public authority is content that a request is necessary and proportionate for one of the 10 purposes set out in subsection (7). Communications data cannot be acquired in circumstances outside of those purposes and only certain authorities can use certain purposes, as outlined in Schedule 4.

116 Subsection (4) provides for some of the conduct which an authorisation may permit for the purpose of acquiring communications data. The types of conduct that can be engaged in are the same as can currently under Chapter 2 Part 1 of RIPA. For example the conduct to acquire communications data may involve:

a. Serving a notice on a telecommunications service provider that requires them to disclose the relevant data;

b. Serving a notice on a telecommunications service provider that requests they obtain and then disclose the relevant data;

c. A relevant public authority acquiring the data directly from a communications service provider through a secure auditable system

117 Subsection (5) provides examples may be covered by an authorisation. For example, an authorisation may cover data that is not in existence at the time of the authorisation. This allows a relevant public authority to request communications data on a forward looking basis in respect of a known subject of interests. It also provides that an authorisation can authorise the disclosure of communications data by a communications service provider through a secure auditable system.

Clause 47: Additional restrictions on grant of authorisations

118 This clause provides a restriction on who can authorise the request. The authorising officer can only agree to the acquisition of communications data where they are independent of the operation.

119 Examples of this relate to cases where there is an imminent threat to life, where using an independent authorising officer would immediately impact on national security or where it is simply not possible due to the size of the public authority.

120 This clause also provides restrictions concerning the acquisition of internet connection records that are held by communications service providers. Under RIPA there are currently no such restrictions, however communications service providers cannot be required to retain internet connection records under existing legislation. Clause 71(9)(f) of this Bill provides for the retention of internet connection records. A public authority may only acquire internet connection records that are held by a communications service provider for the following three purposes:

a. To identify the sender of an online communication; this will often be in the form of IP address resolution and the internet service used must be known in advance of the application.

b. Identifying which communication services a person has been using, for example determining whether they are communicating through apps on their phone.

c. Identifying where a person has accessed illegal content, for example an internet service hosting child abuse imagery.

121 In practice, in respect of purpose a., the relevant public authority will be aware of an action on a particular internet service at a specific time or range of time, for example that illegal images have been uploaded. The communications data application would be to determine which individual carried out that action at that time.

122 In respect of purposes b. and c., the designated senior officer within a relevant public authority could only approve the application if it was to determine how an individual has been communicating with another individual online, or whether they had been accessing illegal material over a specified timeframe. In practice, if approved, a request would then be made to a communications service provider for all internet connection records in that timeframe.

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

Clause 48: Procedure for authorisations and authorised notices

124 Subsection (1) sets out that every authorisation must specify certain details. These include the position held by the designated senior officer granting the authorisation, which of the limited purposes it is being granted for (as set out in Clause 46(7)), the conduct for which it was authorised, the type of data to be obtained, and who the data will be disclosed to.

125 Subsection (2) sets out that an authorisation which authorises a person to place an obligation on a communications service provider to acquire communications data must specify the name of the communications service provider and the requirements that will be imposed on that communications service provider.

126 Subsection (3) sets out that the notice must specify the position held by the person giving the notice, the requirements that will be imposed on that communications service provider, and the name of the communications service provider.

127 Subsection 4 sets out that a record must be kept of the notice in order to show that it has been applied for or granted.

Clause 49: Duration and cancellation of authorisations and notices

128 Clause 49 limits the duration of authorisations and sets out when they must be cancelled. Subsection (1) provides that an authorisation ceases to have effect at the end of the period of one month beginning from the date it was granted.

129 Subsections (2) and (3) permit an authorisation to be renewed at any period during the month, by following the same procedure as for obtaining a fresh authorisation. The renewed authorisation will last for a period of one month from the date the current authorisation expires.

130 Subsection (4) places a duty on the designated senior officer who has granted an authorisation to cancel it if they are satisfied that the position is no longer as set out clause 46(1).

131 Subsections (5) and (6) permit the Secretary of State to specify by order the person required to carry out the duty set out in subsection (4) in the event that this would otherwise fall on a person who is no longer available to perform it.

Clause 50: Duties of telecommunications operators in relation to authorisations

132 Communications service providers are required to comply with a request for communications data, unless in circumstances where it is not reasonably practicable to comply. If complying with the request is reasonably practicable then the provider should comply in such a way that involves processing the minimum amount of data necessary.

133 Subsection (1) places a duty on communications service providers which are under a notice to comply with authorised requests for data.

134 Subsection (2) places a duty on a communications service provider who is obtaining or disclosing communications data in response to a request or a requirement to carry out these activities in a way that minimises the amount of data that needs to be processed for the purpose concerned.

135 Subsection (3) sets out that a person on whom duties in subsections (1) and (2) are placed is not required to do anything in pursuance of this duty that it is not reasonably practicable to do.

136 Subsection (4) specifies that the duties imposed by subsections (1) or (2) are enforceable by the Secretary of State by civil proceedings for an injunction, or for the specific performance of a statutory duty under clause 45 of the Court of Session Act 1988 or for any other appropriate relief.

Clause 51: Filtering arrangements for obtaining data

137 This clause provides a power to establish filtering arrangements to facilitate the lawful, efficient and effective obtaining of communications data by relevant public authorities and to assist a designated senior officer in each public authority to determine whether he believes the tests for granting an authorisation to obtain data have been met. The filtering arrangements will minimise the interference with the right to privacy, in particular respect for personal correspondence, to which requests for internet based communications data will give rise thereby ensuring that privacy is properly protected. In practice, filtering arrangements would be implemented by the Secretary of State in a Request Filter system which would be used by public authorities granting authorisations for the targeted acquisition of communications data.

> Potential use of the Request Filter
> Example (1): IP address resolution:
> An investigator has details of a number of IP addresses which they believe relate to a specific individual, and have been used to access internet services at known times. However, each IP address cannot be resolved to a single individual because at the known time it has been simultaneously shared between many internet users. In this example the Request Filter would be able to match the specific individual in common between the users of each the IP addresses, then disclose only the communications data about that specific individual to the public authority. Without the Request Filter telecommunications operators would need to disclose details of every individual that had shared the IP addresses at the relevant times, and an analyst working in the public authority would examine all of the individuals data to obtain the same

result.

Example (2): Location correlation:
If an investigator knows that a person of interest has been in a number of places at certain times. The Request Filter would enable them to determine whether communications service providers retained information that can identify the specific individual that matched being in those locations. Without the Request Filter the data of every individual that matched each location would have to be disclosed and the law enforcement agency would need to correlate the data.

138 These type of applications, as all communications data applications, would only be able to be made where necessary and proportionate.

139 The power to establish filtering arrangements in subsection (1) operates solely in the context of Part 3 of the Bill which creates a regulatory regime for obtaining data. The power is intended to facilitate the obtaining of data by public authorities only for the purpose of a specific investigation or a specific operation in accordance with an authorisation, whilst protecting privacy. Any communications data obtained by the filtering arrangements must be immediately deleted once the purposes of the authorisation have been met. The power will be exercised in two main ways.

Clause 52: Use of filtering arrangements in pursuance of an authorisation

140 Clause 52 will apply in relation to the use of any Request Filter established under the power in clause 51. The effect of subsection (2) is that the Request Filter may be used to obtain, process and disclose Part 3 data if, but only if, these uses have been specifically authorised by the authorisation.

141 Subsection (3) sets out the matters which the designated senior officer must record within the authorisation to obtain Part 3 data. These include:

a. whether the Part 3 data may be obtained and disclosed by use of the filter;

b. whether the processing of data under the filter is allowed;

c. if the processing of data is allowed, then a description of data that may be processed must also be included.

142 Subsections (4) and (5) reinforce the conditions that must be met before a designated senior officer can authorise the use of a Request Filter. These conditions are: that it is necessary to obtain the data for a public protection purpose; that it is necessary to obtain the data for a specific investigation or a specific operation; and that the conduct authorised by the authorisation is proportionate to what an investigator is seeking to achieve.

143 Subsections (2) to (5) will accordingly ensure that the use of any Request Filter under Part 3 is specifically authorised by the authorisation, is proportionate and is recorded within the authorisation.

Clause 53: Duties in connection with operation of filtering arrangements

144 Clause 53 imposes duties in connection with the operation of filtering arrangements. In the case of a Request Filter, subsection (1) provides that no communications data must be obtained or processed under the filter except for the purposes of an authorisation granted under clause 46. Data which has been obtained or processed under the filter, and is to be disclosed in accordance with the authorisation or for the purposes of assisting the designated senior officer,

shall only be disclosed to authorised individuals. Further, subsection (1)(c) specifically requires any data obtained by the filter to be immediately destroyed in such a way that it can never be retrieved, once the purposes of the authorisation or of the assistance function have been met or if at any time it ceases to be necessary to retain the data for these purposes.

145 Subsection (1) will ensure that only the filtered data relevant to the investigation is disclosed to the requesting agency. Once the filter has provided the answer to the question, all the data relating to the request will be deleted by the filter.

146 Subsection (2) limits the disclosure of data other than authorised data which is retained under the filtering arrangements:

a. to assist a designated senior officer to determine whether he believes the tests for granting an authorisation are met;

b. for the purposes of support, maintenance, oversight, operation or administration;

c. to the Investigatory Powers Commissioner for the purposes of any his functions;

d. as otherwise authorised by law.

147 Subsection (3) requires strict limits to be placed on the persons who are permitted to read, obtain or otherwise process data for the purposes of support, maintenance, oversight, operation or administration in connection with the Request Filter. No other persons must be permitted to access or use the capability except in pursuance of an authorisation or to assist the designated senior officer to determine whether an authorisation is necessary and proportionate.

148 Subsection (5) requires that an adequate security system is in place to protect against any abuse of access to the Filter, as well as measures to protect against any unauthorised or unlawful data retention, processing, access or disclosure. The duty in subsection (4) will ensure that a Request Filter can only be used in accordance with Part 3 and is subject to adequate and effective safeguards against abuse.

149 Subsection (6)(a) requires procedures to be put in place and maintained to ensure that the Request Filter is functioning properly, including regular testing of the relevant software and hardware. Subsection (6)(b) requires a report to be made, as soon as possible after the end of each calendar year, to the Investigatory Powers Commissioner about the functioning of the Request Filter during that year. Such a report must, in particular, contain information about destruction of data during that year (subsection (6)). Subsections (5) and (6) will ensure that the operation of any Request Filter is subject to rigorous oversight and control.

150 Subsection (8) requires any significant processing errors to be immediately reported to the Investigatory Powers Commissioner. Subsection (7) constitutes a further safeguard with respect to the operation of any Request Filter.

Clause 54: Relevant public authorities and designated senior officers

151 Clause 54 introduces Schedule 4 to the Bill and makes provision in relation to relevant public authorities, designated senior officers and safeguards

152 Schedule 4 includes a table which lists the public authorities permitted to obtain communications data under Part 3 of the Bill (column 1); the minimum office, rank or position of the designated senior officers permitted to grant authorisations to obtain data (column 2); the types of communications data that may be obtained (column 3); and the statutory purposes for they may be obtained (column 4).

153 Subsection (2) provides that a public authority which is listed in column 1 of the table in

Schedule 4 is a "relevant public authority" for the purposes of Part 3.

154 Subsection (3) establishes that, in this Part, a "designated senior officer" of a public authority listed in column 1 of the table means an individual who either holds the office, rank or position specified in column 2 of the table, or (subject to subsections (5) and (6)) an office, rank or position which is higher than the level specified in the table.

155 Subsections (4) and (5) make clear that where column 2 of the table specifies a designated senior officer by reference to a particular branch, agency, or other part of an authority, or particular function of the authority, then only individuals who hold the specified office, rank, or position in that part of the authority, or who have responsibility for those functions, may act as the "designated senior officer".

156 Subsection (7) deals with cases where an individual is a designated senior officer by virtue of more than one entry in the table. For example, a chief superintendent in a police force will be a designated senior officer by virtue of being a higher rank than an inspector, and by virtue of being a higher rank than a superintendent. Subsection (7) ensures that he can do both what an inspector can do and what a superintendent can do.

Clause 55: Power to modify section 54 and Schedule 4

157 This clause provides that the Secretary of State may modify clause 54 and Schedule 4 by order. Subsection (2) gives examples of what may be done under the general power in subsection (1). These include adding or removing a public authority from the list in column 1 of a table in Schedule 4. By virtue of clause 55 and clause 56, most orders under clause 54 will be subject to the enhanced affirmative procedure. The exception is an order which modifies only column 2 of the table, which defines the designated senior officers of a public authority. By virtue of clause 195 such orders will be subject to the negative resolution procedure.

158 Subsection (4) provides the Secretary of State with the power to make modifications by order in any enactment which may be required as a result of a person becoming, or ceasing to be a relevant public authority.

Clause 56: Certain regulations under section 55: supplementary

159 When making changes to the relevant public authorities in Schedule 4 by the affirmative procedure, this clause requires the Government to consult the Investigatory Powers Commissioner and the relevant public authority concerned. An example of this would include adding a new public authority to the list of relevant authorities.

Clause 57: Local authorities as relevant public authorities

160 Clause 57 provides that local authorities are relevant public authorities for the purposes of Part 3, and defines the designated senior officers of local authorities.

Clause 58: Requirement to be party to collaboration agreement

161 This clause ensures that local authorities will only be able to obtain communications data if they are party to a collaboration agreement as certified by the Secretary of State. This is a safeguard that ensures local authorities are only able to acquire communications data through an experienced shared single point of contact service.

Clause 59: Judicial approval for local authority authorisations

162 This clause provides a procedure by which local authority authorisations to obtain communications data can only take effect if approved by a relevant judicial authority.

163 This means that a local authority authorisation granted under clause 57 will not take effect until the "relevant judicial authority" has given its approval. The relevant judicial authority is

defined in subsection (7). In England and Wales, the judicial authority is a justice of the peace, in Northern Ireland it is a district judge (magistrates' court) and in Scotland, a sheriff.

Clause 60: Requirement to consult a single point of contact

164 The single point of contact (SPoC) is an accredited individual trained to facilitate lawful acquisition of communications data and effective co-operation between a public authority and CSPs. Clause 60 sets out how the SPoC and designated senior officer work together when granting an authorisation for the acquisition of communications data.

165 Subsections (1), (2) and (3) set out that the designated senior officer must consult the SPoC before granting an authorisation for communications data, unless there are exceptional circumstances, such as an imminent threat to life or in the interests of national security.

166 Subsection (4) sets out what constitutes a SPoC, specifically that they must be an officer in a relevant pubic authority with communications data powers and that they have a responsibility for advising both those applying for the acquisition of communications data, and designated senior officers that authorise such applications.

167 Subsections (5) and (6) set out the advisory role that a SPoC plays to both those applying for communications data, and the designated senior officer that authorises the application. SPoCs should advise whether the application and authorisation is lawful, appropriate and cost-effective, and takes into consideration any unintended consequences.

168 Subsection (7) sets out that a SPoC may also provide advice to the designated senior officer about whether the requirements of an authorisation have been met, its use in support of operation or investigations and any other effects the authorisation may have.

Clause 61: Commissioner approval for authorisation to identify or confirm journalistic sources

169 Clause 61 sets out the procedure for authorising communications data requests made by public authorities, in order to identify a journalist's source. In these instances it is necessary to obtain the approval of a Judicial Commissioner before the data can be acquired.

170 Subsections (1), (2) and (3) set out that an authorised communications data application made by certain public authorities for the purpose of identifying the source of journalistic information must not take effect until approved by a Judicial Commissioner. Prior Judicial Commissioner approval is not required in an imminent threat to life situation.

171 Subsection (4) sets out that in making an application for data to identify a journalistic source, the applicant is not required to notify either the person to whom the applications relates i.e. the journalistic source, nor that person's legal representative.

172 Subsections (5) and (6) sets out that a Judicial Commissioner should only approve an authorisation to acquire communications data to identify a journalistic source if satisfied that the conditions of the authorisation by the designated senior officer have been met.

173 Subsection (6) sets out that the Judicial Commissioner must quash any authorisation given by the designated senior officer, if the Judicial Commissioner refuses to approve it.

174 Subsection (7) sets out what is meant by the "source of journalistic information". It is defined as an individual (i.e. the source) who provides material intending the recipient (i.e. the journalist) to use it for the purpose of journalism or knowing that it is likely to be used for journalism.

Clause 62 and 63: Collaborations agreements

175 Clause 63 and 64 provide for collaboration agreements that allow designated senior officers

and SPoCs to be shared between public authorities. Such agreements can be voluntary or there is a power for the Secretary of State to require them. Relevant public authorities may enter into collaboration agreements in order to pool resources during busy periods. The power to require collaboration agreements will be used to require public authorities that are less frequent users of communications data to use the expertise of designated persons and SPoCs in other public authorities who are more experienced in making applications.

Clause 64: Police collaboration agreements

176 The Police are already permitted to be in collaboration agreements and this outlines their arrangements.

Clause 65: Lawfulness of conduct authorised by this Part

177 Subsection (1) has the effect of making conduct lawful for all purposes if it is conduct in which that person is authorised to engage by virtue of an authorisation, and the conduct is in accordance with, or in pursuance of, the authorisation.

178 Subsection (2) exempts a person from civil liability in respect of conduct which is incidental to, or reasonably undertaken in conjunction with, that authorised in subsection (1). The conduct must not itself be conduct for which an authorisation or warrant:

a. is capable of being granted under the enactments referred to in subsection (3), and;

b. might reasonably have been expected to have been sought in the case in question.

Clause 66: Offence of making unauthorised disclosure

179 Clause 66 creates a criminal offence, with a maximum prison sentence of two years, if a communications services provider discloses any obligations under this Part of the Bill. It is a reasonable excuse if such a requirement is disclosed with the permission of the public authority who requested the data.

180 The intent of these provisions is to prevent the so called 'tipping-off' of criminal suspects or subjects of interest that their data has been sought, thus informing them that they are under suspicion.

181 Subsections (1) and (2) set out that employee from a communications service provider should not disclose any information about a request from a relevant public authority for communications data to a customer, without prior permission from the relevant public authority.

182 Subsection (3) sets out that the punishment for being found guilty of such an offence.

183 Subsection (4) sets out the maximum prison term for committing such an offence in England Wales, Scotland and Northern Ireland.

Clause 67: Certain transfer and agency arrangements with public authorities

184 This clause allows for the Secretary of State by making regulations to transfer ownership of the filtering arrangements to a public authority.

Clause 68: Applications of Part 3 to postal operators and postal services

185 Clause 68 provides that out that all clauses in Part 3 relating to communications service providers also apply to postal operators.

Clause 69: Extra-territorial applications of Part 3

186 Clause 69 sets out that communications service providers overseas that handle communications data of UK citizens are also covered by the provisions set out in Part 3 of the

Bill.

Clause 70: Part 3: interpretation

187 Clause 70 clarifies terms that are regularly referred to throughout Part 3 of the Bill.

Part 4: Retention of Communications Data

Clause 71: Powers to require retention of certain data

188 This clause provides a power to require communications service providers to retain communications data, where necessary and proportionate for one or more of the statutory purposes (at clause 46(7)) for which it can be acquired for a maximum period of 12 months

189 Subsection (9) specifies the communications data that can be retained by what it can be used to identify. For example, communications data can be retained if it may be used to identify, or could assist in identifying, 'the sender or recipient of a communication (whether or not a person)'. Such communications data would include phone numbers, email addresses and source IP addresses.

190 Subsection (9)(f) provides for the retention of internet connection records. Internet connection records are a record of the internet services that a specific device connects to – such as a website or instant messaging application – captured by the company providing access to the internet. They could be used, for example, to demonstrate a certain device had accessed an online communications service but they would not be able to be used to identify what the individual did on that service. Clause 47 provides certain restrictions on the acquisition of internet connection records. Clause 193 provides that in the particular context of web browsing anything beyond data which identifies the telecommunication service (e.g. bbc.co.uk) is content.

Clause 72: Matters to be taken into account before giving retention notices

191 Clause 72 sets out that before giving a retention notice to a communications service provider, the Secretary of State must take into account a number of factors. These include: the likely benefits of giving such a notice; the likely number of users of the CSP; the technical feasibility of CSPs complying with the notice; and, any other impact that the notice may have on the CSP. In addition the Secretary of State must take reasonable steps to consult a CSP before giving the notice.

Clause 73: Review by the Secretary of State

192 This clause permits the recipient of a notice to refer the notice back to the Secretary of State where the recipient of the notice considers an obligation unreasonable. Subsection (1) states that the provider will have the opportunity to refer a notice either within a specified time period or specified circumstances which will be set out in the regulations.

193 Subsection (4) states that the person is not required to comply with the specific obligations under referral until the notice has been reviewed by the Secretary of State. The actions that the Secretary of State must take in reviewing the notice and the role of the Technical Advisory Board and the Investigatory Powers Commissioner are outlined at subsections (5-8).

194 Subsection (9) requires the Commissioner and the Technical Advisory Board to consult the operator and report their conclusions to the operator and Secretary of State. After consideration of the conclusions of the Commissioner and Board, the Secretary of State may decide to confirm the effect of the notice, vary the notice or withdraw it.

195 Subsection (12) imposes an obligation on the Secretary of State to keep a notice under review, regardless of whether or not it has been referred.

Clause 74: Data integrity and security

196 This clause requires data retained by virtue of this legislation must be kept securely and, once the retention period expires, deleted in a way that ensures access is impossible.

Clause 75: Disclosure of retained data

197 Clause 75 sets out that communications service providers must put in place adequately security procedures governing the access of communications data in order to protect it against unlawful disclosure.

Clause 76: Variation or revocation of notices

198 Subsections (1)-(8) provide for the Secretary of State to vary a notice. Where a notice is varied the same considerations will apply as in the giving of a notice.

199 Subsections (9)-(12) provide for the revocation of data retention notices in full or in part.

Clause 77: Enforcement of notices and certain other requirements and restrictions

200 This clause provides a power to the Secretary of State to enforce compliance of notices and other matters by civil proceedings.

Clause 78: Application of Part 4 to public postal operators and public postal services

201 This clause specifies that the provisions of this Part also apply to postal services.

Clause 79: Extra-territorial application of Part 4

202 This provides that communications service providers based outside the United Kingdom, but providing services to customers based within the United Kingdom, can retain relevant communications data related to such customers. The communications service provider based outside the United Kingdom has a duty to give regard to the requirement but they cannot be compelled to comply with it.

Clause 80: Part 4: interpretation

203 This clause provides for interpretation of this Part, including references for relevant definitions.

Part 5: Targeted Equipment Interference Warrants

Clause 81: Warrants under this Part: general

204 Clause 81 establishes a targeted equipment interference warrant, the activities and conduct it may authorise together with the test of necessity and proportionality. Subsection (1) sets out that a targeted equipment interference warrant authorises the interference with equipment for the purpose of obtaining communications, private information or equipment data.

205 Subsection (3), (4) and (8) set out the activities that an equipment interference warrant may authorise. An equipment interference warrant may authorise the recipient to obtain (subsection (3)(a)), disclose (subsection (3)(b)), monitor (subsection (4) and examine (subsection (9)) any communications, private information and equipment data. Subsection (5) provides that any conduct necessary by any person, or a requirement on any person in the warrant, can be carried out in order to give effect to an equipment interference warrant.

206 Subsection (6) of this clause ensures that an equipment interference warrant is not able to permit activity that should be carried out under an interception warrant. If an investigation requires both equipment interference and interception techniques then a combined warrant may be issued.

Clause 82: Meaning of "equipment data"

207 This clause defines the material which is equipment data in relation to a targeted equipment interference warrant. Equipment data includes:

a. Communications data (see clause 193);

b. Data which enables or otherwise facilitates the functioning of any system or any service provided by means of the system

c. Data which is included in or associated with a communication or an item or private information and either:

i. Does not form part of the content of the communication or the item of private information, or

ii. If it does:

1. Can be logically extracted from the content of any communication or piece of private information;

2. Which does not, once extracted, convey the meaning of any communication or piece of private information; and

3. Can identify, or assist in identifying, any person, apparatus, system or service, or which describes an event, or the location of any person, event or thing.

208 This definition provides a distinction between different types of data that may be obtained from equipment interference, allowing appropriate restrictions to be applied to the selection for examination of the more intrusive data. This ensures that if an equipment interference operation gathers data of a UK person, their personal communications are subject to the same strict authorisation process that applies to targeted equipment interference warrants. All material obtained under targeted and bulk equipment interference warrants will be subject to the stringent handling safeguards as out in Part 5 of the Bill.

209 Related communications data obtained under a bulk interception warrant is equivalent to related communications data obtained under a targeted interception warrant, and equipment data obtained pursuant to an equipment interference warrant.

210 In addition to communications data held on the device the data falling within this category could include:

a. The name of the person or account who stored a file on the device;

b. the time and date of any files on the device were created or last modified;

c. the operating system of the device and when it was last updated.

211 Subsection (8) provides a definition of the content of any communication or item of private information based around the meaning of the communication or item of private information excluding any meaning that can be inferred from the fact of the communication or existence of the item of information.

Clause 83: Subject-matter of warrants

212 This clause sets out the scope of equipment interference warrants. For interference to be considered targeted it must relate to a particular person or persons (so for example, the computer equipment of Person X); organisation or organisations (so, for example, the computer equipment of Organisation X); a particular location where the equipment being

interfered with is present (so for example, computer equipment located at House X); or equipment that is being used for testing and development. The targeted equipment interference warrant may also relate to equipment where there is a common link between multiple people, locations or organisations where the interference is for the purpose of the same investigation or operation (so, for example, computers believed to being used by Terrorist Plot Group X), or equipment that is being used for a particular activity . These latter warrants have sometimes been described as 'thematic'.

Clause 84: Power to issue warrants to intelligence services: the Secretary of State

213 Clause 84 establishes the process and requirements for equipment interference warrants that are applied for and issued to a director of one of the intelligence services. The intelligence services comprise the Security Service (MI5), the Secret Intelligence Service and Government Communication Headquarters (GCHQ).

214 Subsection (1) sets out that equipment interference warrants issued to the intelligence services must be necessary for one of three statutory purposes, set out in full in subsection (4). Either the warrant must be in the interest of national security, for the purposes of preventing or detecting serious crime, or in the interests of the economic wellbeing of the United Kingdom so far as those interests are also relevant to the interests of national security.

215 Subsection (1) also sets out that it is permitted for a warrant to be applied for on behalf of the head of one of the services, meaning it is not necessary for every warrant application to be made personally by the head of service. Subsection (7) states that when a warrant is applied for on behalf of a head of service the application must be made by a person holding office under the Crown.

216 Subsection (2) prevents the Secretary of State issuing a warrant that relates to serious crime in Scotland. This is because Scotland have devolved responsibility for matters relating to crime. Clause 86 addresses the process for such warrants.

217 Subsections (3) and (6) together ensure that the a warrant may only be issued if the Secretary of State believes that the activity set out in the warrant is proportionate to the intended outcome and that there is not a reasonable alternative method to achieving the same outcome.

Clause 85: Additional protection for Members of Parliament etc.

218 This clause requires the Secretary of State to consult the Prime Minister before deciding to issue a targeted equipment interference or examination warrant where the purpose may be to obtain the communications of a person who is a member of a relevant legislature. Subsection (3) defines "member of a relevant legislature".

Clause 86: Power to issue warrants to intelligence services: the Scottish Ministers

219 Clause 86 explains that when a targeted EI warrant – for the purpose of preventing and detecting serious crime - relates to interference with equipment believed to be in Scotland, it is the responsibility of Scottish Ministers, rather than the Secretary of State, to issue the warrant. This only applies to the intelligence services, as law enforcement agencies will apply to their chief constable, or equivalent. The same consideration of necessity and proportionality still applies as set out in (1) (b) and (c) and the same independent judicial approval process will follow, should the warrant be issued.

Clause 87: Power to issue warrants to the Chief of Defence Intelligence

220 Clause 87 makes provision for the Chief of Defence Intelligence to apply for equipment interference warrants. The same restrictions as outlined in clause 84(1) apply but in respect to the Chief of Defence Intelligence, with approval also dependent upon the Secretary of State's acceptance. The exception in this instance is that warrants issued to the Chief of Defence

Intelligence are reserved for national security purposes.

Clause 88: Decision to issue warrants under sections 84 to 87 be taken personally by Ministers

221 Clause 88 states that the Secretary of State or Scottish Minister must be the decision maker and signatory of any warrant issued under this power to the intelligence services and defence intelligence. This ensures that they are accountable for the use of this power and have the opportunity in all cases to ensure that its use is necessary and proportionate.

222 There are some instances in which the Secretary of State or Scottish Minister will not be able to physically sign a warrant in sufficient time to allow crucial operations to take place. In these circumstances a designated senior official will sign the warrant, as per subsections (3) and (4) (b). The Secretary of State or Scottish Minister is still the decision maker in these instances and will confirm verbally with the designated official that he or she is in agreement that the warrant is to be signed.

> Example:
> A person has been kidnapped and a ransom is being demanded with the threat that the individual will be shot imminently. In such urgent threat to life cases, especially outside of normal working hours, it may not be possible or practical for the Secretary of State to physically sign a warrant.

Clause 89: Power to issue warrants to law enforcement officers

223 Clause 89 establishes the process and requirements for equipment interference warrants that are applied for by law enforcement officers and issued by a law enforcement chief.

224 Subsection (1) sets out the conditions that must be met for a law enforcement chief to issue a targeted equipment interference warrant. Subsections (1)(a) and (1)(b) establish the tests of necessity and proportionality, with subsection (1)(a) providing that the purpose of a warrant being necessary to prevent and detect serious crime. In other words, a law enforcement chief may only issue a targeted information warrant if he believes that the warrant is necessary to prevent and detect serious crime and that the conduct authorised is proportionate. Subsection (1) (d) provides that all decisions to issue a warrant require the approval of a Judicial Commissioner, except where the law enforcement chief believes there is an urgent case to issue the warrant. The process for urgent warrants is covered at clause 91. Subsection (1)(c) provides that in order to issue a warrant a law enforcement chief must be satisfied that satisfactory arrangements are in place to safeguard the material obtained (as detailed in clause 101).

225 Subsection (2) provides that a law enforcement chief may delegate the power to issue a targeted equipment interference warrant to an appropriate delegate. The power to issue warrants should usually only be delegated in urgent cases, and only when it is not reasonably practical for a law enforcement chief to consider the application and issue the warrant. The appropriate delegates in each law enforcement agency that can apply for an equipment interference warrant is detailed in the table at subsection (3) including details of other statutory delegation arrangements (such as for the Director General of the National Crime Agency).

226 Subsection (3) sets out the different roles and responsibilities that fall within the categories of law enforcement chief, appropriate delegate, and law enforcement officer for all the law enforcement agencies that may apply for an equipment interference warrant.

227 Subsection (4) sets out the additional arrangements for the applications and issuing of equipment interference warrants where a police force is a collaborative force under section 22A

of the Police Act 1996.

228 Subsection (5) sets out the definition of a police force in Part 5.

229 Subsection (6) provides that the reference to the purpose of preventing and detecting serious crime in subsection (1)(a), in the case of the Police Service of Northern Ireland, should also be read as a reference to the interests of national security.

Clause 90: Approval of warrants by Judicial Commissioners

230 This clause explains the role of a Judicial Commissioner in targeted equipment interference warrants. Subsection (1) reiterates the same test of necessity and proportionality that the Secretary of State, Scottish Minister or law enforcement chief will have applied when issuing the warrant. The Judicial Commissioner, as per subsection 89 (2), will apply the same principles as they would apply in a judicial review and determine whether the person issuing the warrant has properly considered the necessity and proportionality of the operation or investigation.

231 Following their considerations a Judicial Commissioner can approve the warrant, refuse to approve the warrant or refer the warrant to the Investigatory Powers Commissionerfor further consideration.

232 Subsections (4) and (5) set out that should a warrant be refused by a Judicial Commissioner they must give written reasons for the refusal to the applicant. Should the person requesting the warrant so wish they may then refer the application to the Investigatory Powers Commissioner for their opinion.

Clause 91: Approval of warrants issued in urgent cases

233 Clause 91 establishes the process for the approval of equipment interference warrants in urgent cases. These are warrants that will be issued in cases that demand very quick actions from the applicant that cannot wait until a Judicial Commissioner has approved the warrant. For example, in a serious crime context an urgent warrant may be required if a law enforcement agency understands that a person's life is in immediate danger and equipment interference would obtain the communications etc, that may be used to prevent imminent harm. These warrants will still be issued by the Secretary of State or law enforcement chief. In the case of the intelligence agencies and Defence Intelligence there may be urgent circumstances where the warrant may be signed by a designated official on behalf of the Secretary of State. In those circumstances it will still be incumbent on the Secretary of State to make the decision to issue the warrant before authorising the designated official to sign the warrant.

234 Subsections (2) to (6) set out the role of the Judicial Commissioner once a warrant has been issued through the urgent process. It is the duty of the person who issues an urgent warrant to inform the Judicial Commissioner that they have done so. This will prompt the Judicial Commissioner to either approve the warrant, allowing it to continue to have effect; or refuse to approve the warrant, in which case the activity described within the warrant should cease. This process must not exceed 5 working days.

235 If the Judicial Commissioner neither approves nor refuses to approve an urgent warrant it will cease to have effect five working days from the date that it was issued – this is described in subsection (3).

Clause 92: Warrants ceasing to have effect under section 91

236 This clause details the process that follows when a warrant is refused by a Judicial Commissioner, having previously been issued under urgent provisions.

237 The Judicial Commissioner has responsibility for determining what should be done with the

data obtained up to this point. In all instances this will be the same Judicial Commissioner (or the Investigatory Powers Commissioner) that refused the warrant.

238 Subsection (3) explains that a Judicial Commissioner has the power to authorise additional equipment interference after refusing to approve a warrant, where such interference will enable any ongoing or future interference to cease as soon as possible.

239 Subsection (8) clarifies that if a warrant is refused, or not approved, the actions carried out whilst the warrant was active are not made invalid or unlawful by the ceasing of the warrant. This ensures that the recipient and their delegated officials can act appropriately and with confidence as soon as the urgent warrant is issued.

Clause 93: Requirements that must be met by warrants

240 Clause 93 directs the warrant applicant to include a description of what activity the warrant will be intended to facilitate. The applicant will also explain why the warrant is needed, provide an understanding of who the warranted activity will effect and describe the techniques that will be used to effect the warrant. This is the information that the Secretary of State or law enforcement chief and Judicial Commissioner will use whilst considering whether the activity is necessary and proportionate when compared to the expected outcome.

Clause 94: Duration of warrants

241 Subsection (2) sets the standard duration of a warrant at 6 months. It also states when that 6 months begins, both for the initial warrant and any subsequent renewals. An exception applies for urgent warrants, which are described in subsection (3) and last for five working days.

Clause 95: Renewal of warrants

242 Subsections (1), (2) and (3) state that at any time before the warrant expires a renewal can be issued by the Secretary of State, Scottish Minister or law enforcement chief where relevant. In either case a Judicial Commissioner will also need to approve the renewal of the warrant. The person renewing the warrant will at this stage need to confirm that the activity described in the warrant remains necessary and proportionate.

243 Subsections (5) (6) and (7) ensures that any renewals are done personally by the Secretary of State, law enforcement officer or Scottish Minister where relevant. This provides the opportunity to review the necessity and proportionality of the action. The warrant will not be renewed if the action is no longer necessary or proportionate.

244 In the context of urgent warrants, renewals serve the purpose of allowing the Secretary of State, law enforcement chief or Scottish Minister and a Judicial Commissioner to review the warrant and, should they consider it necessary and proportionate, extend the duration to 6 months.

Clause 96: Modifications of warrants

245 This clause addresses the possibility that warrants may need to be modified. For instance this may be when different action is required to progress the investigation because, for example, the target of the investigation has a new smart phone) or when new subjects of interest become relevant to the investigation.

246 Subsection (2) sets out the different elements of a warrant that are subject to modification. These elements have the potential to change as an operation or investigation develops.

247 Modifications can also include the removal of subjects from a warrant. This may occur if an operation determines that one or more of the subjects are not of intelligence interest, but other subjects also on the warrant remain of interest. In this instance the Secretary of State or Scottish

Minister, or a designated senior official, can remove the unnecessary subjects from the warrant, minimising any incursions in to their privacy. In the case of warrants issued by law enforcement chiefs such modifications will be made by the relevant law enforcement chief or a designated official, with approval from a Judicial Commissioner, as explained in subsection (3).

248 Subsection (6) makes clear that all modifications to equipment interference must be approved by a Judicial Commissioner. This ensures that once a warrant has been approved by a Judicial Commissioner any changes that may alter the effects of the warrant are also visible and can, if necessary, be refused.

Clause 97: Modification of warrants: supplementary provision

249 This clause sets out that only the warrant granter, or a designated official, are able to enact modifications to targeted equipment interference warrants. In cases when a modification is enacted by a senior official they have a duty under subsections (2) and (3) to inform the Secretary of State/Scottish Minister.

Clause 98: Cancellation of warrants

250 This clause sets out that a Secretary of State, Scottish Minister, law enforcement chief or designated senior official in a warrant granting department has the power to cancel a warrant at any time, if the warrant was originally issued by their organisation.

251 Subsection (2) makes it a requirement that once a warrant is no longer necessary, or if through a change of circumstance the conduct is no longer proportionate, the appropriate person must cancel that warrant. This provision will ensure that equipment interference is not able to continue for any longer than is strictly necessary, minimising any potential incursions of privacy.

Clause 99: Implementation of warrants

252 Subsection (1) gives the recipient of the warrant the power to work with others to carry out the actions outlined in the warrant. Subsection (2) specifies that the warrant recipient can serve a copy of the warrant to a person if they think that the person is able to help them carry out the warranted actions.

Clause 100: Service of warrants

253 This clause sets out how a targeted equipment interference warrant may be served upon a person outside the United Kingdom when the warrant recipient requires their assistance. Subsection (2) sets out the three possible options for serving a warrant in this situation. Subsection (3) states that the third option set out in subsection (2) – to make the warrant available for inspection in the United Kingdom – should not be used unless the options under subsection (2) (a) and (b) are not reasonably practicable.

Clause 101: Duty of telecommunications providers to assist with implementation

254 Clause 101 places a duty upon telecommunications providers to assist with the implementation of targeted equipment interference if they are served with a copy of a warrant by the warrant recipient.

255 Subsections (1) (2) and (3) set out that this duty is limited to a selection of organisations that mirrors the agencies permitted to use interception techniques. In all cases the Secretary of State or Scottish Minister will approve the proposed interference, even if the normal warrantry process would not require their involvement (for instance, for warrants issued to law enforcement officers).

256 Subsection (7) provides that the duty to comply with a warrant is enforceable by civil

proceedings brought by the Secretary of State.

Clause 102: Offence of making unauthorised disclosure

257 Clause 102 details the requirement for telecommunications providers to not disclose the existence of any equipment interference warrant that they may be required to assist with to the subject of that warrant.

258 Subsection (2) gives the warrant recipient the power to allow the telecommunications provider to disclose the existence and nature of the warrant should they need to.

Clause 103: Safeguards for material obtained

259 Clause 103 places a duty on the warrant requestor to ensure safeguards are in place for any data acquired by the activity permitted through that warrant. This is intended to protect the privacy of anyone affected by a warrant and maintain the integrity of the operations to which a warrant relates.

260 Subsection (6) defines appropriate authority, which means that the Secretary of State or Scottish Ministers must be satisfied that adequate arrangements are in place for warrants issued under clauses 84-87. For warrants issued under clause 89, it is for the person to whom the warrant is addressed (the law enforcement officer) to ensure arrangements are in place.

Clause 104: Restriction on issue of targeted equipment interference warrants to certain law enforcement officers

261 Clause 104 established the jurisdiction of equipment interference warrants for law enforcement officers, with restrictions applying to UK police forces. The limitations rest on the activity having a connection to the British Islands

262 Subsection (1) provides that UK police forces may only apply for an equipment interference warrant where there is a connection to the British Islands. A UK police force is a police force maintained under section 2 of the Police Act 1996, the Metropolitan Police force, the City of London Police, the Police Service of Scotland and the Police Service of Northern Ireland.

263 Subsection (2) described a connection to the British Islands as:

a. the proposed activity would take place in the British Islands (regardless of where the equipment to be interfered with is located); or

b. the UK police force believes the equipment to be interfered with may be located in the British Islands at some point during the interference itself. The computer would be located in the British Islands or carried by someone transiting through the British Islands at the time the interference is taking place; or

c. the purpose of the interference is to enable the acquisition of the private information or the communications sent to or from a person believed to be in the British Islands. The interference is aimed at a person in the British Islands.

264 Subsection (3) provides that all other law enforcement officers are able to apply for an equipment interference warrant under section 85 [j905] in circumstances where there is a connection to the British Islands and also where there is no connection to the British Islands. Subsection (3) applies to the National Crime Agency, HM Revenue and Customs, Ministry of Defence Police, Royal Military Police and the Royal Air Force Police.

Clause 105: Part 5: Interpretation

265 Clause 105 provides definitions for 'communications', 'equipment', 'private information' and 'senior official' that ensure that all intended applications of equipment interference are

captured under the powers set out in this Bill.

Part 6: Bulk Warrants

Chapter 1: Bulk interception warrants

Clause 106: Bulk interception warrants

266 This clause describes a bulk interception warrant and sets out the two conditions that a warrant issued under this chapter must meet.

267 Subsection (2) limits the main purpose for which a warrant may be sought to obtaining overseas-related communications or the obtaining of related communications data from such communications. This prevents the issue of a bulk interception warrant with the primary purpose of obtaining communications between people in the British Islands.

268 Subsection (3) defines "overseas-related communications" as communications that are sent or received by persons outside of the British Islands.

269 Subsection (4) sets out the conduct that may be authorised under a bulk interception warrant in order to intercept overseas-related communications or related communications data.

270 Subsection (5) sets out the conduct that a bulk interception warrant authorises, other than the conduct described in the warrant itself. This might include the interception of communications between persons in the British Islands if that interception is unavoidable in order to achieve the main purpose of the warrant.

> Example:
> A bulk warrant is sought for the interception of communications. The primary objective of the warrant is to obtain the communications of persons believed to be outside the UK, which are likely to be of national security interest and may be selected for examination subsequently. Due to the nature of internet-based communications, it is inevitable that some communications between persons in the UK will also be intercepted. In order to examine those communications, a targeted examination warrant must be sought. This will need to be issued by the Secretary of State and approved by a judge.

271 Subsections (6)-(9) define what related communications data is in relation to a bulk interception warrant. In contrast to the position for targeted warrants, the data may (but need not) be obtained by, or in connection with, interception. Related communications data includes:

a. Communications data (see clause 193);

b. Data obtained through a warrant which enables or otherwise facilitates the functioning of any telecommunications system or any telecommunications service provided by means of the system;

c. Data which:

   i. Can be logically extracted from the content of the communication;

   ii. Which does not, once extracted, reveal the meaning of the content of the

communication; and

iii. Can identify, or assist in identifying, any person, apparatus, telecommunication system or telecommunications service, or which describes an event, or the location of any person, event or thing.

272 Related communications data as defined in this clause may only be obtained under a bulk interception warrant and, once the data is obtained, will be subject to the safeguards set out in Chapter 1 of Part 6.

273 Related communications data obtained under a bulk interception warrant is equivalent to related communications data obtained under a targeted interception warrant, and equipment data obtained pursuant to an equipment interference warrant.

274 This clause makes clear that the extraction of any data from the content of a communication that has been acquired during the course of its transmission can only take place under an interception warrant.

275 In addition to communications data the data falling within this category could include:

a. The version of the app sending the message;

b. Data relating to any files attached to a message such as the date and time it was created and the author;

c. Any location information related to the communication, for example the location required to enable an application;

d. Any email addresses contained within a communication.

Clause 107: Power to issue bulk interception warrants

276 This clause sets out the power to issue bulk interception warrants. Subsections (1) to (7) set out the power for the Secretary of State to issue a bulk interception warrant, only where it is necessary and proportionate, which must also be approved by a Judicial Commissioner, on behalf of an intelligence agency for one or more specified statutory purposes. The interests of national security must always be one of those purposes.

277 Subsection (1) also requires the Secretary of State to believe it is necessary to examine material obtained under the warrant for specified Operational Purposes. This will provide a detailed list of purposes for which examination of intercepted material may be necessary. Before selecting any material for examination, a member of an intelligence service will need to be sure that the examination is necessary for one of those purposes.

278 Subsection (5) requires the Secretary of State, when considering whether the warrant is necessary and proportionate, to take into account whether the information it is thought necessary to obtain under the warrant could reasonably be obtained by other means.

Clause 108: Additional requirements in respect of warrants affecting overseas operators

279 This clause outlines the requirements relating to warrants that the Secretary of State believes are likely to require the assistance of a telecommunications operator who is based outside the United Kingdom to give effect to the warrant.

280 Subsection (2) requires that the Secretary of State must consult the relevant telecommunications operator before issuing the warrant.

281 Subsection (3) sets out factors that must be taken into account before issuing the warrant in

those cases. These include costs and technical feasibility, as well as the likely benefits of the warrant.

Clause 109: Approval of warrants by Judicial Commissioners

282 Subsection (1) sets out the matters that must be reviewed by a Judicial Commissioner when deciding whether to approve a bulk interception warrant, including a consideration of necessity and proportionality and the necessity of the operational purposes.

283 Subsection (2) requires that, in determining the matters in subsection (1), a Judicial Commissioner must apply judicial review principles.

Clause 110: Decisions to issue warrants to be taken personally by Secretary of State

284 This clause requires the Secretary of State personally to take the decision to issue a bulk interception warrant and that the warrant must be signed by the Secretary of State before it can be issued.

Clause 111: Requirements that must be met by warrants

285 This clause sets out the information which must be contained in a bulk interception warrant. Subsection (3) requires that a warrant must set out the Operational Purposes for which any intercepted material, or related communications data, obtained under the warrant can be examined.

Clause 112: Duration of warrants

286 This clause sets out the details surrounding the duration of a bulk interception warrant. Bulk interception warrants will last for six months, beginning on the day the warrant was issued.

Clause 113: Renewal of warrants

287 This clause sets out the conditions for renewing a bulk interception warrant. The decision to renew a bulk interception warrant must be taken personally by the Secretary of State.

288 Subsection (2) sets out the conditions that must be met for a warrant to be renewed. These include that the Secretary of State believes that the warrant continues to be necessary and proportionate in relation to relevant statutory purpose(s) and that the decision to renew the warrant has also been approved by a Judicial Commissioner.

Clause 114: Modification of warrants

289 This clause sets out the conditions for modifying a bulk interception warrant.

290 Subsection (2) specifies that the only modifications that may be made under this section are adding, varying or removing any Operational Purpose specified in the warrant.

291 Subsection (4) requires that any modification to add or vary an Operational Purpose must be made by a Secretary of State and approved by a Judicial Commissioner.

292 Subsection (6) provides for a senior official, acting on behalf of the Secretary of State, to make a modification where an Operational Purpose is being removed. Subsection (8) requires that, where this is the case, the Secretary of State must be personally notified of the modification, as well as the reasons for making it.

Clause 115: Cancellation of warrants

293 This clause sets out the circumstances under which a bulk interception warrant may be cancelled.

294 Subsection (2) requires that where a Secretary of State or senior official decides the warrant is no longer necessary, or the conduct authorised by it is no longer proportionate, they must

cancel the warrant.

Clause 116: Implementation of warrants

295 This clause sets out the requirements for giving effect to a bulk interception warrant. This replicates the provisions relating to the implementation of a targeted interception warrant.

Clause 117: General safeguards

296 This clause sets out the general safeguards which apply to bulk interception warrants. This replicates the general safeguards which apply to the handling of targeted interception warrants.

Clause 118: Safeguards relating to disclosure of material or data overseas

297 This clause sets out the safeguards relating to the disclosure of intercept material overseas in relation to a bulk interception warrant. This replicates the safeguards for overseas disclosure in relation to targeted interception warrants.

Clause 119: Safeguards relating to examination of material or data

298 This clause sets out the safeguards relating to the examination of intercepted material and related communications data which has been acquired under a bulk interception warrant. Subsection (1) requires that intercepted material and related communications data may only be examined for specified purposes and must be necessary and proportionate. Subsection (2) explains that examination is for specified purposes if material or data is only examined in so far as is necessary for the Operational Purposes specified in the warrant.

299 Subsection (4) places a prohibition on selecting intercepted material for examination if any criteria used for the selection of that material refer to an individual known to be currently in the British Islands and are aimed at identifying the content of communications sent by or intended for that individual. Where such examination is required, a targeted examination warrant must be obtained, issued by the Secretary of State and approved by the Judicial Commissioner.

> Example:
> A member of an intelligence service is investigating an international terrorist group and one of that group regularly travels to the UK. In order to enable the selection of that person's communications for examination, including during the periods when he is in the UK, a targeted examination warrant must be sought. This will need to be issued by the Secretary of State and approved by a judge.

300 Subsection (5) deals with cases in which there is a change of circumstances such that a person whose communications were being selected for examination is discovered to be in the British Islands or has entered the British Islands. In those cases, a senior official may authorise the continued selection for examination for a period of five days. Any selection after that point will require the issue of a targeted examination warrant.

> Example:
> A member of an intelligence service is investigating an international terrorist group and suddenly one of that group is discovered to have arrived in the UK. In order to continue investigating that member of the

group a senior official must authorise further selection. This authorisation only lasts for five days, after which the selection for examination of his communications must cease or a targeted examination warrant must be sought. This will need to be issued by the Secretary of State and approved by a judge before any further selection is permitted.

Clause 120: Application of other restrictions in relation to warrants

301 This clause sets out that the exclusion of matters from legal proceedings apply to bulk interception warrants. The duty not to make unauthorised disclosure also applies to bulk interception warrants.

Clause 121: Chapter 1: interpretation

302 This clause defines various terms relating to bulk interception warrants which are used in this chapter.

Chapter 2: Bulk acquisition warrants

Clause 122: Power to issue bulk acquisition warrants

303 Subsection (1) sets out the power for the Secretary of State to issue a bulk acquisition warrant, only where it is necessary and proportionate, which must be approved by a Judicial Commissioner, on behalf of an intelligence agency for one or more specified statutory purposes. The interests of national security must always be one of those purposes.

304 Subsection (1) also requires the Secretary of State to believe it is necessary to examine material obtained under the warrant for specified operational purposes. This will provide a detailed list of purposes for which examination of bulk communications data may be necessary. Before selecting any material for examination, a member of an intelligence service will need to be sure that the examination is necessary for one of those purposes.

305 Subsection (4) requires the Secretary of State, when considering whether the warrant is necessary and proportionate, to take into account whether the information it is thought necessary to obtain under the warrant could reasonably be obtained by other means.

306 Subsection (5) describes a bulk acquisition warrant. Subsection (6) sets out that the warrant authorises requiring a telecommunications operator to disclose specified communications data in its possession or obtain and disclose communications data which is not in its possession; the selection for examination of the data obtained under the warrant and the onward disclosure of such data.

307 Subsection (7) provides for a bulk acquisition warrant to authorise conduct necessary to do what is required by the warrant.

308 Subsection (8) provides that a bulk acquisition warrant may be issued on a forward looking basis.

Clause 123: Approval of warrants by Judicial Commissioners

309 Subsection (1) sets out the matters that must be reviewed by a Judicial Commissioner when deciding whether to approve a bulk acquisition warrant, including a consideration of necessity and proportionality and the necessity of the operational purposes.

310 Subsection (2) requires that, in determining the matters in subsection (1), a Judicial Commissioner must apply judicial review principles.

311 Where a Judicial Commissioner refuses to approve a warrant they must set out written reasons for their refusal. This will allow the agency requesting the warrant to alter their application and what action they are seeking to take in order to meet any concerns expressed by the Judicial Commissioner.

312 Should a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuse to approve a decision to issue a warrant the Secretary of State may escalate the case to the Investigatory Powers Commissioner and ask them to approve the decision to issue the warrant. Should the Investigatory Powers Commissioner refuse to approve the warrant then there is no further right of appeal from that decision.

Clause 124: Decisions to issue warrants to be taken personally by Secretary of State

313 This clause requires that the decision to issue a bulk acquisition warrant must be taken by the Secretary of State and that the Secretary of State must sign the warrant before it is issued.

Clause 125: Requirements that must be met by warrants

314 This clause requires an application for the issue of a bulk acquisition warrant to be made by or on behalf of the head of an intelligence agency and that the warrant must be addressed to the intelligence agency which made the application.

315 Subsection (3) requires a warrant to identify the operational purposes for which data can be examined and selected for examination. Subsection (4) sets out the scope of operational purposes.

Clause 126: Duration of warrants

316 This clause sets out that a bulk acquisition warrant has a duration of 6 months from the date of issue or, in the case of a renewed warrant from the day after it would otherwise have expired.

Clause 127: Renewal of warrants

317 This clause sets out the conditions for renewing a bulk interception warrant. The decision to renew a bulk acquisition warrant must be taken personally by the Secretary of State.

318 Subsection (2) sets out the conditions that must be met for a warrant to be renewed. These include that the Secretary of State believes that the warrant continues to be necessary and proportionate in relation to relevant statutory purpose(s) and that the decision to renew the warrant has also been approved by a Judicial Commissioner.

Clause 128: Modification of warrants

319 This clause sets out the conditions for modifying a bulk acquisition warrant.

320 Subsection (2) specifies that the only modifications that may be made under this section are adding, varying or removing any operational purpose specified in the warrant.

321 Subsection (4) requires that any modification to add or vary an operational purpose must be made by a Secretary of State and approved by a Judicial Commissioner.

322 Subsection (6) provides for a senior official, acting on behalf of the Secretary of State, to make a modification where an operational purpose is being removed. Subsection (8) requires that, where this is the case, the Secretary of State must be personally notified of the modification, as well as the reasons for making it.

Clause 129: Cancellation of warrants

323 This clause sets out the circumstances under which a bulk acquisition warrant may be cancelled.

324 Subsection (2) requires that where a Secretary of State or senior official decides the warrant is no longer necessary, or the conduct authorised by it is no longer proportionate, they must cancel the warrant.

Clause 130: Implementation of warrants

325 This clause sets out how a bulk acquisition warrant is implemented, including assistance with giving effect to the warrant and how the warrant may be served, with reference to the applicable provision relating to the implementation of a targeted interception warrant. Subsection (6) provides that the duty to comply with a warrant is enforceable by civil proceedings brought by the Secretary of State.

Clause 131: General safeguards

326 This clause sets out the safeguards which apply to bulk acquisition warrants. Subsection (2) and (3) require the Secretary of State concerned ensure arrangements are in place to limit the disclosure of data to that which is required for an authorised purpose and that data is only held securely and destroyed when there are no longer grounds for retaining it. Subsection (6) provides protection for data disclosed to authorities of a country or territory outside the UK.

Clause 132: Safeguards relating to examination of data

327 This clause provides that data obtained under a warrant may only be examined in accordance with the warrant.

Clause 133: Offence of making unauthorised disclosure

328 This clause makes it an offence for persons specified in subsection (1) to make an unauthorised disclosure to another person in relation to a bulk acquisition warrant. Subsection (2) lists the circumstances where disclosure is authorised. Subsection (3) sets out the maximum penalties for the offence.

Clause 134: Chapter 2: interpretation

329 This clause defines the terms used in this Chapter.

Chapter 3: Bulk Equipment Interference Warrants

Clause 135: Bulk equipment interference warrants

330 Clause 135 sets out the characteristics of bulk equipment interference. Unlike the equipment interference described in Part 5 bulk equipment interference is not targeted against particular person(s), organisation(s) or location(s) or against equipment that is being used for particular activities.

Clause 136: Meaning of "equipment data"

331 This clause defines the material which is equipment data in relation to a bulk equipment interference warrant. Equipment data includes:

a. Communications data (see clause 193);

b. Data which enables or otherwise facilitates the functioning of any system or any service provided by means of the system;

c. Data which is included in or associated with a communication or an item or private information and either:

i. Does not form part of the content of the communication or the item of private information, or

ii. If it does:

1. Can be logically extracted from the content of any communication or piece of private information;

2. Which does not, once extracted, convey the meaning of any communication or piece of private information; and

3. Can identify, or assist in identifying, any person, apparatus, system or service, or which describes an event, or the location of any person, event or thing.

332 This definition provides a distinction between different types of data that may be obtained from equipment interference, allowing appropriate restrictions to be applied to the selection for examination of the more intrusive data. This ensures that if an equipment interference operation gathers data of a UK person, their personal communications are subject to the same strict authorisation process that applies to targeted equipment interference warrants. All material obtained under targeted and bulk equipment interference warrants will be subject to the stringent handling safeguards as out in Chapter 3 of Part 6 of the Bill.

333 Related communications data obtained under a bulk interception warrant is equivalent to related communications data obtained under a targeted interception warrant, and equipment data obtained pursuant to an equipment interference warrant.

334 In addition to communications data held on the device the data falling within this category could include:

a. The name of the person or account who stored a file on the device;

b. The time and date of any files on the device were created or last modified;

c. The operating system of the device and when it was last updated.

335 Subsection (8) provides a definition of the content of any communication or item of private information based around the meaning of the communication or item of private information excluding any meaning that can be inferred from the fact of the communication or existence of the item of information.

Clause 137: Power to issue bulk warrants

336 This clause sets out the power to for the Secretary of State to issue a bulk equipment interference warrant, only where it is necessary and proportionate, which must be approved by a Judicial Commissioner, on behalf of an intelligence agency for one or more specified statutory purposes. The interests of national security must always be one of those purposes. It also requires the Secretary of State to believe it is necessary to examine material obtained under the warrant for specified Operational Purposes. Only three authorities may apply for a bulk equipment interference warrant - the Security Service, the Secret Intelligence Service and GCHQ.

Clause 138: Approval of warrants by Judicial Commissioners

337 Subsection (1) sets out the matters that must be determined by a Judicial Commissioner when deciding whether to approve a bulk equipment interference warrant, including a consideration of necessity and proportionality.

338 Subsection (2) requires that, in determining the matters in subsection (1), a Judicial Commissioner must apply judicial review principles.

339 Subsections (3) and (4) set out that a Judicial Commissioner can either approve a warrant,

refuse to approve a warrant or refer the application to the Investigatory Powers Commissioner for further consideration.

Clause 139: Decisions to issue warrants to be taken personally by Secretary of State

340 This clause ensures that the decision to issue a bulk equipment interference warrant may only be taken by a Secretary of State. Subsection (2) sets out that the warrant must also be subsequently signed by the Secretary of State.

Clause 140: Requirements that must be met by warrants

341 This clause sets out the information which must be contained in a bulk equipment interference warrant.

342 Subsection (3) requires the person requesting a warrant to set out specifically what the purpose/s are for which the selection for examination of the material from the interference is necessary. The person requesting the warrant might for example state that the proposed interference will be used to gather intelligence relating to terrorism in a particular country.

Clause 141: Duration of warrants

343 This clause sets out the details surrounding the duration of a bulk equipment interference warrants. Upon approval, bulk equipment interference warrants will last for a maximum of six months.

Clause 142: Renewal of warrants

344 This clause sets out the conditions for renewing a bulk equipment interference warrant. The decision to renew a bulk equipment interference warrant must be taken personally by the Secretary of State. The six month period between renewals ensures that the Secretary of State will periodically review whether a warrant is still necessary should the agency wish to renew. An independent Judicial Commissioner will also review any warrants submitted for renewal.

Clause 143: Modification of warrants

345 This clause sets out the conditions for modifying a bulk equipment interference warrant. Any modifications to the stated purposes of the interference will be enacted by the Secretary of State with approval of a Judicial Commissioner, maintaining the authorisation level that applied to the original warrant application. If the requested modification is to remove a stated purpose the Secretary of State may delegate a senior official for this task, as set out in subsection (6). If a senior official makes a modification they must inform the Secretary of State of this change.

Clause 144: Cancellation of warrants

346 This clause sets out the circumstances under which a bulk equipment interference warrant may be cancelled.

347 Subsection (2) ensures that if an appropriate person is satisfied that the warrant is no longer required, they must cancel it. This may include a designated senior official in the warrant granting department, or in the warrant requesting agency.

Clause 145: Implementation of warrants

348 This clause sets out the requirements for giving effect to a bulk equipment interference warrant. This replicates the provisions relating to the implementation of a targeted equipment interference warrant and ensures that a person to whom the warrant is addressed may work with others to effect the activity described within it.

349 Subsection (4) states that the same provision for targeted equipment interference that allows a warrant holder to compel a telecommunications provider to assist in the implementation of

warranted activity applies in the same way for bulk equipment interference.

Clause 146: General safeguards

350 This clause sets out the general safeguards which apply to bulk equipment interference warrants. This replicates the general safeguards which apply to the handling of targeted equipment interference warrants.

351 The clause ensures that any disclosure of the information obtained through bulk equipment interference is kept to a minimal amount. Any copies of the information are also kept to a minimum. However subsection (4) states that the disclosure of material obtained through these methods is permitted in the interest of legal proceedings. This ensures that the product of bulk equipment interference activities can be used as evidence, should it be required.

352 Subsection (7) sets out that should the information obtained be shared with authorities outside of the United Kingdom, that equivalent measures are in place.

Clause 147: Safeguards relating to examination of material etc

353 This clause sets out the safeguards relating to the examination of material which has been acquired under a bulk equipment interference warrant.

354 Subsection (4) introduces the safeguards that apply to 'protected content'. This is any content of persons within the British Islands, mirroring the safeguards provided in the bulk interception regime. So, where a UK person's communications are being targeted for examination, a targeted EI warrant will be required.

355 This distinction ensures that any examination of UK persons data obtained through these techniques is authorised by the Secretary of State and an independent Judicial Commissioner on the grounds of necessity and proportionality.

> Example:
> A member of an intelligence service is targeting a hostile foreign intelligence officer through a bulk EI operation. The foreign intelligence officer is overseas, so the analyst can examine the content that they acquire through the provisions made in the bulk EI warrant. That foreign intelligence officer decides to visit the UK. At this point, a targeted EI examination warrant must be sought in order to examine any content acquired through bulk EI relating to the target.

Clause 148: Application of other restrictions in relation to warrants under this Chapter

356 This clause is self-explanatory.

Clause 149: Chapter 3: interpretation

357 This clause defines various terms relating to bulk equipment interference warrants which are used in this chapter.

Part 7: Bulk Personal Datasets

Clause 150: Bulk personal dataset: interpretation

358 Subsection (1) sets out the circumstances in which, for the purposes of this Bill, an intelligence

service obtains a bulk personal dataset (BPD). An intelligence service is defined in the general definitions clause of the Bill to mean the Security Service (MI5), Secret Intelligence Service (MI6) or GCHQ. As a result, the safeguards set out in later clauses must be followed if these circumstances are met.

359 Subsection (2) sets out the circumstances in which it is considered that an intelligence service retains a BPD. As a result, the safeguards set out in later clauses must be followed if these circumstances are met.

360 Subsection (3) defines personal data. The definition is the same one as in the Data Protection Act 1998 (DPA) except that it also encompasses data relating to deceased persons. This slight widening of the DPA definition is because the bulk personal datasets that an intelligence agency may obtain or acquire might include data relating to deceased persons.

> Example:
> The electoral roll, which would be a bulk personal dataset if it was obtained by an intelligence service and retained in one of its analytical systems, will inevitably include persons who are deceased given it is not updated constantly.

Clause 151: Requirement for authorisation by warrant: general

361 This clause specifies that an intelligence service may not exercise a power to obtain, retain or examine a BPD without a warrant. Subsection (4) describes the two types of warrant provided for under this Part of the Bill – a 'class' or a 'specific' warrant.

Clause 152: Exceptions to Section 151(1) to (3)

362 This clause explains when the general requirements listed in the previous clause do not apply. Subsection (1) states that a BPD warrant is not required as long as the acquisition, retention and examination of the BPD is governed by another regime outlined in this Bill - for example an interception warrant under which a BPD as well as intercept material is acquired.

363 Subsection (2) clarifies that a warrant is not needed when a BPD is being retained for the purpose of enabling an application for a specific BPD warrant relating to that dataset. This allows intelligence agencies who have received unsolicited BPD or a BPD that falls outside an existing class BPD warrant to retain the dataset while going through the process of obtaining the necessary specific BPD warrant.

364 Subsection (3) clarifies that BPD can be retained or examined to enable the information contained in it to be deleted. If a warrant is cancelled or a specific warrant is not approved, it will not always be possible for the intelligence agency to delete it immediately from their systems. This provision allows the agencies to hold the BPD while they are ensuring that the relevant data is entirely removed from their systems and ensure that they are legally compliant.

Clause 153: Class BPD warrants

365 This clause explains how the class BPD warrant authorisation process works.

366 Subsection (2) specifies what an application to get a class warrant must include – a description of the class of BPD and an explanation of the purposes for which the intelligence agency wishes to examine the dataset.

367 Subsection (3) explains that a Secretary of State can issue a class warrant (thus enabling the

obtaining, retention and examination of BPDs of that class) if s/he believes that the warrant is necessary (for the standard reasons of national security etc.) and proportionate, and that satisfactory handling measures (for example, protective security measures) are in place. The Secretary of State must also consider that the examination of the BPDs is necessary for the operational purposes specified in the warrant. In addition, a Judicial Commissioner must have approved the decision to issue a warrant. (A subsequent clause includes further provision relating to approval of warrants by the Judicial Commissioner, including that in deciding this matter the Judicial Commissioner applies judicial review principles.) This is the same process as for the interception and equipment interference powers in the Bill – before a warrant can come into force the Secretary of State must issue it and then a Judicial Commissioner must review the Secretary of State's decision and approve it and only then may the warrant come into force.

368 Subsection (4) requires a class BPD warrant to include a description of the class of BPD to which the warrant relates and the operational purposes for which the dataset may be examined.

369 Subsections (5) and (6) explains that BPD cannot be examined for an operational purpose not specified in the warrant and that an application can only be made on behalf of the head of an intelligence service by a person holding office under the Crown.

Clause 154: Specific BPD warrants

370 As well as class warrants, in certain circumstances the Bill states that an intelligence service may seek a specific warrant (i.e. one for a specific dataset rather than a 'class' of them). The cases in which it would be appropriate to seek a specific warrant are set out in subsections (2) and (3).

371 Subsection (2) describes the first scenario for this type of warrant being used. This is where the dataset does not fall within a class described by an existing BPD warrant. An example of this could be when a new or novel type of dataset is obtained.

372 Subsection (3) describes the second scenario for this type of warrant being used. This is when a dataset falls within a class warrant, but, for any reason, the intelligence service believes that it would be appropriate to seek a specific warrant. An example of this could be when an intelligence agency receives a dataset that, while already covered by a class warrant, could raise international relations concerns such that the intelligence agency believes that the Secretary of State should decide whether to authorise the obtaining and use of that specific dataset.

373 The terms of what the application must include is set out in subsection (4) – a description of the specific dataset and an explanation of the operational purposes for which the dataset is to be examined.

374 Subsection (5) describes the circumstances in which a specific BPD warrant can be issued by the Secretary of State. They are the same ones as for a class BPD warrant: the Secretary of State can issue a specific warrant if s/he believes that it is necessary for specified purposes and proportionate, and that adequate handling arrangements (for example through appropriate protective security measures) are in place. And the Secretary of State must also consider that the examination of the BPDs is necessary for the operational purposes specified in the warrant. In addition, a Judicial Commissioner must have approved the decision to issue a warrant. (A subsequent clause includes further provision relating to approval of warrants by the Judicial Commissioner, including that in deciding this matter the Judicial Commissioner applies judicial review principles.)

375 Subsection (6) makes provision to ensure a warrant can authorise the use of a particular BPD

and replacements to that BPD – for example if the BPD was updated on a regular basis.

376 Subsection (7) indicates that a specific BPD warrant must also contain a description of the particular BPD to which the warrant relates; a description allowing the identification of replacement datasets (see subsection (6)); and the operational purposes for which the dataset may be examined.

377 Subsections (8) and (9) explains that the specific BPD cannot be examined for an operational purpose not specified in the warrant and that an application can only be made on behalf of the head of an intelligence service by a person holding office under the Crown.

Clause 155: Approval of warrants by Judicial Commissioners

378 This clause explains the process by which the Judicial Commissioner will consider whether to approve the Secretary of State's decision to issue the warrant. It is consistent with role of Judicial Commissioners in authorisation in the rest of the Bill (e.g. in authorising interception warrants).

Clause 156: Approval of warrants issued in urgent cases

379 This clause applies for specific BPD warrants only, where, if the Secretary of State believed that there was an urgent need to issue it, a specific BPD warrant may be made without the approval of the Judicial Commissioner. It states that if this happens, the Commissioner must be informed that an urgent warrant has been issued and, within five working days, decide whether to approve the issue of that warrant and notify the Secretary of State of their decision. This is the same approach as for urgent targeted interception warrants. Subsection (4) explains that this is not required if the Judicial Commissioner is notified within that time that the warrant will be renewed through the normal renewal process outlined in a later clause. Subsection (5) explains that if the Commissioner refuses to approve the decision to issue the warrant, it ceases to have effect.

Clause 157: Warrants ceasing to have effect under section 156

380 This clause explains the process if a specific warrant that was issued under the urgency procedure above ceases to have effect. Subsection (2) states that anything being done under that warrant should stop as soon as possible. Subsection (3) explains that if a Judicial Commissioner refused to approve the warrant, he/she may determine what to do with the material that was obtained under that warrant. They may direct that the material is destroyed or impose conditions as to the retention or examination of any of the material. Subsections (4) and (5) explain that the Commissioner can require representations from either the intelligence service or the Secretary of State, and must have regard to any representations received by these parties, before deciding what to do with the material. Subsections (6) and (7) explain that an appeal can be made to the Investigatory Powers Commissioner. Subsection (8) ensures that actions taken in reliance on a warrant before it ceases to have effect or at the point it ceases to have effect (and which cannot reasonably be stopped) remain lawful.

Clause 158: Decisions to issue warrants to be taken personally by Secretary of State

381 This section specifies that the decision to issue a class or specific BPD warrant must be taken personally by the Secretary of State. A warrant must also be signed by the Secretary of State, unless it is an urgent case as outlined in an earlier clause, when a senior official can sign the warrant, with a statement included that the Secretary of State has personally expressly authorised the issue of the warrant.

Clause 159: Requirements that must be met by warrants

382 This clause explains that a BPD warrant application must state that it is a 'class' or 'specific' BPD warrant and must be addressed to the intelligence service concerned.

Clause 160: Duration of warrants

383 This clause explains that, for non-urgent warrants, the warrant comes into effect at the point at which it is issued or, in the case of a renewed warrant, the day following the day on which it would otherwise have ceased to have effect. In either case, it lasts for six months. An urgent warrant lasts for five working days after the day on which it was issued. These durations are consistent with other forms of warrants in the Bill.

Clause 161: Renewal of warrants

384 Subsections (1) to (3) set out that a Secretary of State may renew a 'class' or 'specific' BPD warrant if s/he continues to believe it is necessary and proportionate, and if s/he considers that the examination of the BPDs continues to be necessary for the operational purposes specified in the warrant, and provided that the Secretary of State's renewal decision is approved by a Judicial Commissioner. This is consistent with other forms of warrant in the Bill.

Clause 162: Modification of warrants

385 This clause explains the process by which BPD warrants can be modified, what constitutes a major or minor modification to a BPD warrant and who would be authorised to make or approve those modifications.

Clause 163: Cancellation of warrants

386 This clause sets out that a Secretary of State or senior official designated by the Secretary of State can cancel a BPD warrant at any time.

Clause 164: Non-Renewal or cancellation of class BPD warrants

387 This clause sets out the process if a class BPD warrant is not renewed or is cancelled and in particular what to do with the material that was obtained under that class BPD warrant. Subsection (2) specifies that the intelligence service may apply to the Secretary of State for directions as to what should be done with this material. Subsection (3) specifies that the Secretary of State can direct that any of the material should be destroyed or, with the approval of the Judicial Commissioner, can authorise the retention or examination of any of the material. This may be the case if, for example, the Secretary of State no longer believes that an entire class of BPD should be retained, but that it is necessary and proportionate to retain a subset or subsets of that material. If the Judicial Commissioner does not approve a decision to authorise the continued retention or examination of any of the material, he or she must give the Secretary of State written reasons for this (subsection (4)). Subsection (5) provides that if a Judicial Commissioner other than the Investigatory Powers Commissioner does not approve such a decision, the Secretary of State can ask the Investigatory Powers Commissioner to decide whether to approve the decision.

Clause 165: Duty to have regards to code of practice

388 This clause requires the intelligence services to have regard to any Code of Practice issued under this Bill that is applicable to BPDs. The Government intends to issue such a Code of Practice.

Clause 166: Interpretation of Part

389 This clause defines specific terms used in this Part.

Part 8: Oversight Arrangement

Chapter 1: Judicial Commissioners

Clause 167: Investigatory Powers Commissioner and other Judicial Commissioners [j760]

390 This clause establishes the office of the Investigatory Powers Commissioner, who will be supported in fulfilling their functions by other Judicial Commissioners. No-one will be appointed as the Investigatory Powers Commissioner or as a Judicial Commissioner unless they have held a judicial position at least as senior as a high court judge. To allow them to work effectively, the Investigatory Powers Commissioner will be able to delegate functions to the other Judicial Commissioners. The Investigatory Powers Commissioner is a Judicial Commissioner, so where the Bill or these Explanatory Notes refers to a Judicial Commissioner this includes the Investigatory Powers Commissioner.

Clause 168: Terms and conditions of employment

391 The Judicial Commissioners will be appointed for fixed terms of three years and can be re-appointed. Subsections (2)-(5) ensure the independence of the Judicial Commissioners by limiting the circumstances in which they can be removed from office. The Investigatory Powers Commissioner can only be removed from office with the say so of both Houses of Parliament, unless some very limited circumstances apply, including the Commissioner being given a prison sentence or disqualified from being a company director. Other Judicial Commissioners can be removed from office in the same way, but they can also be removed from office by the Investigatory Powers Commissioner (subsection (6)).

Clause 169: Main oversight functions

392 This clause gives the Investigatory Powers Commissioner a very broad remit to keep under review the use of investigatory powers. The Investigatory Powers Commissioner must do so through audits, inspections and investigations. In particular the Investigatory Powers Commissioner will undertake, with the assistance of their office, the functions currently undertaken by the Intelligence Services Commissioner, the Interception of Communications Commissioner and the Surveillance Commissioner.

393 However, subsection (4) explains that, to prevent inefficiency and duplication of oversight, the Investigatory Powers Commissioner will not oversee particular areas that are already subject to oversight by other individuals or bodies. The Investigatory Powers Commissioner will not oversee decisions by other judicial authorities or where information is obtained through a search warrant or production order issued by a judicial authority. The Investigatory Powers Commissioner will not oversee matters which are overseen by the Information Commissioner.

394 Subsection (5) and (6) seek to ensure that the oversight activities do not have a negative effect upon the ability of law enforcement agencies and security and intelligence agencies to perform their statutory functions. These subsections do not apply to the judicial functions of the Commissioners – such as deciding whether to approve the issuing, renewing or modification of a warrant.

Clause 170: Additional directed oversight functions

395 As the policies, capabilities and practices of the security and intelligence agencies change with time, subsections (1)-(3) allow the Prime Minister to direct the Investigatory Powers Commissioner to oversee new areas. This is important to ensure that independent oversight keeps pace with developments within the security and intelligence agencies.

396 Subsection (5) sets out that the Prime Minister must publish any direction that he makes to the Investigatory Powers Commissioner to ensure that there is full transparency about their role. However, this will need to be balanced against a situation where saying too much about what is being overseen will give away details of the policy or capability to the extent that it damages

national security.

Clause 171: Error reporting

397 This clause provides for a process through which people can be informed of serious errors in the use of investigatory powers. An error means any error made by a public authority in complying with any requirement which the Investigatory Powers Commissioner has oversight of.

398 When the Investigatory Powers Commissioner becomes aware of an error, the Commissioner must decide whether the error is serious. An error can only be considered serious if it has caused significant prejudice to the person concerned. If the Commissioner thinks that the error is serious the IPT must be informed. If the IPT agrees that the error is serious, the IPT must then decide whether it is in the public interest for the person concerned to be informed. In doing so the IPT must balance on one hand the seriousness of the error and the impact on the person concerned, and on the other hand the extent to which disclosing the error would be contrary to the public interest or would be prejudicial to national security, the prevention and detection of serious crime, the economic well-being of the UK, or the ability of the intelligence agencies to carry out their functions.

399 If the IPT decides that the person should be informed, that person must also be informed of their right to bring a claim in the IPT. The person must also be provided with the details necessary to bring such a claim, to the extent that disclosing information is in the public interest.

400 The Investigatory Commissioner's annual report (see clause 172(1)) must include details regarding errors, including the number of errors the Commissioner becomes aware of, the number referred to the IPT and the number of times a person has been informed of an error.

Clause 172: Additional functions under this Part

401 This clause sets out that a Judicial Commissioners must give the IPT any assistance the IPT may ask for, including Commissioner's opinion on anything the IPT has to decide. This allows the IPT to take advantage of the Investigatory Powers Commissioner's expertise and the expertise of his office when reaching a decision or carrying out an investigation.

402 Subsection (2) allows the Investigatory Powers Commissioner to provide advice and information to both public authorities and the general public. If the Commissioner thinks that providing such information or advice might be contrary to the public interest or be damaging to one of the things listed, including national security, the Commissioner must consult with the Secretary of State first.

Clause 173: Functions under other enactments

403 This clause means that authorisations that are currently approved by the Surveillance Commissioner will instead be approved by the Investigatory Powers Commissioner.

Clause 174: Annual and other reports

404 Subsection (1) means that the Investigatory Powers Commissioner must report to the Prime Minister on an annual basis about their work and subsection (2) lists matters which must be included in the report. The Prime Minister may require additional reports. The Investigatory Powers Commissioner may report at any time on any matter the Commissioner has oversight of. The Investigatory Powers Commissioner's reports can include any recommendations the Commissioner thinks are appropriate.

405 Subsections (3) & (4) state that upon receipt of an annual report from the Investigatory Powers Commissioner the Prime Minister must publish that report and lay it before Parliament.

However, the Prime Minister may redact information from the report if that information would damage national security or damage operational effectiveness. The Prime Minister must consult with the Investigatory Powers Commissioner before deciding to redact anything from the report.

406 Reports that are laid before Parliament must be sent to the Scottish Ministers and the First Minister and deputy First Minister to be laid before the Scottish Parliament and the Northern Irish Assembly.

Clause 175: Information and inspection powers

407 This clause ensures that the Investigatory Powers Commissioner has access to the information necessary to carry out the Commissioner's oversight role effectively. The clause does this by requiring people to provide the Investigatory Powers Commissioner with all the information and documents that the Commissioner may need. They must also provide the Commissioner with any assistance the Commissioner may need when carrying out an inspection. The persons to whom these obligations apply includes public authorities and also telecommunications and postal operators who are subject to obligations under this Act.

Clause 176: Funding, staff and facilities

408 Subsection (1) explains that the Judicial Commissioners will be paid a salary and may be paid expenses. The amount will be decided by the Treasury.

409 Subsection (2) requires the Secretary of State to provide the Investigatory Powers Commissioner with the staff, accommodation, equipment and facilities that the Secretary of State thinks necessary. It is intended that the resources afforded to the Investigatory Powers Commissioner will ensure that the office is fully staffed with judicial, official, legal and technical support to ensure that the Commissioners are fully able to perform their oversight and authorisation functions and to hold those that use investigatory powers to account. In determining the resources that should be provided the Secretary of State will consult with the Investigatory Powers Commissioner. Treasury approval will be required as to the number of staff. Should the Investigatory Powers Commissioner believe that the resources afforded to them are insufficient then they may publicly report the fact in their Annual Report.

Clause 177: Power to modify functions

410 This clause allows the functions of the Investigatory Powers Commissioner to be changed. This would require the approval of both Houses of Parliament. The ability to change the function allows a level of flexibility about the role of the Commissioner to ensure that it can be modified and adapted to fit with the work that needs to be overseen.

Clause 178: Abolition of existing oversight bodies

411 This clause confirms that the Investigatory Powers Commissioner will replace the existing commissioners who provide oversight of investigatory powers: the Interception of Communications Commissioner, the Surveillance Commissioner (including Assistant Surveillance Commissioners), the Intelligence Services Commisisoner and the Investigatory Powers Commissioner for Northern Ireland. The abolition of the Surveillance Commissioner and Assistant Surveillance Commissioner includes those appointed by Scottish Ministers for the purposes of the Regulation of Investigatory Powers (Scotland) Act 2000.

Chapter 2: Other arrangements

Clause 179: Codes of practice

412 This clause provides for the Secretary of State to issue Codes of Practice covering the use of powers covered by the Bill, as outlined in Schedule 6.

Clause 180: Right of appeal from the Tribunal

413 Currently there is no domestic route of appeal from decisions of the Investigatory Powers Tribunal, with Claimant's having to issue appeals to the European Court of Human Rights if they wish to challenge a decision. This clause introduces a domestic appeal route from decisions of the IPT on a point of law, to the Court of Appeal (for England and Wales) or its equivalent in Scotland or Northern Ireland (to be detailed in Regulations).

414 Where there is a point of law, the decision on whether to grant permission to appeal will be taken by the Investigatory Powers Tribunal in the first instance. If the Tribunal refuses to grant permission to appeal then this decision may be reviewed by the appeal court.

415 The Tribunal must only give permission to appeal on a point of law where the appeal would raise an important point of principle or practice or they consider that there are other compelling reasons to grant permission to appeal.

Clause 181: Functions of Tribunal in relation to Part 4

416 This clause extends the functions of the Investigatory Powers Tribunal in relation to retention notices under Part 4.

Clause 182: Oversight by Information Commissioner in relation to Part 4

417 The Information Commissioner must audit requirements related to the retention of communications data, for example, to ensure the data is retained securely. This is distinct from the Investigatory Powers Commissioner's requirements in respect of the acquisition of communications data.

Clause 183: Technical Advisory Board

418 This Clause provides for the continued existence by order of a Technical Advisory Board. Its make-up will be prescribed by Secretary of State regulations and must include a balanced representation of the interests of communications service providers and of those people listed in subsection (2b).

Part 9: Miscellaneous

Clause 184: Combination of warrants and authorisations

419 This clause explains that Schedule 7 (which is explained further below) allows for the combination of targeted interception and equipment interference warrants with other warrants or authorisations. This builds on the existing ability to combine certain warrants and authorisations (RIPA allows authorisations that combine Property interference (under the Intelligence Services Act 1994) and Intrusive Surveillance).

Clause 185: Payments towards certain compliance costs

420 This clause requires the Secretary of State to ensure that there are arrangements to secure that communications service providers receive a fair contribution towards their costs of complying with the provisions in the Act. Subsection (6) makes clear that the appropriate contribution must never be nil. Subsection (7) requires that a retention notice under Part 4 or national security notice under clause 188 must specify the level of contribution to be made.

Clause 186: Power to develop compliance systems etc

421 This clause enables the Secretary of State to develop, provide, maintain or improve equipment that can be used by the Secretary of State, another public authority or any other person to facilitate compliance with the provisions in the Act. The clauses also enables the Secretary of State to enter into financial arrangements with any other person to develop, provide, maintain

or improve any such system.

Clause 187: Amendments of the Intelligence Services Act 1994

422 Subsection (1) describes the act to be amended - the Intelligence Services Act 1994.

423 Subsection (2)(a) adds in to subsection (1)(a) of the existing clause 3 of ISA, that GCHQ can "make use of" as well as "monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material". This clarifies that GCHQ may, in the performance of its functions, make use of communications services in the manner in which it was intended they would be used. This could be used for public communications as well as for investigative purposes.

424 Subsection (2)(b) amends ISA to allow GCHQ to provide advice and assistance on the protection of information to other organisations and members of the public as appropriate. This will enable GCHQ to provide information assurance advice to a wide audience on issues which impact not just HMG but also business and the public in general e.g. cyber security.

425 Subsection (3) amends ISA to remove the restriction on GCHQ and SIS to take action in support of the prevention and detection of serious crime in the UK, as well as overseas. Currently ISA only permits such activity where it is in support of MI5. The security and intelligence agencies have a remit to support law enforcement to help prevent and detect serious crime.

Clause 188: National security notices

426 This clause provides for the Secretary of State to issue a national security notice to any telecommunications operator requiring the operator to take steps as appear to the Secretary of State to be necessary in the interests of national security.

427 Subsection (2) specifies that a national security notice may only be given by the Secretary of State where it is necessary and proportionate to do so.

428 Subsection (3) outlines the types of support that the telecommunications operator may be required to provide to satisfy the requirement, for example to provide services or facilities which would assist the intelligence agencies in safeguarding the security of their personnel and operations.

429 Subsection (4) stipulates that the notice cannot be used where the primary purpose is to authorise interference with privacy. In any circumstance where a notice would involve the acquisition of communications or data a warrant or authorisation from the relevant part of this Act would always be required in parallel.

Clause 189: Maintenance of technical capability

430 This clause allows for the making of regulations by the Secretary of State to impose obligations upon telecommunications operators, which would be required to effect warrants or acquisition notices on a recurrent basis

431 Subsection (1) provides the mechanism by which the Secretary of State may impose obligations upon persons providing or planning to provide public postal services or public telecommunications services. The Secretary of State will do this through regulations which specify the obligations on those service providers listed in subsection (2). These regulations will enable the Secretary of State to impose obligations on particular providers by the service of individual notices describing in much greater detail the precise steps they are required to take.

432 Subsection (3) sets out the cases in which regulations may specify an obligation in relation to

warrants issued under Part 2, 5 or 6, or authorisations or notices given under Part 3. The Secretary of State may specify an obligation only where the Secretary of State believes the obligations are reasonable, and with the aim of ensuring that providers are capable of providing the technical assistance

433 Subsection (4) sets out the types of obligations that may be imposed for example in (a) providing communications facilities and capacity to support the implementation of warrants or (d) ensuring the security of facilities or staff who may be required to handle classified material.

434 Subsection (5) requires the Secretary of State to consult with a number of people prior to making the regulations. These include the Technical Advisory Board, the persons likely to have obligations imposed on them and their representatives, and persons with statutory functions affecting providers of communication services.

435 Subsection (6) explains that the technical capability notice will set out specific steps that the providers will be required to provide in order to comply with the obligations and subsection (7) makes clear that the steps must be necessary to ensure the subject of the notice has the practical capability to provide assistance as required.

436 Subsection (8) confirms that a technical capability notice can be given to persons outside the United Kingdom. These may relate to conduct outside of the United Kingdom.

Clause 190: Further provision about notices under section 188 or 189

437 This clause provides further details about notices under the previous two sections. Subsection (3) sets out the considerations the Secretary of State must take into account prior to serving either a national security notice or technical capability notice. Consideration of the time required to comply with the notice is covered in subsection (4).

438 Subsection (5) set out the mechanisms by which a notice may be given to a person outside the United Kingdom.

439 Subsection (9) requires persons served with a notice under sections 178 or 179 to comply with it.

440 Subsections (10-11) outlines that the Secretary of State may bring civil proceedings to enforce both a national security and technical capability notice on persons within the UK. For persons outside of the UK, the Secretary of State may only bring civil proceedings to enforce a technical capability notice which relates to only interception warrants or an authorisation or notice given under Part 3.

Clause 191: Review by the Secretary of State

441 This clause permits the recipient of a notice to refer the notice back to the Secretary of State where the recipient of the notice considers an obligation unreasonable. Subsection (1) states that the provider will have the opportunity to refer a notice either within a specified time period or specified circumstances which will be set out in the regulations.

442 Subsection (4) states that the person is not required to comply with the specific obligations under referral until the notice has been reviewed by the Secretary of State. The actions that the Secretary of State must take in reviewing the notice and the role of the Technical Advisory Board and the Investigatory Powers Commissioner are outlined at subsections (5-8).

443 Subsection (9) requires the Commissioner and the Technical Advisory Board to consult the person and the Secretary of State, and report their conclusions to the person and Secretary of State. After consideration of the conclusions of the Commissioner and Board, the Secretary of State may decide to confirm the effect of the notice, vary the notice or withdraw it.

Clause 192: Amendments of the Wireless Telegraphy Act 2006

444 This clause makes clear that the Wireless Telegraphy Act 2006 no longer provides authority for the use of wireless telegraphy to intercept information as to the contents, sender or addressee of a message. Instead, this Bill provides for such interception.

Chapter 2: General

Clause 193: Telecommunications definitions

445 This clause provides relevant definitions in relation to telecommunication systems, services and operators. These new categories are intended to be technology neutral and replace the three categories of communications data in RIPA: traffic data, service-use data and subscriber data which no longer adequately reflect the data available from telecommunication operators or systems.

446 Subsection (2) defines a telecommunication. It includes communications between persons, between a person and a machine and between machines.

447 Subsection (3) defines entity data as data about entities or links between them but does not include information about individual events. Entities could be individuals, groups and objects.

448 Subsection (4) defines events data as data which identifies or describes events taking place on a telecommunication system or other device which consist of one or more entity engaging in an activity at a specific point, or points, in time and space.

449 Subsection (5) defines the subset of entity data and events data which constitute communications data. The authorisation levels provided for in Schedule 4 reflect the fact that the set of events data as a whole contains the more intrusive communications data.

> Example 1: Entity Data:
> Phone numbers or other identifiers linked to communications devices; address provided to a communications service provider; IP address allocated to an individual by an internet access provider.
>
> Example 2: Events Data:
> The fact that someone has sent or received an email, phone call, text or social media message; the location of a person when they made a mobile phone call or the Wi-Fi hotspot that their phone connected to; the destination IP address that an individual has connected to online.

450 Subsection (6) provides a definition of content based around the meaning of the communication excluding any meaning that can be inferred from the fact of the communication. While it is possible to draw an inference from the fact a person has contacted another person this is distinct from the content of the call.

451 Subsection (6)(a) provides that in the particular context of web browsing anything beyond data which identifies the telecommunication service (e.g. bbc.co.uk) is content. Accordingly bbc.co.uk, google.co.uk or facebook.com would be communications data but data showing what searches have been made on Google or whose profiles have been viewed on Facebook would be content.

452 Subsections (8-14) define communication service providers and systems for the purpose of the bill.

Clause 194: Postal definitions

453 This provision defines the scope of communications data in the postal context. Subsection (3)(a), (b) and (c) are traffic data, service use data and subscriber data respectively. These definitions will continue to remain relevant in a postal context.

Clause 195: General definitions

454 This provision is self-explanatory.

Clause 196: Offences by bodies corporate

455 This provision applies if a body corporate or Scottish partnership, or a senior officer within a body corporate or Scottish partnership commits an offence under this Act.

Clause 197: Regulations

456 This clause outlines the procedure under which the Secretary of State may make regulations. It sets out that regulations made under certain specified sections of the Bill must be laid before Parliament and approved by a resolution of both Houses.

Clause 198: Enhanced affirmative procedure

457 This clause outlines the 'enhanced affirmative procedure'. This is a procedure for making secondary legislation that allows for further scrutiny than the affirmative procedure, outlined in the proceeding clause. It applies to clause 55, which deals with modifying Schedule 4. In particular this means that there will be an enhanced scrutiny process should the Government wish to provide for additional authorities to be able to acquire communications data. The enhanced scrutiny process includes a statutory duty to consult and for a relevant parliamentary committee to comment on the draft legislation. The Secretary of State must have regard to these representations.

Clause 199: Financial provisions

458 This provision is self-explanatory.

Clause 200: Transitional, transitory or saving provision

459 This clause states that Schedule 7 applies and gives power for the Secretary of State to make any transitional, transitory or saving provisions as he or she considers appropriate in connection with the coming into force of the provisions in the Bill. This standard power enables the changes made the Bill to be implemented in an orderly manner.

Clause 201: Minor and consequential provision

460 This clause states that Schedule 6 applies and that the Secretary of State may make any provision by regulation as is considered necessary as a consequence of the provisions of the Bill.

Clause 202: Commencement, extent and short title

461 This clause is self-explanatory.

Schedules

Schedule 1: Monetary Penalty Notices

Part 1: Monetary Penalty Notices

462 Schedule 1 provides for the of paying of monetary fines to the Investigatory Powers Commissioner for the penalty of carrying out interception without authority, without a

warrant or carrying out interception which is not in accordance with a warrant, as specified in clause 6. This provision was originally inserted into the Regulation of Investigatory Powers Act 2000 in 2011 (SI 2011/1340). This followed a letter in April 2009 in which the European Commission set out that the UK had not properly transposed Article 5 (1) of the E-Privacy Directive and Articles 2(h), 24 and 28 of the Data Protection Directive.

463 Paragraph 1 requires any fine imposed by the Commissioner to be paid within the period specified in the penalty notice which begins the day after the penalty notice is imposed and cannot be less than 28 days. Any fine must be paid into the Consolidated Fund.

464 Paragraph 2 subsections (a) to (h) set out the information which a monetary penalty notice issued by the Commissioner must contain.

465 Paragraph 3 provides for an enforcement obligation to be included in the monetary penalty notice if the Commissioner believes the interception is continuing. Subsection (2) sets out that the enforcement obligation requires the person on whom the notice is served to either cease interception on a specified day, or to either - take such steps or refrain from taking specified steps as appropriate, within a specified period, which results in the cessation of the interception. Subsection (3) specifies that an enforcement obligation may not be acted upon for a period of 7 days which begins on the day after the monetary penalty notice is served.

466 Paragraphs 4-6 set out the requirement to consult before a monetary penalty notice may be served. Paragraph 4 specifies that before serving a monetary penalty notice on a person, the Commissioner must serve a notice of intent alerting a person to the fact that the Commissioner intends to serve a monetary penalty notice. Subsection (4) (a)-(g) specifies the information which a notice of intent must contain. The notice of intent must inform the person of their right to make written submissions to the Commissioner or request an oral hearing within a specified period. The specified period cannot be less than 21 days which begins on the day after the notice is served.

467 Paragraph 4(6) requires the Commissioner to arrange an oral hearing if the person on whom the notice is served makes this request during the specified period. At the hearing, the person may make representations to explain interception activity which the Commissioner considers was not acting in accordance with a warrant but which the warrant may explain. They may also make representations to on other matters which they may be unable to disclose on appeal by virtue of the criteria in Clause 43. If the Commissioner subsequently decides not to serve a monetary penalty notice they must inform the person of that fact.

468 Paragraph 5 sets out procedure for variation or cancellation of a notice of intent. It specifies that a Commissioner may not vary a notice of intent except to extend the specified period during which the person on whom the notice is served may provide written submission or request an oral hearing. This does not preclude the Commissioner from serving a new notice of intent.

469 Paragraph 6 specifies that the Commissioner must not service a monetary penalty notice on person if the notice of intent was served on that person more than three months earlier unless the Commissioner considers it reasonable to do so and sets out the reasons in the monetary penalty notice.

470 Paragraph 7 sets out procedure for variation or cancellation of a monetary penalty notice. The Commissioner may not vary the notice in any way which disadvantages the person on who it is served. If the monetary penalty is reduced or cancelled, any money already paid by the person must be repaid. Where the Commissioner has cancelled a monetary penalty notice, he or she cannot issue another notice on the person for the same interception activity.

471 Paragraph 8 provides for a person to appeal to the First-tier Tribunal in respect of a monetary penalty notice or any refusal to vary or cancel it. Subparagraph (2) specifies that a person appealing against a monetary penalty notice does not have to comply with its provisions, with the exception of any enforcement obligations, until the appeal is determined. The First Tier Tribunal must allow the appeal if it considers the monetary penalty notice under appeal is not lawful or where it considers the Commissioner has exercised discretion and ought to have done so differently. Where the appeal is against a refusal to vary or cancel the notice, subparagraphs (8)-(10) provide that the Tribunal may direct the Commissioner to make the variation or cancellation if it considers the Commissioner ought to have done so.

472 Paragraph 9 specifies where a monetary penalty notice is recoverable in England, Wales and Scotland.

473 Paragraph 10 specifies that any enforcement obligation contained in the monetary penalty notice is enforceable by legal proceedings.

474 Paragraph 11 requires the Commissioner to produce guidance on the functions provided for under Clause 6 and Schedule 1 and specifies that the guidance must set out the circumstances under which the Commissioner would consider issuing a monetary penalty notice, determining the amount payable and setting out in what circumstances it would be appropriate to impose an enforcement obligation.

Part 2: Information Provisions

475 Paragraphs 13 and 14 provide for the Commissioner to issue an information notice in order to determine whether a notice of intent or monetary penalty notice should be issued. Subsections (3) and (4) set out the information which must be contained in an information notice and specifies that the period within which the information is provided cannot be less than 28 days beginning on the day after the notice is served. The Commissioner may vary an information notice to extend the time within which the information is to be provided if the person on whom the notice is serves appeals.

476 Paragraph 15 provides for a person to appeal to the First-tier Tribunal in respect of an information notice or any refusal to vary or cancel it. Subject to the Commissioner extending the time period, any appeal does not affect the need to comply with the information notice until the outcome of the appeal is determined. The First Tier Tribunal must allow the appeal if it considers the information notice under appeal is not lawful or where it considers the Commissioner has exercised discretion and ought to have done so differently. Where the appeal is against a refusal to vary or cancel the information notice, the Tribunal may direct the Commissioner to make the variation or cancellation if it considers the Commissioner ought to have done so.

477 Paragraph 16 provides for the Commissioner to serve a monetary penalty notice on a person who refuses to comply or knowingly provides false material in response to an information notice. Subparagraphs (2)-(5) set out the types of monetary penalty that the Commissioner may require which must not exceed £10,000. If the Commissioner imposes a monetary penalty by reference to a daily rate it may not start until after the day on which the notice is served and must specify the period in which the amount starts to accrue, when it ceases to accumulate and the period within which it must be repaid, which cannot be less than 28 days from the day the amount starts to accumulate.

478 Paragraph 17 specifies the modifications applied to a monetary penalty notice issued under Part 2 of the Schedule from a notice issued under Part 1. The provisions relating to enforcement obligations do not apply to a Part 2 notice. The effect of paragraph 4 is modified to specify that representations made at an appeal hearing of a Part 2 notice, outlined in

subparagraph (4), are only in relation to matters which they may be unable to disclose on appeal by virtue of the criteria in Clause 43. Subparagraph (4) applies the criteria of paragraph 6 which specifies that the Commissioner must not service a monetary penalty notice on person for failure to comply with a notice or for providing false information if the notice of intent was served on that person more than three months earlier unless the Commissioner considers it reasonable to do so and sets out the reasons in the monetary penalty notice. As in paragraph 7(5) the Commissioner may not issue another notice for the conduct outlined in paragraph 16(1)(a) or (b) if a previous notice has already been cancelled.

479 Paragraph 18 requires OFCOM to comply with any reasonable request in connection functions under clause 6 or Schedule 1 and that in doing so the Commissioner may disclose any information obtained under the provisions in the Schedule.

Schedule 2: Abolition of Disclosure Powers

480 Schedule 2 repeals certain powers so far as they enable public authorities to secure the disclosure by a telecommunications operator of communications data without the consent of the operator and ensures the definitions within these Acts have the same meaning as this Act.

481 Paragraph 1 requires an insertion to the end of section 20 of the Health and Safety at Work etc Act 1974 to state that none of the section enables an inspector to secure disclosure of communications data from a telecommunications operator or postal operator without the operator's consent.

482 Paragraph 2 requires an insertion after section 2(10) of the Criminal Justice Act 1987 (investigation powers of Director of Serious Fraud Office) to state that none of the section enables a person to secure disclosure of communications data from a telecommunications operator or postal operator without the operator's consent.

483 Paragraph 3 requires an insertion to the end of section 29 of the Consumer Protection Act 1987 to state that the officer to whom the section relates may not use the power under the section to secure disclosure of communications data from a telecommunications operator or postal operator without the operator's consent.

484 Paragraph 4 requires an insertion to the end of section 71 of the Environmental Protection Act 1990 to state that none of the section enables a person to secure disclosure of communications data from a telecommunications operator or postal operator without the operator's consent.

485 Paragraph 5(a)-(c) repeals section 109B (power to require information), subsection (2A) paragraph (j) and subsection (2F) of the Social Security Administration Act 1992. It amends subsection (2E) of that Act to ensure the section does not enable a person to secure disclosure of communications data from a telecommunications operator or postal operator without the operator's consent. Paragraph 6 applies the same abolition of disclosure powers to section 109C (powers of entry) of the same Act.

486 Paragraph 7 requires an insertion after section 175, subsection (5) of the Financial Services and Markets Act 2000 (information gathering and investigations: supplemental provision) to state that nothing in the Part enables a person to secure disclosure of communications data from a telecommunications operator or postal operator without the operator's consent.

487 Paragraph 8 requires an insertion to the end of paragraph (19) (restrictions on powers: types of information) of Schedule 36 of the Finance Act 2008 (information and inspections powers) to state that an information notice does not require a telecommunications operator or postal operator to provide or produce communications data.

488 Paragraph 9 sets outs the required deletions and substitutions to regulation 4 of the Prevention

of Social Housing Fraud (Power to Require Information) (England) Regulations 2014 (power to require information from persons who provide telecommunications services etc) to repeal the power to compel disclosure by a telecommunications operator of communications data without the consent of the operator.

Schedule 3: Exceptions to Section 42

489 Schedule 2 sets out the exceptions to clause 42, which prohibits the disclosure of interception for the purposes of or in connection with legal proceedings. The schedule sets out the circumstances in which this prohibition would not apply.

490 Paragraph (2) provides that the contents of a communication may be disclosed if the communication is obtained under a statutory power exercised to obtain information, documents or property. This specifically applies to stored communications. It also allows for disclosure of any lawful interception carried out in accordance with clauses 26-33.

491 Paragraph (3) provides that there is no prohibition to doing anything which discloses the person has been convicted of offences under the Acts listed.

492 Paragraphs (4) and (5) specify that clause 42(1) does not apply in relation to proceedings before the Investigatory Powers Tribunal or the Special Immigration Appeal Commission, providing the conditions specified in sub-paragraph (5)(b)(i) or (ii) are met, which prohibits disclosure to a SIAC applicant or representatives.

493 Paragraph (6) specifies that clause 42(1) does not apply in relation to proceedings before the Proscribed Organisations Appeal Commission, providing there is no disclosure to the persons or bodies listed in sub-paragraph (6)(2).

494 Paragraph (7) specifies that clause 42(1) does not apply to certain civil proceedings where provision for disclosure within closed material proceedings is made under section 14(1) of the Justice and Security Act 2013.

495 Paragraphs (8) and (9) specify that clause 42(1) does not apply in any proceedings relating to TPIMs or TEO providing there is no disclosure to any person involved or party to the proceedings other than the Secretary of State.

496 Paragraphs (10)-(12) specifies that clause 42(1) does not apply into proceedings relating to the freezing of terrorist assets providing there is no disclosure to any person who is party to the proceedings other than the Treasury.

497 Paragraph (13) specifies that clause 42(1) does not apply in proceedings relating to the release of prisoners in Northern Ireland providing there is no disclosure to any person who is party to the proceedings or their representatives.

498 Paragraphs (14)-(15) specifies the conditions where clause 42(1) does not apply in relation to employment or industrial tribunal proceedings providing there is no disclosure to any person who is party to the proceedings or their representatives.

499 Paragraph (16) specifies that clause 42(1) does not prevent anything done in connection with legal proceedings relating to dismissal for offences under the Acts listed.

500 Paragraphs (17)-(18) specifies that clause 42(1) does not apply in relation to appeal proceedings relating to claims of discrimination in Northern Ireland, providing there is no disclosure to any person who is party to the proceedings or their representatives.

501 Paragraph (19) specifies that clause 42(1) does not apply in relation to civil enforcement proceedings where a relevant service provider has refused to assist in the implementation of a warrant.

502 Paragraph (20) lists the offences under relevant sections of specific Acts where clause 42(1) does not apply.

503 Paragraph (21) provides that disclosure can be permitted during criminal proceedings to prosecutors and judges in the interests of a fair prosecution. Sub-paragraph (4) makes provisions for judges to direct the prosecution to make relevant admissions if, as a consequence of the disclosure, the judge believes this is essential in the interests of justice as longs as it does not contravene clause 42(1).

Schedule 4: Relevant Public Authorities

504 Column 1 of the table in Part 1 of this Schedule lists all the authorities that are able to acquire communications data. Column 2 provides a minimum rank for designated senior officers. These are the staff within the relevant public authorities that are able to authorise the acquisition of communications data. Columns 3 and 4 provide the types of data that each designated senior officer is able to authorise the acquisition of and the statutory purposes, listed in clause 46(7), for which it can be accessed.

505 Many authorities are only able to acquire communications data for the purpose of preventing or detecting crime or of preventing disorder. Certain purposes only apply to certain authorities. For example, the purpose of exercising functions relating to the regulation of financial services and markets or to financial stability only applies to the Financial Conduct Authority.

506 Some authorities have two designated senior officers at different ranks. This is because 'entity' data is generally less intrusive than 'events' data and can therefore be acquired at a lower authorisation level. For example, in police forces, an Inspector can authorise acquisition of 'entity' and 'reference' data, whereas a Superintendent can authorise acquisition of all types of communications data. Where only one rank of designated senior officer is provided for, that rank is deemed to be senior enough to authorise acquisition of all types of communications data.

Schedule 5: Transfer and Agency Arrangements with Public Authorities: Further Provisions

507 This clauses outlines the provisions that apply should the Home Secretary transfer ownership of the Request Filter to a public authority. Subparagraph (2) requires the Secretary of State to approve the measures to be adopted by a designated public authority for complying with the requirements in clause 67(1). A designated public authority must send the reports required under paragraph (2) to the Secretary of State as well as to the Investigatory Powers Commissioner.

508 Paragraph 3 sets out that the Secretary of State, in connection with regulations made under clause 67(1), may make a scheme for the transfer of property, rights or liabilities (including rights and liabilities relating to contracts of employment). Such transfers may be from the Secretary of State (in practice, the Home Office) to a designated public authority or from one designated public authority to the Secretary of State or to another designated public authority.

509 Sub-paragraph (3) lists consequential, supplementary, incidental and transitional provision that may be made by a transfer scheme. These include making provision the same as or similar to the TUPE regulations (the Transfer of Undertakings (Protections of Employment) Regulations 2006 (S.I. 2006/246). By virtue of sub-paragraph (5), a scheme may make provision for the payment of compensation, example to a designated public authority in circumstances where functions conferred on that body are brought back within the Home Office. Sub-paragraph (6) provides that a transfer scheme may either be included in regulations made

under clause 67(1) but even if not, must be laid before Parliament after being made.

510 Paragraph 4 provides a power for the Treasury to make regulations providing for the tax consequences of a transfer scheme made under paragraph 3. For the purposes of this power the relevant taxes are income tax, corporation tax, capital gains tax, stamp duty and stamp duty reserve tax.

Schedule 6: Codes of Practice

511 Paragraph 1 requires the Secretary of State to issues codes of practice in respect of the exercise of functions under Parts 1-7 of the Bill but not in relation to any functions of any Part conferred on the individuals or bodies listed in subparagraph (a)-(f).

512 Paragraph 2 specifies that a code of practice about the functions in Part 2 of the Bill must cover arrangements for the disclosure and handling of intercepted material to overseas authorities. It must also cover the process for making sharing requests to overseas authorities for intercepted material obtained through a postal or telecommunications system and handling arrangements for any material obtained.

513 Paragraph 3 requires a code of practice to cover communications data held by public authorities acquired under the powers provided by Part 3. Subsection 2 specifies that the code of practice must explain the criteria listed in (a)-(f) covering why the data is held, access to the data, disclosure of the data, interrogation of the data and destruction of the data.

514 Paragraph 4 specifies that a code of practice about obtaining or retaining relevant communications data under the powers provided by Part 3 must also include provisions designed to protect the confidentiality of journalistic sources. It should also outline particular considerations which should be applied to data relating to a member of a profession which would regularly hold legally privileged or relevant confidential information, such as medical professionals, those in the legal profession or MPs. Both legally privileged information and confidential information are defined in subparagraph 2.

515 Paragraph 5 specifies that the Secretary of State must consult on any draft code of practice but may modify a code on the basis of representations made after its publication. The Secretary of State must specifically consult the Investigatory Powers Commissioner on the draft code. A code come into force in accordance with regulations made by the Secretary of State, which must be made by statutory instrument and laid in draft before Parliament and approved by each House. The draft code should be laid alongside the draft instrument. No statutory instrument can be laid until the consultation has taken place.

516 Paragraph 6 makes provision for the Secretary of State to make revisions to a code of practice. The Secretary of State is required to publish and consult on the revised code, and in particular, the Investigatory Powers Commissioner must be consulted. A revised code comes into force in accordance with regulations made by the Secretary of State, which must be made by statutory instrument and laid before Parliament. The revised code should be laid alongside the draft instrument. No statutory instrument can be laid until the consultation on the revised code has taken place.

517 Paragraph 7 requires a person exercising any function to which a code relates to have due regard for the code. Subparagraph (2) clarifies that failure to comply with the code does not make a person liable to criminal or civil proceedings. Subparagraphs (3) and (4) specify however, that the code can be admissible in evidence in any such legal proceedings and a court or tribunal may take a person's failure to comply with the code into account in determining a question in such proceedings.

Schedule 7: Combination of Warrants

518 This schedule allows for warrants authorising different powers to be combined in the same warrant instrument. Those requesting a warrant are under no obligation to apply for a combined warrant and may still apply for individual warrants if that is more operationally efficient. Part 1 explains combinations with targeted interception warrants. Subsections (1)-(3) detail that the Secretary of State may issue a combined warrant on behalf of the Security and Intelligence Agencies. Subsection (4) outlines that the Secretary of State may issue a combined warrant where one of the constituent parts of the combined warrant authorises targeted interception on behalf of the listed Law Enforcement Agencies.

519 Part 2 explains how other combinations of warrants are permitted in terms of combinations with targeted equipment warrants. Subsections (5)-(7) relate to combining an intelligence service equipment interference warrant with various other authorisations / warrants (both within this Bill – a targeted examination warrant; and within RIPA – a directed surveillance or intrusive surveillance authorisation – and the Intelligence Services Act1994 in terms of a property interference warrant under section 5). Subsection (9) provides for law enforcement to combine a targeted equipment interference warrant with a directed or intrusive surveillance authorisation or a police property interference authorisation (under the Police Act 1997).

520 Part 3 provides some general points on how combined warrants should operate. Subsection (9) provides some interpretations.

521 Subsections (10)-(14) confirm that the procedure for issue of these warrants conforms to the issue of its constituent parts. Therefore, regardless of who issues the warrant, where two or more powers are authorised under the same warrant then the authorisation of that warrant will be subject to approval by a Judicial Commissioner. Subsection (11) makes clear that a request for a combined warrant may only be put forward if those applying for the warrant are able to apply for each constituent part of that warrant as an individual warrant. Subsection (12) makes clear that the duration of the combined warrant is determined by the constituent part of the combined warrant which would end first.

522 Combined warrants will still contain all of the information that would be required should the constituent parts of that warrant be applied for individually. Similarly the protections and safeguards that apply to material gathered under a combined warrant will still apply as relevant to the constituent parts of the combined warrant.

Schedule 8: Transitional, Transitory and Saving Provision

523 Schedule 8 explains transitional, transitory and saving provisions for the Bill. Paragraph 1 provides for agreements in force under section 1(4) of RIPA to be considered as international mutual assistance agreements on the day the Act comes in to force, by the virtue of the regulations under section 7 of this Bill.

524 Paragraph 2 specifies how provisions in force under DRIPA 2014 should be transferred under the Bill upon enactment and remain in force.

Schedule 9: Minor and Consequential Provision

525 Schedule 9 makes minor and consequential amendments to other enactments.

Commencement

526 Clauses 193 to 199, 200(2), 201(2) and (3) and 202 and Part 9 of the Bill will commence on Royal Assent. The main provisions of the Bill will be brought into force by means of regulations made by the Secretary of State.

Financial implications of the Bill

527 The provisions enabled by the Bill is estimated to lead to an increase in public expenditure of £247 million over 10 years from 2015/16. These costs are based on:

a. costs to Government Departments associated with the establishment of the Investigatory Powers Commission and authorisation of warrantry;

b. costs associated with the ongoing running costs, compliance and reimbursement to business of costs associated with new communications data provisions;

c. costs associated with increased compliance, reporting and safeguards to the agencies, law enforcement and other public authorities;

d. costs to the justice system for offences and changes to the Investigatory Powers Tribunal.

Compatibility with the European Convention on Human Rights

528 The Government is satisfied that, in the event that the Bill is introduced into Parliament, the responsible Minister could make a statement under section 19(1)(a) of the Human Rights Act 1998 that, in the Minister's view, the provisions of the Bill are compatible with the Convention rights.

529 The Government has published a separate ECHR memorandum which explains its assessment of the compatibility of the Bill's provisions with the Convention rights; the memorandum is available on the Home Office website.

ISBN 978-1-4741-2565-9