EXPLANATORY NOTES

Investigatory Powers Act 2016

Chapter 25

£19.00

INVESTIGATORY POWERS ACT 2016

EXPLANATORY NOTES

What these notes do

These Explanatory Notes relate to the Investigatory Powers Act 2016 (c. 25) which received Royal Assent on 29 November 2016.

- These Explanatory Notes have been prepared by the Home Office in order to assist the reader in understanding the Act. They do not form part of the Act and have not been endorsed by Parliament.
- These Explanatory Notes explain what each part of the Act will mean in practice; provide background information on the development of policy; and provide additional information on how the Act will affect existing legislation in this area.
- These Explanatory Notes might best be read alongside the Act. They are not, and are not intended to be, a comprehensive description of the Act. So where a provision of the Act does not seem to require any explanation or comment, the Notes simply say in relation to it that the provision is self-explanatory.

Table of Contents

Overview of the Act

1 The Investigatory Powers Act 2016 provides an updated framework for the use (by the security and intelligence agencies, law enforcement and other public authorities) of investigatory powers to obtain communications and communications data. These powers cover the interception of communications, the retention and acquisition of communications data, and equipment interference for obtaining communications and other data. It is not lawful to exercise such powers other than as provided for by the Act. The Act also makes provision relating to the security and intelligence agencies' retention and examination of bulk personal datasets.

2 The Act governs the powers available to the state to obtain communications and communications data. It provides consistent statutory safeguards and clarifies which powers different public authorities can use and for what purposes. It sets out the statutory tests that must be met before a power may be used and the authorisation regime for each investigative tool, including a new requirement for Judicial Commissioners to approve the issuing of warrants for the most sensitive and intrusive powers. The Act also creates a new IPC to oversee the use of these powers. Finally, the Act provides a new power for the Secretary of State to require, by notice, communications services providers to retain internet connection records.

Policy background

3 The Government introduced legislation to replace the emergency legislation passed in July 2014, the Data Retention and Investigatory Powers Act 2014 (DRIPA), which was subject to a sunset clause providing for DRIPA to be repealed on 31 December 2016. DRIPA replaced the Data Retention (EC Directive) Regulations 2009 (S.I. 2009/859), following the European Court of Justice judgment of April 2014 in the Digital Rights Ireland case, which declared the Data Retention Directive invalid. During the passage of DRIPA, the Government committed to bring forward new legislation which would provide the security and intelligence agencies, law enforcement and other public authorities with the investigatory powers necessary to address evolving threats within a changing communications environment. The Act updates the legal framework governing the state's ability to acquire communications and data about communications.

4 The Act also consolidates and updates powers available to the state to obtain communications and communications data which were previously provided for in a number of different statutes (see 'Legal background', below), many of which were enacted before the internet became a widely-used means of communication.

5 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. David Anderson published his review in June 2015. This Act responds to the recommendations made in that review and those of the reviews undertaken by the ISC and the Panel of the Independent Surveillance Review convened by the Royal United Services Institute. All three reviews agreed that investigatory powers remain essential in tackling the current and evolving threats to the United Kingdom.

6 A draft Bill was published on 4 November 2015 to facilitate pre-legislative scrutiny by a Joint Committee of Parliament. The Committee took evidence from a broad selection of witnesses including the Government, parliamentarians, law enforcement, oversight commissioners, lawyers, journalists, academics, civil society groups, communications service providers and charities and victims' groups. It also published 148 submissions (over 1500 pages) of written

evidence. The Committee's report, including its recommendations, was published on 11 February 2016.

7 In addition to the Joint Committee, a number of other Committees were involved in scrutinising the draft Bill. The ISC published a report on 9 February 2016, building on the Committee's 2015 Privacy and Security report. The House of Commons Science and Technology Committee also conducted an inquiry into the Bill. The Science and Technology Committee focused on the obligations that will be placed on communications service providers and the feasibility and costs associated with implementing the Bill's provisions. Their report was published on 1 February 2016.

8 Following pre-legislative scrutiny, the Government introduced a revised Bill to Parliament, accompanied by further explanatory material including a response to each of the three committees' recommendations, on 1 March 2016. The Bill was carried over into the second session and reintroduced in the House of Commons on 19 May 2016.

9 During its passage through the House of Commons, a number of Government amendments were made to the Bill, in response to concerns raised by the Opposition and others. These included overarching provisions making explicit the privacy protections which run throughout the Bill; further enhancements to safeguards, such as those which apply to the modification process for warrants; and changes to the warrant and notice serving procedure to provide greater reassurance to communications service providers. The Government also accepted an Opposition amendment which placed protections for trade unions on the face of the Bill, putting beyond doubt that investigatory powers cannot be used where the only purpose is to intrude on legitimate trade union activity.

10 Other amendments included enhanced protections for sensitive professions and parliamentarians, including the requirement that a Judicial Commissioner must consider that there is "an overriding public interest" before any request to identify a journalist's source can be approved. The Prime Minister must also personally approve a warrant to obtain the communications of an MP or a member of another relevant legislature.

11 The Government also announced at Report stage that David Anderson QC would carry out an independent review into the operational case for the bulk powers in the Bill. David Anderson, supported by an expert team of his own choosing, looked at 60 case studies provided by the three security and intelligence agencies and questioned 85 intelligence officials. His report, published on 19 August 2016, concluded that bulk powers are of vital importance to the security and intelligence agencies. Where alternative methods exist, David Anderson found that they are "often less effective, more dangerous, more resource-intensive, more intrusive or slower". His report made one recommendation: the creation of a Technology Advisory Panel (TAP) to advise on the impact of changing technology, and how MI5, SIS and GCHQ could reduce the privacy footprint of their activities.

12 The Bill was introduced in the House of Lords on 8 June 2016. A number of Government amendments were made at Report stage, with a particular focus on protections for legally privileged material and journalistic sources and material, and stronger safeguards for retention of communications data. They also amended the Bill to give effect to David Anderson's recommendation that a TAP should be created.

13 The ISC successfully tabled amendments to create an offence for the misuse of bulk powers, and to provide the ISC with access to the results of investigations carried out by the Investigatory Powers Commissioner (IPC) on the basis of a referral from the ISC, in so far as they relate to the Committee's functions. The Government also accepted an Opposition amendment requiring that access to internet connection records for the purpose of preventing or detecting crime should only be permitted, subject to limited exceptions, for the

investigation of offences carrying a maximum sentence of at least twelve months.

Legal background

14 With limited exceptions, the investigatory powers provided for in this Act already existed. This includes the interception of communications, the retention and acquisition of communications data, equipment interference, and the acquisition of bulk data. The Act has to an extent consolidated these powers in one place, though certain powers continue to exist elsewhere in legislation. There are also other enactments relevant to investigatory powers, as this section describes.

15 RIPA contained much of the legislative scheme governing the investigatory powers used to interfere with communications which the Act replaces. Part 1 of RIPA concerned communications. Chapter 1 of Part 1 concerned the interception of communications. It is repealed by the Act and replaced by Part 2 and Chapter 1 of Part 6. Chapter 2 of Part 1 concerned powers to acquire communications data (information concerning a communication, but not its content) from communications service providers. It is repealed and replaced by Part 3 of the Act. DRIPA made clear the extra-territorial extent of Part 1 of RIPA, which is now made clear in this Act.

16 The Wireless Telegraphy Act 2006 (section 49) provided for the authorisation of the use of wireless telegraphy equipment to obtain information about a communication, or the disclosure of such information. This is repealed by the Act, with such interception provided for in Part 2.

17 Sections 1 and 2 of DRIPA and the Data Retention Regulations 2014 contained the legislative scheme concerning the power of the Secretary of State to require communications service providers to retain communications data. Part 3 of the Counter-Terrorism and Security Act 2015 amended DRIPA so that an additional category of data - that necessary to resolve Internet Protocol addresses – could be included in a requirement to retain data. These provisions are replaced by Part 4 of the Act.

18 The power to interfere with property existed prior to this Act, being provided for in the Police Act 1997 and ISA. Part 3 of the Police Act 1997 provides for the authorisation of interference with property and wireless telegraphy. That continues to be the case, but those provisions have a much reduced scope: they cannot be used to authorise the obtaining of communications, private information or equipment data. Instead an authorisation under Part 5 is required. ISA similarly allows for the three intelligence services to be authorised to interfere with property and wireless telegraphy. Again, those provisions continue to exist but with a reduced scope. Section 13 of the Act sets out when the agencies must obtain an equipment interference warrant under Part 5 of Chapter 3 of Part 6.

19 Chapter 2 of Part 6 of the Act provides for warrants authorising the bulk acquisition of communications data. Before the Act, the bulk acquisition of communications data was authorised by a direction given under section 94 of the Telecommunications Act 1984. The section 94 power is repealed by the Act.

20 The security and intelligence agencies have the power to acquire information. The Security Service Act 1989 sets out the functions of MI5 and provides that MI5 can only obtain or disclose information so far as is necessary for those functions. ISA sets out the functions of SIS and GCHQ, and contains similar provision concerning the obtaining and disclosure of information. Part 7 of the Act does not provide a power for the security and intelligence agencies to acquire information, but provides for the retention and examination of BPDs.

21 Part 8 of the Act contains oversight arrangements. The IPC replaces the Interception of Communications Commissioner and the Intelligence Services Commissioner (provided for in Part 4 of RIPA) and the Surveillance Commissioners (provided for in the Police Act 1997 and given additional functions by Part 4 of RIPA). Part 4 of RIPA provides for the IPT, which continues to exist and is amended by this Act to have jurisdiction regarding matters in this Act.

22 Part 2 of RIPA (which concerns surveillance and covert human intelligence sources) and Part 3 of RIPA (which concerns the investigation of encrypted data) are not significantly amended by this Act. RIPSA makes similar provision to Part 2 of RIPA.

European law

23 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. Article 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 or detection of crime and the purposes laid down in Article 13 of the Data Protection Directive. Article 15(1) specifically provides for the retention of communications data.

24 Directive 2006/24/EC ('the Data Retention Directive') harmonised the retention of communications data. The Data Retention Directive was struck down by the European Court of Justice 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

25 The provisions in this Act extend to the whole of the United Kingdom.

26 See the table in Annex B for a summary of the position regarding territorial extent and application in the United Kingdom.

Commentary on provisions of Act

Part 1: General Privacy Protections

Section 1: Overview of the Act

27 As well as providing an overview of the Act, this section lists offences elsewhere in statute, beyond those in the Act, that provide relevant privacy protections for the powers contained in the Act.

Section 2: General duties in relation to privacy

28 This section sets out the numerous duties and considerations to which public authorities must have regard when taking decisions regarding the exercise functions under the Act, including whether to issue warrants, grant authorisations or give notices. Subsection (2) makes clear that when taking such decisions the public authority must consider whether what is sought to be achieved could reasonably be achieved by less intrusive means. The public authority must also have regard to the public interest in the protection of privacy and the integrity and security of telecommunication systems and any other aspect of the public interest in the protection of privacy.

29 This section requires that a public authority exercising functions under the Act must have regard to whether the level of protection to be applied to information should be higher because of the particular sensitivity of that information. Applying a higher level of protection in relation to obtaining information will include both considering whether particular safeguards should be applied and taking the sensitivity of the information into account when considering whether obtaining the information is proportionate. Subsection (5) includes examples of sensitive information, including items subject to legal privilege and information that identifies or confirms the identity of a source of journalistic information.

30 Subsection (3) makes clear that public authorities must also have regard to other considerations that are relevant in the context. This section does not list all of the considerations that may be relevant (as this will depend on the context of the particular decision) but lists some of the considerations, including the requirements of the Human Rights Act 1998.

31 This section does not provide that the public authority must comply with the Human Rights Act 1998 because that is already the case. Subsection (4)(d) does not affect the requirements imposed by the Human Rights Act 1998, including that it is unlawful for a public authority to act in a way that is incompatible with the European Convention on Human Rights.

32 While the title of this section is "General duties in relation to privacy", this does not imply that the requirements of the Human Rights Act 1998 are relevant only where privacy may be interfered with. Which of the Convention rights may be relevant to a decision will depend on the circumstances, but in the context of the use of investigatory powers, Article 8 (Right to respect for private and family life), Article 10 (Freedom of expression) and Article 1 of the First Protocol (Protection of property) are most likely to be relevant.

Section 3: Offence of unlawful interception

33 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

communications in the course of transmission via a public telecommunications system, a private telecommunications system or a public postal service. This offence previously existed under RIPA.

34 Subsection (2) provides 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 express or implied consent of such a person to carry out the interception. This is relevant to computer networks in the home or workplace for example.

35 Subsections (3), (4) and (5) signpost the sections of the Act which define:

a. interception and when this is understood to be taking place in the UK;

b. public telecommunications system, private telecommunications system and public postal service; and

c. when a person has lawful authority to carry out interception.

36 A public telecommunications system is a system 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.

37 Subsection (6) sets out the penalties for a person who is found guilty of the offence of unlawful interception under subsection (1). The penalty for unlawful interception replicates the penalty which existed under RIPA.

38 No one can be prosecuted under this section except 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.

Section 4: Definition of "interception" etc.

39 This section defines interception and sets out when interception is regarded as taking place in the United Kingdom.

40 Subsections (1) to (5) set out what constitutes intercepting a communication in the course of its transmission by a telecommunications system. There are three elements. Firstly the person must perform a "relevant act", which is defined in subsection (2) and includes modifying or interfering with the system. Secondly, the consequence of the relevant act must be to make the content of the communication available to a person who is not the sender or intended recipient. Thirdly, the content must be made available at a "relevant time", which means a time while the communication is being transmitted or any time when the communication is stored in or by the system.

41 The definition of a relevant time makes it clear that interception includes obtaining stored communications, such as messages stored on phones, tablets and other individual devices whether before or after they are sent.

> ### 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. This would also include an email which had not been sent by an individual but was stored on a server (e.g. a draft email).

42 Section 125(3) of the Postal Services Act 2000 explains that a postal packet is in the course of transmission from the time it is posted (i.e. delivered to a post office or letter box) to the time it is delivered to the person to whom it was addressed. The same rule applies in this Act.

Section 5: Conduct that is not interception

43 The purpose of this section 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 for the purposes of this Act. That means, for example, that watching television is not interception.

44 Subsection (2) excludes certain conduct in relation to postal data attached to the communication, e.g. reading the address on the outside of a letter in order to ensure it is delivered to the appropriate location.

Section 6: Definition of "lawful authority"

45 This section sets out the circumstances in which a person has lawful authority to carry out interception, so the offence of unlawful interception is not committed. There are three ways in which a person may have lawful authority to carry out interception. The first is through a targeted or bulk warrant. The second is through any of the other forms of lawful interception provided for in sections 44 to 52 of the Act, such as interception in prisons or interception with consent. Thirdly, in relation to stored communications, interception is lawful if authorised by an equipment interference warrant or if it is in exercise of any statutory power for the purpose of obtaining information or taking possession of any document or other property or in accordance with a court order.

46 This section also provides that interception or any other conduct authorised by a warrant under Part 2, a warrant under Chapter 1 of Part 6, or sections 44-52 of the Act is lawful for all purposes. This means that in complying with the authorisations and provisions listed above, a relevant authority or operator is not at risk of being found to be in breach of any other legal requirement.

Section 7: Monetary penalties for certain unlawful interceptions

47 This section provides for the IPC to impose fines (via a monetary penalty notice) 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.

48 Subsections (3) and (4) set out the conditions which must be met for IPC to issue a monetary penalty notice. The IPC 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.

Schedule 1: Monetary Penalty Notices

49 Schedule 1 sets out further details about monetary penalty notices. Part 1 sets out what a notice must contain, procedural requirements for giving a notice (including serving a notice of intent), powers for the IPC to vary or cancel a notice, and contains appeals and enforcement provisions. Part 2 of Schedule 1 provides for the IPC to give information notices requesting

further information from a person on whom the Commissioner is considering serving a monetary penalty notice, and sets out procedural requirements in relation to information notices, an appeal procedure and enforcement powers.

Section 8: Civil liability for certain unlawful interceptions

50 This section provides a right of redress through the civil courts for the sender or intended recipient of a communication in certain circumstances. The cause of action arises where a communication is intercepted, without lawful authority, in the course of its transmission by means of a private telecommunication system or by means of a public telecommunication system to or from apparatus that is part of a private telecommunication system.

Section 9: Restrictions on requesting interception by overseas authorities

51 This section provides that if a person in the UK asks the authorities of another country or territory to carry out the interception of communications of an individual believed to be in the British Islands at the time of the interception, a warrant authorised under Chapter 1 of Part 2 must always be in place.

Section 10: Restriction on requesting assistance under mutual assistance agreements etc.

52 This section provides that a mutual assistance warrant authorised under Chapter 1 of Part 2 must be in place before a request for interception can be made to authorities outside the UK under an EU mutual assistance instrument or an international mutual assistance agreement. Subsection (3) sets out the meaning of "international mutual assistance agreement" and "EU mutual assistance instrument", which must be designated in regulations made by the Secretary of State.

Section 11: Offence of unlawfully obtaining communications data

53 This section creates the offence of knowingly or recklessly obtaining communications data from a telecommunications or postal operator without lawful authority. The offence may be committed by a person within a public authority with powers to acquire communications data under Part 3 of the Act. It is a defence if a person in a public authority can show that they acted in the reasonable belief that they had lawful authority to obtain the communications data.

Section 12: Abolition or restriction of certain powers to obtain communications data

54 This section and Schedule 2 restrict general information gathering powers and certain specific pieces of legislation from being used to acquire communications data from a telecommunications or postal operator without the consent of the operator.

55 Numerous pieces of legislation provide public authorities with powers to require information in certain circumstances. This section ensures those pieces of legislation will no longer be able to be used to acquire communications data from telecommunications or postal operators.

56 This section does not apply where the power specifically relates to telecommunications or postal operators and is exercisable in connection with the regulation of such operators. This is to allow Ofcom and the Information Commissioner's Office to carry out legitimate regulatory functions, such as ensuring the radio spectrum is used in an effective way. These powers can only be used in such a way if it is not possible for the regulator to use the powers in the Act.

57 The restrictions in this section also do not apply where a power is being used to acquire communications data in relation to the conveyance or expected conveyance of any postal item into or out of the United Kingdom. Again, separate powers should only be used if it is not possible for the powers in the Act to be used.

58 Schedule 2 lists the powers that are being repealed or modified.

Schedule 2: Abolition of disclosure powers

59 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.

Section 13: Mandatory use of equipment interference warrants

60 This section requires that equipment interference conducted by the intelligence service must be authorised under the Act where the purpose of the interference is to obtain communications, private information or equipment data, in circumstances where the intelligence service considers that the conduct may constitute one or more offences under sections 1 to 3A of the Computer Misuse Act 1990, and there is a connection to the British Islands.

61 Subsection (2) defines a British Islands connection, establishing that there will be such a connection in circumstances where:

a. the proposed activity would take place in the British Islands (regardless of where the equipment to be interfered with is located). When an intelligence service is operating from the British Islands, they must use this Act to authorise their activity, even if the equipment itself leaves or does not enter the British Islands; or

b. the intelligence service believes that any of the equipment to be interfered with may be located in the British Islands at some point during the interference taking place. For example, this would include circumstances where a computer is located in the British Islands or is 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 relating to, or the communications sent to or from, a person believed to be in the British Islands (or the connected equipment data).

62 Subsection (3) clarifies that where the conditions in subsection (1) are not met, an intelligence service may still apply for an equipment interference warrant. The Codes of Practice will give examples of the circumstances in which the intelligence services may decide to do so.

Section 14: Restriction on use of section 93 of the Police Act 1997

63 This section means that applications by law enforcement agencies for property interference authorisations under section 93 of the Police Act 1997 may not be made where the purpose of the interference is to obtain communications, private information or equipment data, if the applicant considers the conduct constitutes an offence under sections 1 to 3A of the Computer Misuse Act 1990 and the conduct can be authorised under an equipment interference warrant. This restriction does not remove or otherwise limit the power to authorise property interference under the Police Act 1997 where the purpose of the interference is not to obtain communications, equipment data or any other information. Nor does this section prohibit the use of other legislation (e.g. the Police and Criminal Evidence Act 1984) to authorise conduct that may otherwise constitute a Computer Misuse Act offence.

Part 2: Lawful interception of communications

Chapter 1: Interception and examination with a warrant

Section 15: Warrants that may be issued under this Chapter

64 Subsection (1) explains that there are three types of warrants which can be issued under this chapter: a targeted interception warrant, a targeted examination warrant and a mutual assistance warrant.

65 Subsection (2) describes a targeted interception warrant and provides that such an interception warrant may authorise any activity for obtaining secondary data. Subsection (3) explains that a targeted examination warrant authorises the examination of material that has been collected under a bulk interception warrant. A targeted examination warrant must be sought whenever a member of an intelligence service wishes to look at material which relates to a person who is known 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.

66 Subsection (4) describes a mutual assistance warrant. Such a warrant gives effect to an incoming request, or authorises an outgoing request, for assistance in relation to the interception of communications. Such a request may be made in accordance with the EU Mutual Legal Assistance Convention, or another international agreement designated in regulations made by the Secretary of State.

67 Subsection (5) confirms that a warrant authorises any conduct necessary to fulfill what is authorised or required by the warrant, including the interception of communications not specifically described in the warrant, or the obtaining of secondary data from such communications. For example, a warrant can authorise the interception of communications of other individuals who may use the phone line or email account subject to a warrant. A warrant needs to be able to authorise this conduct because it would not be possible to intercept only those communications belonging to the person that is subject to the interception warrant where other people use the same device.

Section 16: Obtaining secondary data

68 This section describes secondary data which can be obtained under a targeted interception warrant. Secondary data means systems data or identifying data associated with or attached to the communications being transmitted. In order to be secondary data, identifying data must be capable of being separated from the communication in such a way that, when separated, it would not reveal the meaning (if any) of the content of the communication.

69 Systems data is defined in section 263 as data which enables or otherwise facilitates, or identifies or describes anything connected with enabling or facilitating, the functioning of any postal service, telecommunications system or any telecommunications service provided by means of that system. Anything that is systems data is not content.

70 Identifying data is defined in section 263 as data which can identify, or assist in identifying, any person, apparatus, telecommunication system or telecommunications service, or which identifies an event, or may be used to identify the location of any person, event or thing.

71 In the context of the interception of postal communications, secondary data does not include identifying data.

72 Secondary data obtained under a targeted interception warrant will be subject to the relevant safeguards set out in Part 2.

73 Secondary data may also be obtained under a bulk interception warrant. Equipment data comprising systems data and identifying data may be obtained pursuant to an equipment interference warrant.

74 Secondary data could include:

a. messages sent between items of network infrastructure to enable the system to manage the flow of communications;

b. router configurations or firewall configurations;

c. software operating system (including the version of that system);

d. the period of time a router has been active on a network;

e. the location of a meeting in a calendar appointment;

f. photograph information - such as the time/date and location it was taken; and

g. contact 'mailto' addresses within a webpage.

Section 17: Subject-matter of warrants

75 This section sets out the permitted subject matter of a warrant under this Chapter. 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 that a warrant may also relate to a group of linked persons, or to more than one person or organisation, or set of premises in the context of a single investigation or operation. A warrant may also relate to testing or training activities, explained in more detail in subsection (3).

Section 18: Persons who may apply for issue of a warrant

76 This section lists those persons who may apply to the Secretary of State for an interception warrant. These are the heads of: the three intelligence agencies; the National Crime Agency (NCA); the Metropolitan Police; the Police Services of Northern Ireland and Scotland; and HM Revenue & Customs, and the Chief of Defence Intelligence. A competent authority of another country may also apply for a mutual assistance warrant.

Section 19: Power of Secretary of State to issue warrants

77 This section sets out the circumstances in which the Secretary of State has power to issue a Part 2 warrant. Subsections (1), (2) and (3) require that the Secretary of State considers that the targeted interception, mutual assistance or examination warrant is necessary (for the purposes set out in section 20) 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 can be issued.

78 Subsection (4) makes clear that the Secretary of State may not issue a warrant under this section if it relates to serious crime activity in Scotland. In such circumstances the warrant will be issued by the Scottish Ministers (see section 21).

Section 20: Grounds on which warrants may be issued by Secretary of State

79 Subsection (2) sets out the grounds on which a warrant may be issued by the Secretary of State. These are: in the interests of national security, for the purpose of preventing or detecting serious crime, in the interests of the economic well-being of the United Kingdom (in circumstances relevant to the interests of national security), or for giving effect to the provisions of a mutual assistance agreement. Subsection (4) makes clear that a warrant may only be considered necessary in the interests of the economic well-being of the UK when it relates to the acts or intentions of persons outside the British Islands.

80 Subsections (5) and (6) specify circumstances in which a warrant may not be considered necessary. A warrant cannot be considered necessary if its only purpose is gathering evidence for use in legal proceedings, or only on the basis that the information that would be obtained

relates to trade union activity in the British Islands.

Section 21: Power of Scottish Ministers to issue warrants

81 This section provides that the Scottish Ministers may issue a warrant under this Chapter, on a relevant Scottish application (see section 22), where they consider that the warrant is necessary for the prevention or detection of serious crime, and proportionate to what is sought to be achieved. The decision of the Scottish Ministers to issue the warrant must also have been approved by a Judicial Commissioner. The same limits regarding gathering evidence for legal proceedings and trade union activity apply as for warrants issued by the Secretary of State.

Section 22: "Relevant Scottish applications"

82 This section sets out the cases in which the Scottish Ministers, rather than the Secretary of State, may issue a warrant (referred to as a "relevant Scottish application"). A targeted interception or examination warrant may be issued by the Scottish Ministers if the application relates to a person or premises in, or reasonably believed to be in, Scotland.

83 A mutual assistance warrant which authorises the making of an outgoing request may be issued by the Scottish Ministers if the application is made by or on behalf of the chief constable of Police Scotland, the Commissioners for HM Revenue and Customs or the Director General of the National Crime Agency for the purpose of preventing or detecting serious crime in Scotland and if the application relates to a person or premises in, or reasonably believed to be in, Scotland.

Section 23: Approval of warrants by Judicial Commissioners

84 This section sets out the test that the Judicial Commissioner must apply when considering whether to approve a decision to issue a warrant. He or she must review the conclusions the Secretary of State (or the Scottish Ministers) came to regarding the necessity and proportionality of the warrant. In doing so the Judicial Commissioner must apply the same principles that a court would apply on an application for judicial review. The Judicial Commissioner must review the conclusions as to necessity and proportionality with sufficient care to comply with the general privacy duties set out in section 2.

85 Subsection (4) makes clear that where a Commissioner refuses to approve a warrant he or she must set out written reasons for the 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.

86 Subsection (5) sets out that the person who issued the warrant 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 right of appeal and the warrant cannot be issued.

Section 24: Approval of warrants issued in urgent cases

87 This section sets out the process for issuing a warrant in urgent cases. If the person issuing the warrant deems the warrant to be urgent then it can be issued without the approval of a Judicial Commissioner. Subsection (2) requires that a Judicial Commissioner must be notified that the urgent warrant has been issued. Subsection (3) provides that the Commissioner must decide whether to approve the decision to issue the warrant within three working days.

88 If the Judicial Commissioner refuses to approve the urgent warrant then subsection (4) provides that the warrant ceases to have effect and may not be renewed. The Investigatory Powers Commissioner cannot be asked to reconsider a Judicial Commissioner's decision to refuse an urgent warrant.

Section 25: Failure to approve warrant issued in urgent case

89 If a Judicial Commissioner refuses to approve the decision to issue a warrant, those exercising powers under the warrant must, as far and as quickly as they can, stop any activity being undertaken.

90 A Judicial Commissioner can determine what can happen to any material gathered under an urgent warrant that has not been approved.

91 Subsection (4) provides for representations to be made to the Judicial Commissioner by the person who issued the urgent warrant or the authority who applied for it.

92 Subsections (6) and (7) provide for the person who issued an urgent warrant to ask the Investigatory Powers Commissioner to review a Judicial Commissioner's decision as to what can happen to any material obtained under an urgent warrant that the Commissioner refused to approve. The Investigatory Powers Commissioner can confirm the Judicial Commissioner's decision or make a fresh determination.

93 Subsection (8) provides that the urgent warrant being cancelled does not mean that anything already done under the warrant is unlawful. The same applies to anything that it is not reasonably practicable to stop doing.

Section 26: Members of Parliament etc.

94 This section requires the Secretary of State to obtain the approval of the Prime Minister (as well as a Judicial Commissioner) before issuing a targeted interception or examination warrant where the purpose is to obtain the communications of a person who is a Member of Parliament, a Member of the European Parliament representing the United Kingdom, or a member of one of the devolved legislatures.

Section 27: Items subject to legal privilege

95 This section sets out the safeguards which apply to the interception or selection for examination of legally privileged material authorised under this Chapter. Items subject to legal privilege can be understood as communications between a lawyer and their client, or a person representing that client, in connection with legal advice or legal proceedings. Further detail is provided in the Interception of Communications Code of Practice.

96 Where the purpose, or one of the purposes, of a warrant is to obtain communications subject to legal privilege, the warrant application must make that clear. The person issuing the warrant must consider the public interest in the confidentiality of items subject to privilege. That person must be satisfied that there are exceptional and compelling circumstances which make the interception or selection for examination of these items necessary, and that there are specific arrangements in place for how these items will be handled, retained, used and destroyed. Subsection (5) provides that a warrant for the purpose of protecting the interests of the economic well-being of the UK so far as those interests are also relevant to national security cannot be issued with the purpose of targeting legally privileged material. Subsection (6) provides further detail on what may constitute exceptional and compelling circumstances.

97 Where an agency applies for a targeted interception warrant and believes it is likely that they will obtain items subject to legal privilege, this must be made clear in the warrant application, including an assessment of the likelihood of obtaining such items. The person authorising the warrant may do so only if they are satisfied that there are specific arrangements in place for how such items would be handled, retained, used and destroyed.

98 Subsections (11) to (13) set out the safeguards which apply when the purpose of a targeted interception or examination warrant is to authorise or require the interception or selection for

examination of communications that, if they were not made with the intention of furthering a criminal purpose, would be items subject to privilege. They provide that in those circumstances the warrant application must set out the reasons for believing the communications are likely to be made with the intention of furthering a criminal purpose, and the person authorising the warrant may only do so if they consider that the communications are likely to be made with the intention of furthering a criminal purpose.

Section 28: Confidential journalistic material

99 This section sets out the additional safeguards which apply when the purpose, or one of the purposes of a targeted interception or examination warrant is to authorise or require the interception or selection for examination of communications which the agency believes will contain confidential journalistic material. It provides that the warrant application must include a statement that the purpose or one of the purposes of the warrant is to identify or confirm a source of journalistic information. In addition, specific arrangements must be in place for the handling, retention, use and destruction of communications containing confidential journalistic material. The definition of "journalistic material" and "confidential journalistic material" is provided in section 264.

Section 29: Sources of journalistic information

100 This section sets out the additional safeguards which apply when an agency applies for a targeted interception warrant and the purpose, or one of the purposes, of the warrant is to identify or confirm a journalist's source. It provides that the warrant application must make clear that this is the purpose or one of the purposes. In addition, specific arrangements must be in place for the handling, retention, use and destruction of material that identifies sources of journalistic information.

Section 30: Decisions to issue warrants to be taken personally by Ministers

101 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. Where that is not reasonably practicable, the warrant may be signed by a senior official designated by a Secretary of State or member of the Scottish Government, but the Secretary of State or member of the Scottish Government must personally and expressly authorise the issuing of the warrant.

102 Wherever the Act refers to "a member of the Scottish Government" this is a reference to one of the Scottish Ministers. It does not refer to an official or any other person.

Section 31: Requirements that must be met by warrants

103 This section deals with the information which needs to be contained in Part 2 warrants. Subsections (2) to (8) specify the information a warrant must contain. If a warrant relates to a single person, organisation or set of premises, the warrant must name that person or organisation or those premises.

104 A warrant may relate to a group of persons linked by a common purpose or activity, or to more than one person, organisation or set of premises linked to a single operation or investigation. In such a case the link must be described and the warrant must name or describe as many of the persons, organisations or sets of premises as is reasonably practicable.

105 The warrant must specify the factors that are to be used to identify the communications that are to be intercepted or selected for examination. This section does not include an exhaustive list of possible factors but a factor may be an address or a telephone number, for example.

106 Subsection (10) makes clear that communications from or intended for a person or

organisation includes communications from or intended for anything owned, controlled or operated by that person or organisation.

Section 32: Duration of warrants

107 This section deals with the duration of a Part 2 warrant. An interception warrant will last for six months (unless it is cancelled earlier). If the warrant is not renewed it will cease to have effect after that period. Urgent warrants will last for five working days unless renewed.

Section 33: Renewal of warrants

108 Subsections (1) to (3) state that a warrant may be renewed by the Secretary of State or, in the case of a warrant issued by the Scottish Ministers, a member of the Scottish Government. In order to be renewed, a warrant must remain necessary and proportionate, applying the same tests as for issuing a warrant. As with an application for an interception warrant, the decision to renew the warrant must also be approved by a Judicial Commissioner. The additional protections for Members of Parliament, etc. (see section 26), for legally privileged material (see section 27), for confidential journalistic material (section 28), and for sources of journalistic information (section 29) apply when renewing warrants as they do when issuing warrants. A warrant may not be renewed more than 30 days in advance of the warrant ceasing to have effect.

Section 34: Modification of warrants

109 This section sets out the modifications which may be made to a targeted interception or examination warrant, or a mutual assistance warrant.

110 The only modifications that may be made are adding, varying or removing the name or description of a person, organisation or premises, or adding, varying or removing a factor specified in the warrant. Adding or varying a name or description is referred to as a major modification. Adding, varying or removing a factor, or removing a name or description, is a minor modification.

111 Subsection (3) provides that a warrant relating to a single person, organisation or a single set of premises cannot be modified to add, vary or remove a person, organisation or set of premises.

112 A decision to modify a warrant must be taken personally by the person making the modification, and the modification instrument must be signed by that person.

Section 35: Persons who may make modifications

113 This section sets out who is able to make major and minor modifications. The effect of the provision is that major modifications may be made by the person who issued the warrant or their senior officials. Minor modifications may, in addition, be made by a person holding a senior position in the authority that applied for the warrant. Subsection (3) provides that, in urgent cases, major modifications may be made by a person holding a senior position in the authority that applied for the warrant.

114 However, what this section says is subject to special rules when the additional safeguards in sections 26 to 29 apply.

Section 36: Further provision about modifications

115 A modification which adds a name or description to a warrant, or which adds a factor to a warrant, can only be made if the modification is necessary and the conduct authorised by the modification is proportionate to what is sought to be achieved. This means that adding something to a warrant is subject to the same necessity and proportionality test as issuing a warrant. This section also sets out that the additional protections for Members of Parliament,

etc. (section 26), items subject to legal privilege (section 27), items containing confidential journalistic material (section 28) and communications that identify a journalist's source (section 29) apply in relation to a decision to make a major modification of a warrant as apply in relation to a decision to issue a warrant.

116 Subsection (5) makes clear that a modification which relates to the communications of a Member of Parliament or member of another relevant legislature can only be made by a Secretary of State (or a member of the Scottish Government for warrants issued by the Scottish Minister) and only has effect after the decision to make the modification has been approved by the Judicial Commissioner. Subsection (6) provides that a major modification in relation to items subject to legal privilege, items which contain confidential journalistic material, and communications which identify a journalist's source can only be made by a Secretary of State or a member of the Scottish Government, or in urgent case, a senior official acting on their behalf. Such modifications must be approved by a Judicial Commissioner before they have effect, except where the person making the modification considers that there is an urgent case to make it. Subsections (8) and (9) provide for circumstances where the Secretary of State has taken a decision to modify a warrant but it is not reasonably practicable for them to sign the instrument. The rules in subsections (8) and (9) are the same as for issuing warrants.

Section 37: Notification of major modifications

117 A Judicial Commissioner must be notified as soon as is reasonably practicable of a major modification and the reason for it. This notification requirement does not apply in circumstances where the Judicial Commissioner is required to approve the modification before it has effect, such as where it relates to Members of Parliament, legally privileged communications, confidential journalistic material or the identification of a journalist's source. It also does not apply to urgent modifications where a different procedure applies (see section 38).

118 Where a major modification 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 informed.

Section 38: Approval of major modifications made in urgent cases

119 This section sets out the process for approving a major modification to a warrant which has been made urgently. In most cases the fact that a major modification was made urgently means that the modification could be made by a person holding a senior position in the intercepting authority, rather than by a senior official acting on behalf of the Secretary of State or the Scottish Ministers. The urgent modification must then be approved within 3 working days by a senior official designated by the Secretary of State or the Scottish Ministers.

120 Where the additional safeguards in sections 26 to 29 apply, the case being urgent means that the warrant may be modified without the prior approval of a Judicial Commissioner. The modification must then be approved within 3 working days by a Judicial Commissioner.

121 Where a designated senior official takes a decision, a Judicial Commissioner and either the Secretary of State or, in the case of a warrant issued by the Scottish Ministers, a member of the Scottish Government must be informed. Where the decision whether or not to approve the modification is taken by a Judicial Commissioner, the Secretary of State or a member of the Scottish Government will have to be informed courtesy of section 37(3), which is why that notification requirement is not dealt with in this section.

122 If the designated senior officer or the Judicial Commissioner refuses to approve the modification, the warrant (unless it no longer has effect) has effect as if the modification had not been made.

Section 39: Cancellation of warrants

123 This section provides that the Secretary of State, a member of the Scottish Government or a senior official acting on their behalf may cancel a warrant at any time. They must do so if the warrant is no longer necessary on any relevant grounds or the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved.

Section 40: Special rules for certain mutual assistance warrants

124 This section deals with the process for certain mutual assistance warrants. This applies to incoming requests to provide assistance with intercepting the communications of an individual outside the United Kingdom or in relation to premises outside the United Kingdom.

125 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.

Section 41: Implementation of warrants

126 This section provides that the person who has obtained the warrant (i.e. the head of the intercepting authority) may require other persons to assist in giving effect to a targeted interception warrant or mutual assistance 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 the warrant may be served by providing a copy of the warrant itself or one or more of the schedules contained in the warrant. Subsection (5) sets out that the provision of assistance includes the disclosure of anything obtained under the warrant.

Section 42: Service of warrants outside the United Kingdom

127 This section sets out the process for serving a targeted interception warrant or a mutual assistance warrant on a person outside the United Kingdom. Subsection (2) provides that a warrant must be served in such a way as to bring its contents to the attention of the person who is to be required to give effect to it. Subsections (3) and (4) set out the ways a warrant may be served on a person outside the United Kingdom.

Section 43: Duty of operators to assist with implementation

128 This section provides that a telecommunications or postal operator served with a targeted interception warrant or a mutual assistance warrant is required to take steps to give effect to it. The obligation applies whether or not the operator is in the UK. However, the operator is not required to take any steps that it is not reasonably practicable for the operator to take. Subsection (5) makes clear that in considering what is reasonable, any requirements or restrictions under the laws of the country in which an operator is based must be taken into account. Subsection (6) provides that, where a technical capability notice under Part 9 has been given to the operator, the requirements placed on the operator are relevant to the consideration of what is reasonable.

129 Subsection (7) sets out the offence for knowingly failing to comply with the obligation to give effect to an interception warrant. The duty to comply with a warrant is enforceable against a person (whether or not they are in the UK) by civil proceedings brought by the Secretary of State.

Chapter 2: Other forms of lawful interception

Section 44: Interception with the consent of the sender or recipient

130 Subsection (1) provides that communications may be intercepted if both the person sending the communication and the intended recipient of the communication have given consent for the interception to take place.

131 Subsection (2) states 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 RIPA, or under RIPSA.

> ### Example:
> A kidnapper is telephoning relatives of a hostage, and the police wish to listen to the calls in order to identify or trace the kidnapper. The intended recipient of the communication (i.e. the relatives of the hostage) consent to the interception. That means that the police listening to the call can be authorised using an authorisation under Part 2 of RIPA and an interception warrant is not required.

Section 45: Interception by providers of postal or telecommunications services

132 This section authorises interception where it takes place for the purpose of providing or operating a postal service or telecommunications service, of enforcing any enactment relating to the use of such a service, or of the provision of services aimed at restricting access to the content of communications. For example, a postal provider may need to open a postal item to determine the address of the sender because the recipient's address is unknown. A further example is where a telecommunications operator 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).

133 Subsection (3) makes clear that a telecommunications operator 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.

Section 46: Interception by businesses etc. for monitoring and record-keeping purposes

134 This section allows the Secretary of State to make regulations which authorise interception where it would constitute a legitimate practice that is reasonably required for the carrying out of the activities of a business, a government department or public authority.

> ### Example:
> The recording of telephone conversations by businesses, such as call centres, for training or quality control purposes.

Section 47: Postal services: interception for enforcement purposes

135 This section provides that the interception of postal items is authorised where it is carried out by HM Revenue & Customs in exercising the power in section 159 of the Customs and Excise Act 1979, or by an examining officer under paragraph 9 of Schedule 7 of the Terrorism Act 2000.

Section 48: Interception by Ofcom in connection with wireless telegraphy

136 This section allows the interception of communications if carried out by the Office of Communications (Ofcom) in the exercise of certain of its functions, including the granting of wireless telegraphy licences and preventing and detecting interference with wireless telegraphy.

137 Ofcom use equipment to find the source of radio frequency interference rather than to listen to or read communications.

Section 49: Interception in prisons

138 Prison rules provide a power to intercept communications in prisons in certain circumstances. This section provides that such interception is lawful if it is carried out in accordance with the prison rules. This section does not set out the circumstances in which such interception may be carried out or the safeguards that apply as that detail is contained in the prison rules.

Section 50: Interception in psychiatric hospitals etc.

139 Interception may be carried out in certain psychiatric hospitals if it is in accordance with a direction given under certain other legislation, or in exercise of a power provided in certain other legislation. This section provides that such interception is lawful if is carried out in accordance with the direction or statutory power. This section does not set out the circumstances in which such interception may be carried out or the safeguards that apply as that detail is contained in the relevant direction or legislation.

Section 51: Interception in immigration detention facilities

140 Certain statutory rules contain powers to intercept communications in immigration detention facilities. This section provides that such interception is lawful if carried out in accordance with those rules. This section does not set out the circumstances in which such interception may be carried out or the safeguards that apply as that detail is contained in the rules.

Section 52: Interception in accordance with overseas requests

141 This section deals with the issue of interception when a request is made from overseas.

142 Subsections (2) to (5) set out the conditions which need to be met in order that a telecommunications or postal operator may intercept the communications of an individual, at the request of another country. This includes that the individual about whom information is being sought is outside the UK or that the person making the request and the person carrying out the interception believe that the individual is outside of the UK. Further conditions may be contained in regulations made by the Secretary of State.

Chapter 3: Other provisions about interception

Section 53: Safeguards relating to retention and disclosure of material

143 This section sets out that the issuing authority must ensure that arrangements are in force for securing that certain requirements are met relating to retention and disclosure of material obtained under the warrant. The number of persons who see the material, the extent of disclosure and the number of copies made of any material must be to the minimum necessary for the authorised purposes. Subsection (3) sets out the circumstances in which something is necessary for the authorised purposes - for example where it is necessary for the functions of the Secretary of State or a Judicial Commissioner under the Act.

144 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. Subsection (7) requires that the Investigatory Powers Commissioner must be informed where confidential

journalistic material or material which identifies a source of journalistic material is retained for purposes other than destruction.

145 The requirements in this section do not apply to material, or copies of material, handed over to an overseas authority. Section 54 applies instead.

Section 54: Safeguards relating to disclosure of information overseas

146 This section sets out the safeguards which apply when disclosing intercepted content and secondary data to an overseas authority. The Secretary of State or the Scottish Ministers must be satisfied that safeguards equivalent to those required by section 53 are in place, to the extent that the Secretary of State or Scottish Ministers considers appropriate. They must also be satisfied that restrictions are in place that would prevent, to the extent that they think appropriate, disclosure of the material in legal proceedings.

Section 55: Additional safeguards for items subject to legal privilege

147 This section sets out the safeguards which apply when an item subject to legal privilege is retained for purposes other than its destruction. The Investigatory Powers Commissioner must be informed as soon as is reasonably practicable. The Commissioner has the power to order that the item subject to legal privilege is destroyed, or to impose conditions as to the use or retention of the material.

148 The Investigatory Powers Commissioner must consider that the public interest in retaining the items outweighs the public interest in the confidentiality of items subject to privilege, and that retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury. If that test is not met, the Commissioner must exercise the power to order destructions or impose conditions. Even if the test is met, the Investigatory Powers Commissioner may still impose any conditions the Commissioner thinks necessary to protect the public interest in the confidentiality of items subject to privilege.

149 Subsections (4) and (5) provide that the Commissioner may require the person who issued the warrant and the person to whom the warrant is addressed to make representations to the Commissioner about the retention of items or the conditions that might be imposed and provides that the Commissioner must have regard to those representations, and any representations which those persons choose to make, if not required to do so.

Section 56: Exclusion of matters from legal proceedings etc.

150 This section prevents intercepted communications or secondary data being used or disclosed in legal proceedings or an inquiry held under the Inquiries Act 2005. This includes adducing such material 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.

151 The exceptions to this prohibition are set out in Schedule 3.

Schedule 3: Exceptions to section 56

152 Schedule 3 sets out the exceptions to section 56(1), 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 does not apply.

153 Paragraph 2 provides that the contents of a communication and secondary data may be disclosed if the communication is obtained under certain statutory powers exercised to obtain information, documents or property or a court order allowing the same. Material may be disclosed if obtained under an equipment interference warrants (whether targeted or bulk) or through any of the other forms of lawful interception in sections 44 to 52 (interception in

prisons, for example).

154 Paragraph 3 provides that there is no prohibition on doing anything which discloses conduct for which a person has been convicted of certain offences. So, for example, it will be possible to disclose that someone has been convicted of the offence of unlawful interception (see section 3(1)).

155 Paragraphs 4 and 5 provide that section 56(1) does not apply in relation to proceedings before the Investigatory Powers Tribunal or the Special Immigration Appeals Commission. In proceedings before the Special Immigration Appeals Commission, disclosure is not permitted to the appellant or applicant or their representatives, but may be made to special advocates appointed for the purpose of those proceedings.

156 Paragraph 6 provides that section 56(1) does not apply in relation to proceedings before the Proscribed Organisations Appeal Commission, providing there is no disclosure to certain persons or bodies, including the applicant and the organisation concerned. Disclosure is not permitted to their representatives but can be made to a special advocate appointed for the purpose of the proceedings.

157 Paragraph 7 provides that section 56(1) does not apply to closed material proceedings (i.e. section 6 proceedings as defined by section 14(1) of the Justice and Security Act 2013). However, this does not allow disclosure to anyone who is or was party to the proceedings, or any representative of theirs who is not a special advocate, other than the Secretary of State or the person making the disclosure of sensitive material that made the use of closed material proceedings necessary.

158 Paragraphs 8 and 9 provide that section 56(1) does not apply to TPIM proceedings or TEO proceedings (i.e. proceedings relating to terrorism prevention and investigation measures or temporary exclusion orders). However, this does not allow disclosure to any person involved or party to the proceedings, or any representative of theirs who is not a special advocate, other than the Secretary of State.

159 Paragraphs 10 to 12 provide that section 56(1) does not apply in proceedings relating to financial restrictions or the freezing of terrorist assets providing that there is no disclosure to any person who is party to the proceedings, or any representative of theirs who is not a special advocate, other than the Treasury.

160 Paragraph 13 provides that section 56(1) does not apply in proceedings relating to the release of prisoners in Northern Ireland (proceedings before the Parole Commissioners for Northern Ireland or any Sentencing Review Commissioners) providing there is no disclosure to any person who is party to the proceedings, or their representatives who are not special advocates, other than the Secretary of State.

161 Paragraphs 14 and 15 provide that section 56(1) does not apply in relation to certain employment or industrial tribunal proceedings where the applicant or their representatives are excluded for all of part of the proceedings, providing there is no disclosure to the applicant in the proceedings or their representatives who are not special advocates.

162 Paragraph 16 provides that section 56(1) does not prevent anything done in connection with legal proceedings relating to the fairness of dismissal for offences under the Act, or offences under RIPA or the Interception of Communications Act 1985.

163 Paragraphs 17 and 18 provide that section 56(1) does not apply in relation to appeal proceedings relating to claims of discrimination in Northern Ireland where the party to the appeal or their representatives are excluded from all or part of the proceedings, providing there is no disclosure to any person who is party to the proceedings or their representatives

who are not special advocates.

164 Paragraph (19) provides that section 56(1) does not apply in relation to civil enforcement proceedings where a relevant service provider has failed to comply with the duty to assist with the implementation of a warrant.

165 Paragraph 20 lists the offences in relation to which section 56(1) does not apply. These include proceedings for offences under the Act, and related offences.

166 Paragraph 21 provides that disclosure can be permitted during criminal proceedings to prosecutors so that the prosecutor can determine what the prosecutor needs to do to ensure that the prosecution is fair.

167 The paragraph also allows disclosure to a judge where the judge considers there are exceptional circumstances making the disclosure essential in the interests of justice. Sub-paragraph (3) allows a 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. However, sub-paragraph (3) does not allow a disclosure that contravenes section 56(1).

168 Paragraphs 22 to 24 deal with disclosures to inquiries and inquests. Paragraph 22 provides that disclosure can be made to a panel of an inquiry held under the Inquiries Act 2005 or to someone appointed as a legal adviser to such an inquiry. This includes Counsel to an inquiry or the Solicitor to an inquiry. Paragraph 23 provides that disclosure can be made during restricted proceedings of an inquiry held under the Inquiries Act 2005, and sets out who may be present at such proceedings. Paragraph 24 provides that disclosure can be made to a judge or retired judge nominated to conduct an inquest into a death. Disclosure is also permitted to the legal adviser to such an inquest. In both cases the legal adviser appointed will need to hold suitable security clearance. Subsection (3) allows the fact that intercept material exists in a specific case to be disclosed to the coroner, and to the legal adviser to the inquest, for the purpose of considering whether the material is relevant and, if so, whether it should be disclosed to the person leading the inquest. In such circumstances, the disclosure could only be to a nominated person (i.e. a judge). No disclosure may be made to any other party in connection with these proceedings.

Section 57: Duty not to make unauthorised disclosures

169 This section 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.

Section 58: Section 57: meaning of "excepted disclosure"

170 This section provides that in certain situations the duty not to make an unauthorised disclosure in section 57 does not apply. Disclosures made in such circumstances are called "excepted disclosures". Excepted disclosures are grouped into 4 heads.

171 Head 1 includes disclosure authorised by the warrant. It also includes disclosure which is necessary for the purpose of providing assistance in giving effect to a warrant (for example, where a company may not own the relevant part of the network to undertake the interception and requires the assistance of another company to give effect to the warrant). Head 2 allows disclosure made to or authorised by a Judicial Commissioner, or a disclosure to the Independent Police Complaints Commission or the Intelligence and Security Committee of Parliament. Head 3 allows disclosures made by a professional legal adviser in connection with legal proceedings, or a disclosure between a client and professional legal adviser in connection with advice about Part 2 of the Act or relevant provisions of RIPA. Head 4 allows the disclosure of statistical information by a postal operator or telecommunications operator,

subject to any requirements imposed by regulations made by the Secretary of State, and for the disclosure of information by any person about warrants in general. This does not provide for disclosure of any particular warrant issued under Chapter 1.

Section 59: Offence of making unauthorised disclosures

172 This section provides that it is an offence to fail to comply with the duty in section 57(1) not to make unauthorised disclosures, and sets out the maximum penalties for the offence.

Section 60: Part 2: interpretation

173 This section sets out definitions for a number of terms used throughout this section.

Part 3: Authorisations for obtaining communications data

Section 61: Power to grant authorisations

174 This section provides the power for relevant public authorities to acquire communications data. Communications data is the 'who', 'when', 'where' and 'how' of a communication, but not its content, and is defined in sections 261 and 262 of the Act. An authorisation can be granted where a designated senior officer in a relevant public authority is content that a request is necessary for one of the 10 purposes set out in subsection (7) and proportionate to what is sought to be achieved. Communications data cannot be acquired for any other purposes and only certain authorities can use certain purposes, as outlined in Schedule 4.

175 Subsection (4) provides for some of the conduct which an authorisation may permit for the purpose of acquiring communications data. For example conduct to acquire communications data may involve:

a. serving a notice on a telecommunications or postal operator that requires them to disclose the relevant data;

b. serving a notice on a telecommunications or postal operator that requires them to obtain and then disclose the relevant data;

c. a relevant public authority acquiring the data directly from an operator through a secure auditable system; or

d. a relevant public authority acquiring the data directly from a telecommunications system.

176 An authorisation cannot authorise any conduct which requires the interception of the content of a communication or requires the interference with any equipment on a telecommunications network.

177 Subsection (5) provides that 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 interest. It also provides that an authorisation can authorise the disclosure of communications data by a communications service provider through a secure auditable system.

178 Subsection (8) makes explicit that legitimate trade union activity would never be sufficient grounds, of itself, for a communications data authorisation to be considered necessary.

Section 62: Restrictions in relation to internet connection records

179 This section provides restrictions concerning the acquisition of internet connection records

that are retained by communications service providers in accordance with a notice given under section 87 of the Act. It requires one or more of three conditions - A, B and C – to be satisfied before data which is, or can only be obtained by processing, an internet connection record can be obtained.

180 Condition A is that the data is necessary, for any of the ten purposes in section 61(7), to identify the sender of an online communication. An application for such data will often be for the purposes of IP address resolution - i.e. attributing an internet protocol address to an individual - and the internet service must be known in advance of the application. For example the public authority will be aware of an action – such as the uploading of illegal images - on a particular internet service at a specific time or range of time. The communications data application would be to determine which individual carried out that action at that time.

181 Condition B is that the data is to be obtained for any of the statutory purposes other than the prevention or detection of crime; and the data is necessary to identify:

a. which communication services a person has been using, for example determining whether they are communicating through apps on their phone;

b. where a person has accessed illegal content, for example an internet service hosting child abuse imagery; or

c. which internet service is being used and when and how it is being used.

182 In respect of (a) and (b) 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. If approved, a request would then be made to a communications service provider for all internet connection records in that timeframe.

183 In respect of (c), the designated senior officer within a relevant public authority could approve the application in order to identify what activities a person had been conducting online. This could include activity to determine whether a vulnerable missing person had been accessing travel sites before their disappearance.

184 Condition C is that the data is to be obtained for the prevention or detection of crime and is necessary for the same three investigative purposes described in Condition B. But the crime to be prevented or detected must be serious crime or other relevant crime as defined in subsection (6).

185 Subsection (6) defines "other relevant crime" for the purposes of Condition C, setting the thresholds which must be met before internet connections records can be obtained from communications service providers for the purpose of preventing and detecting crime.

186 Local authorities are prohibited from acquiring internet connection records for any purpose.

187 Subsection (7) defines an internet connection record for the purposes of the Act.

Section 63: Additional restrictions on grant of authorisations

188 This section provides that an authorisation for the acquisition of communications data can only be granted by an authorising officer who is independent of the operation in the context of which the data is sought.

189 The requirement for independent authorisation does not apply in exceptional circumstances, including where there is an imminent threat to life or where it is simply not possible due to the size of the public authority. Such circumstances also include those where the investigation

or operation concerned is one where there is an exceptional need, in the interests of national security, to keep knowledge of it to a minimum; and there is an opportunity to obtain information where the opportunity is rare, the time to act is short and the need to obtain the information is significant and in the interests of national security.

Section 64: Procedure for authorisations and authorised notices

190 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 section 61(7)), the conduct for which it was authorised, the type of data to be obtained, and who the data will be disclosed to.

191 Subsection (2) sets out that an authorisation which authorises a person to place an obligation on a telecommunications operator to acquire communications data must specify the name of the operator and the requirements that will be imposed on that operator.

192 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 operator, and the name of the operator.

193 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.

Section 65: Duration and cancellation of authorisations and notices

194 This section 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.

195 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.

196 Subsection (4) places a duty on the designated senior officer who has granted an authorisation to cancel it if they are satisfied that the authorisation is no longer necessary or proportionate.

197 Subsections (5) and (6) permit the Secretary of State to specify by regulations 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 - for example because the specified rank has ceased to exist.

Section 66: Duties of telecommunications operators in relation to authorisations

198 Communications service providers are required to comply with a request for communications data, except to the extent that 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.

199 Subsection (5) 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 specific performance of a statutory duty under section 45 of the Court of Session Act 1988 or for any other appropriate relief.

Section 67: Filtering arrangements for obtaining data

200 This section 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 communications data obtained, thereby ensuring that privacy is properly protected.

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 individual's 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.

201 These types of applications, as all communications data applications, would only be able to be made where necessary and proportionate.

202 The power to establish filtering arrangements in subsection (1) operates solely in the context of Part 3 of the Act 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.

Section 68: Use of filtering arrangements in pursuance of an authorisation

203 This section will apply in relation to the use of any request filter established under the power in section 67. 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.

204 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; and

b. whether the processing of data under the filter is allowed.

205 If the processing of data is allowed, then a description of data that may be processed must also be included.

206 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, including specifically the use of the request filter, is proportionate to what an investigator is seeking to achieve.

207 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.

Section 69: Duties in connection with operation of filtering arrangements

208 This section imposes duties in connection with the operation of filtering arrangements. Subsection (1) provides that no communications data must be obtained or processed under the filter except for the purposes of an authorisation granted under section 61(1). 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, must 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.

209 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.

210 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 of their functions; and

d. as otherwise authorised by law.

211 Subsection (3) requires strict limits to be placed on the number of 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. Only the Secretary of State and designated 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.

212 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.

213 Subsection (6) 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. A report must also 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. Subsections (5) and (6) will ensure that the operation of any request filter is subject to rigorous oversight and control.

214 Subsection (8) requires any significant processing errors to be immediately reported to the Investigatory Powers Commissioner.

Section 70: Relevant public authorities and designated senior officers

215 This section introduces Schedule 4 to the Act and makes provision in relation to relevant public authorities, designated senior officers and safeguards.

216 Schedule 4 includes a table which lists the public authorities permitted to obtain communications data under Part 3 of the Act (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 which they may be obtained (column 4).

217 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.

218 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. Examples include a police Superintendent in a police force or an immigration inspector in the Home Office.

219 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". An example is a manager in the security group of the National Offender Management Service responsible for intelligence.

220 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.

Schedule 4: Relevant public authorities

221 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 section 61(7), for which it can be accessed.

222 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.

223 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' 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. Entity and events data are defined in section 261.

Section 71: Power to modify section 70 and Schedule 4

224 This section provides that the Secretary of State may modify section 70 and Schedule 4 by regulations. 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 the table of authorities and officers in Schedule 4.

225 Subsection (3) provides that the Secretary of State's regulation-making power includes power to modify any enactment as a result of a person becoming, or ceasing to be a relevant public authority.

Section 72: Certain regulations under section 71: supplementary

226 This section provides that all changes to section 70 and Schedule 4 will be subject to the enhanced affirmative procedure except for changes which:

a. remove a public authority from the list in column 1 of the table; or

b. modify the rank of the designated senior officer in a public authority in column 2 of the table in such a way that does not reduce the rank of the person able to authorise acquisition of communications data.

227 By virtue of section 267 such orders will be subject to the negative resolution procedure.

228 When making changes to the relevant public authorities in Schedule 4 by the enhanced affirmative procedure, the Government must consult the Investigatory Powers Commissioner and the relevant public authority concerned. An example of such a change would be the addition of a new public authority to the list of relevant authorities.

Section 73: Local authorities as relevant public authorities

229 This section provides that local authorities are relevant public authorities for the purposes of Part 3, and defines the designated senior officers of local authorities.

230 Subsection (3) provides that local authorities may only acquire communications data for the purpose of preventing or detecting crime or of preventing disorder.

231 This section provides that the rank of a designated senior officer in relation to a local authority can be amended by regulations made under the enhanced affirmative procedure. Before making such regulations the Government must consult the Investigatory Powers Commissioner and the relevant local authorities concerned.

Section 74: Requirement to be party to collaboration agreement

232 This section 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.

Section 75: Judicial approval for local authority authorisations

233 This section provides a procedure by which local authority authorisations to obtain communications data can only take effect if approved by a relevant judicial authority.

234 This means that a local authority authorisation granted under section 73 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.

Section 76: Use of a single point of contact

235 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 communications service providers. This section sets out how the SPoC and designated senior officer work together when granting an authorisation for the acquisition of communications data.

236 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.

237 Subsection (4) sets out what constitutes a SPoC, specifically that they must be an officer in a relevant public 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.

238 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 may advise whether the application and authorisation is lawful, appropriate and cost-effective, and takes into consideration any unintended consequences.

239 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.

240 Subsection (8) makes clear that nothing prevents a person acting as a single point of contact from also applying for, or being granted, an authorisation or, in the case of a designated senior officer, granting an authorisation.

Section 77: Commissioner approval for authorisations to identify or confirm journalistic sources

241 This section sets out the procedure for authorising communications data requests made by a public authority in order to identify a journalistic source. In these instances it is necessary to obtain the approval of a Judicial Commissioner before the data can be acquired.

242 Subsections (1), (2) and (3) set out that an authorised communications data application made by a public authority for the purpose of identifying a 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.

243 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 application relates i.e. the journalistic source, nor that person's legal representative.

244 Subsections (5) and (6) set 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. In considering whether these conditions have been met, the Judicial Commissioner must have regard to both the public interest in protecting a source of journalistic information and the need for there to be another overriding public interest before approving an authorisation.

245 Subsection (7) sets out that the Judicial Commissioner may quash any authorisation given by the designated senior officer, if the Judicial Commissioner refuses to approve it.

Sections 78 and 79: Collaboration agreements

246 Sections 78 and 79 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 or where public authorities make requests infrequently. 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 senior officers and SPoCs in other public authorities who are more experienced in making applications, and may be used where the statutory purposes for which the collaborating public authorities can acquire communications data are different.

Section 80: Police collaboration agreements

247 The Police are already permitted to be in collaboration agreements, under the Police Act 1996. This section sets out further detail on their use in relation to Part 3. Subsection (6) makes clear that the National Crime Agency can be party to a police collaboration agreement for the purposes of this Act.

Section 81: Lawfulness of conduct authorised by this Part

248 Subsection (1) has the effect of making conduct lawful for all purposes if it is conduct in accordance with, or in pursuance of, an authorisation under this Part.

249 Subsection (2) exempts a person from civil liability in respect of conduct which is incidental to, or reasonably undertaken in conjunction with an authorisation, so long as the conduct could not itself have reasonably been authorised under this Act, the Regulation of Investigatory Powers Act 2000, the Police Act 1997, or section 5 of the Intelligence Services Act 1994.

Section 82: Offence of making unauthorised disclosure

250 This section creates a criminal offence, with a maximum prison sentence of two years, if a communications services provider discloses the existence of an authorisation for the obtaining of communications data to the subject of the authorisation. It is a reasonable excuse if such a requirement is disclosed with the permission of the public authority who requested the data.

251 The purpose 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.

Section 83: Certain transfer and agency arrangements with public authorities

252 This section allows for the Secretary of State, by regulations, to transfer ownership of the filtering arrangements to another public authority.

Schedule 5: Transfer and agency arrangements with public authorities: further provisions

253 This Schedule outlines the provisions that apply should the Home Secretary transfer ownership of the request filter to a public authority. Paragraph 1requires the Secretary of State to approve the measures to be adopted by a designated public authority for complying with the requirements in section 67. A designated public authority must send the reports required under section 69 , about the functioning of the filtering arrangements over the previous calendar year, and immediate reporting of any significant processing errors which have occurred, to the Secretary of State as well as to the Investigatory Powers Commissioner. Paragraph 2 requires the public authority to also report to the Secretary of State at least once per calendar year on their discharge of their functions, and any other matters the Secretary of State may require.

254 Paragraph 3 sets out that the Secretary of State, in connection with regulations made under section 83(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.

255 The consequential, supplementary, incidental and transitional provision that may be made by a transfer scheme 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)). A scheme may make provision for the payment of compensation, for example to a designated public authority in circumstances where functions conferred on that body are brought back within the Home Office. A transfer scheme may be included in regulations made under section 83(1) but if not, must be laid before Parliament after being made.

256 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, stamp duty reserve tax and stamp duty land tax.

Section 84: Applications of Part 3 to postal operators and postal services

257 This section provides that Part 3 of the Act applies to postal operators and postal services as it does to telecommunications operators and telecommunications services.

Section 85: Extra-territorial application of Part 3

258 This section sets out that telecommunications and postal operators overseas are also subject to the provisions of Part 3 of the Act. Subsection (3) sets out the ways in which a notice under Part 3 may be given to a person outside the UK. Subsection (4) sets out the matters to be taken into account in deciding whether it is reasonably practicable for an operator to take steps to comply with a duty under section 66. These include the law of the country in question.

Section 86: Part 3: interpretation

259 This section clarifies terms that are regularly referred to throughout Part 3 of the Act.

Part 4: Retention of communications data

Section 87: Powers to require retention of certain data

260 This section provides a power to require telecommunications operators to retain communications data, where necessary and proportionate for one or more of the statutory purposes for which it can be acquired (set out at section 61(7)), for a maximum period of 12 months.

261 The power is exercised by the Secretary of State giving a retention notice to a

telecommunications operator. The Secretary of State's decision must then be approved by a Judicial Commissioner (section 89). A retention notice, which may relate to one or more operators, will require the retention of specified items of communications data for the period or periods set out in the notice. The period for which data may be retained must be no more than 12 months. In addition to requiring the retention of specified data a notice may impose additional requirements and restrictions in relation to the retention of the data, such as requirements relating to the processing or security of retained data. Unless, or until, a retention notice is given, a telecommunications operator is not required to retain any communications data under this Act.

262 Subsection (4) provides that a retention notice cannot require the retention of so-called 'third party data'. Where one telecommunications operator is able to see the communications data in relation to applications or services running over their network, but where they do not use or retain that data for any purpose, it is regarded as 'third party data'.

263 Subsection (10) makes explicit that legitimate trade union activity would never be sufficient grounds, of itself, to establish that a requirement to retain data is necessary.

264 Subsection (11) describes communications data that can be retained by reference to what it can be used to identify, or assist in identifying. 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.

265 Subsection (11) also makes clear that communications data that can be retained includes internet connection records. Internet connection records, which are defined in section 62(7), 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. Section 62 provides certain restrictions on the acquisition of internet connection records.

Section 88: Matters to be taken into account before giving retention notices

266 This section sets out a number of factors that the Secretary of State must take into account before giving a retention notice to a telecommunications operator. These include: the likely benefits of giving such a notice; the likely number of users of the telecommunications service; the technical feasibility of complying with the notice; the likely costs of compliance; and any other impact that the notice may have on the telecommunications operator. In addition the Secretary of State must take reasonable steps to consult a telecommunications operator before giving it a notice.

Section 89: Approval of retention notices by Judicial Commissioners

267 This section sets out the test that the Judicial Commissioner must apply when considering whether to approve a decision to give a retention notice. He or she must review the conclusions the Secretary of State came to regarding the necessity and proportionality of the requirement to retain communications data. In doing so the Judicial Commissioner must apply the same principles that a court would apply on an application for judicial review. The Judicial Commissioner must review the conclusions as to necessity and proportionality with sufficient care to comply with the general privacy duties set out in section 2.

268 Subsection (4) makes clear that where a Commissioner refuses to approve a decision to give a notice he or she must set out written reasons for the refusal. Subsection (5) sets out that the Secretary of State may ask the Investigatory Powers Commissioner to reconsider an

application that a Judicial Commissioner has refused.

Section 90: Review by the Secretary of State

269 This section permits the recipient of a notice to refer the notice back to the Secretary of State for a review. Subsection (1) states that the provider will have the opportunity to refer a notice within a specified time period or circumstances which will be set out in regulations.

270 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, in particular consultation with the Technical Advisory Board and the Judicial Commissioner, are outlined at subsections (5) to (8).

271 Subsections (9) to (12) further govern the review process. They require the Commissioner and the Technical Advisory Board to consult the telecommunications operator concerned and the Secretary of State before reaching their conclusions. They must then 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. The Secretary of State can only confirm the effect of the notice or vary the notice if the decision has been approved by the Investigatory Powers Commissioner.

272 Subsection (13) imposes an obligation on the Secretary of State to keep a notice under review, regardless of whether or not it has been referred.

Section 91: Approval of retention notices following review under section 90

273 This section sets out the test that the Investigatory Powers Commissioner must apply when considering whether to approve a decision by the Secretary of State to vary a retention notice or give a notice confirming the effect of a retention notice following a review of that notice under section 90. He or she must review the conclusions the Secretary of State came to regarding the necessity and proportionality of the requirement to retain communications data. In doing so the Investigatory Powers Commissioner must apply the same principles that a court would apply on an application for judicial review. The Commissioner must review the conclusions as to necessity and proportionality with sufficient care to comply with the general privacy duties set out in section 2.

274 Subsection (4) makes clear that where the Investigatory Powers Commissioner refuses to approve a decision to vary a retention notice or give a notice confirming the effect of a retention notice, he or she must set out written reasons for the refusal.

Section 92: Data integrity and security

275 This section sets out security requirements and other protections for retained communications data. Data retained under a notice must be kept securely, protected against unauthorised access and, once the retention period expires, destroyed.

Section 93: Disclosure of retained data

276 Telecommunications operators must put in place adequate security procedures governing access to communications data in order to protect it against unlawful disclosure.

Section 94: Variation or revocation of notices

277 Subsections (1) to (12) 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. A Judicial Commissioner must approve the decision to vary a notice.

278 Subsections (13) to (16) provide for the revocation of data retention notices in full or in part.

Section 95: Enforcement of notices and certain other requirements and restrictions

279 Telecommunications operators are required to comply with a data retention notice and the requirements in the Act relating to the security, integrity, destruction and disclosure of data.

280 In addition this section provides that a telecommunications operator, or their staff, and the Information Commissioner, or his or her staff, may not disclose the existence or contents of a notice without the permission of the Secretary of State.

281 Subsection (5) specifies that the duties on telecommunications operators and their staff are enforceable by the Secretary of State by civil proceedings for an injunction, or (in Scotland) for specific performance of a statutory duty, or for any other appropriate relief.

Section 96: Application of Part 4 to postal operators and postal services

282 This section makes clear that the provisions of Part 4 also apply to postal operators and postal services.

Section 97: Extra-territorial application of Part 4

283 This section provides that telecommunications and postal operators based outside the United Kingdom, but providing services to customers based within the United Kingdom, can be required to retain relevant communications data related to such customers. A provider based outside the United Kingdom is subject to the requirement to retain communications data if given a retention notice, and has a duty to comply with the security requirements, but the enforcement provision in section 95(5) does not apply.

Section 98: Part 4: interpretation

284 This section provides for interpretation of this Part, including references for relevant definitions.

Part 5: Equipment interference

Section 99: Warrants under this Part: general

285 This section provides for the issuing of targeted equipment interference and targeted examination warrants and explains the activities and conduct that these warrants may authorise.

286 Subsection (2) sets out that a targeted equipment interference warrant authorises the interference with equipment for the purpose of obtaining communications, information or equipment data.

287 Subsection (3) provides that a targeted equipment interference warrant must also authorise the recipient to obtain communications, equipment data or other information, and may also authorise the recipient of the material under the warrant to subsequently disclose it.

288 Subsection (4) confirms that the acquisition of communications or other information through a targeted equipment interference can include monitoring, observing, or listening to communications or activities. As a result, it will not be necessary for such activity to be authorised separately under Part 2 of RIPA.

289 Subsection (6) provides that a targeted equipment interference warrant does not permit the acquisition of communications (other than stored communications) in circumstances where an interception warrant is required. If an investigation requires both equipment interference and interception techniques then a combined warrant may be issued.

290 Subsection (9) explains that a targeted examination warrant authorises the selection for examination of protected material acquired under a bulk equipment interference warrant. Protected material is any material obtained under a bulk equipment interference warrant other than equipment data or non-private information.

Section 100: Meaning of "equipment data"

291 This section defines the material which is equipment data that can be obtained under a targeted equipment interference warrant. Equipment data means systems data or identifying data. In order to be equipment data, identifying data must be capable of being separated from the communication or item of information in such a way that, when separated, it would not reveal the meaning (if any) of the content of the communication or the meaning (if any) of an item of information (disregarding any inferred meaning).

292 Systems data is defined in section 263 as data which enables or otherwise facilitates, or identifies or describes anything connected with enabling or facilitating, the functioning of any postal service, telecommunications system or any telecommunications service provided by means of the system or any other relevant system or service provided by means of that relevant system.

293 Identifying data is defined in section 263 as data which can identify, or assist in identifying, any person, apparatus, telecommunication system or telecommunications service, or which identifies an event, or may be used to identify the location of any person, event or thing.

294 Equipment data as defined in this section may be obtained under a targeted equipment interference warrant and, once the data is obtained, will be subject to the safeguards set out in Part 5.

295 Equipment data may also be obtained under a bulk equipment interference warrant. Secondary data comprising systems data and identifying data may be obtained pursuant to an interception warrant.

296 Equipment data could include:

a. messages sent between items of network infrastructure to enable the system to manage the flow of communications;

b. router configurations or firewall configurations;

c. software operating system (version);

d. the period of time a router has been active on a network;

e. the location of a meeting in a calendar appointment;

f. photograph information - such as the time/date and location it was taken; and

g. contact 'mailto' addresses within a webpage.

Section 101: Subject-matter of warrants

297 This section sets out the permitted subject matter of a warrant under this Part. A targeted equipment interference warrant may relate to:

a. a particular person, persons or group of persons who share a common purpose or who carry on, or may carry on, a particular activity (e.g. the computer equipment of Person X);

b. a particular organisation or organisations (e.g. the computer equipment of Organisation X);

c. a particular location or locations where the equipment being interfered with is present (e.g. computer equipment located at House X);

d. equipment which is being, or may be, used for the purposes of a particular activity or activities (e.g. equipment being used to disseminate terrorist publications); or

e. equipment that is being used for testing and development.

298 A targeted equipment interference warrant may 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'.

299 Subsection (2) relates to targeted examination warrants, providing that they may relate to: a person or organisation (or more than one person or organisation subject to the same investigation or operation); a group of persons with a common purpose or who carry on, or may carry on, a particular activity; the testing maintenance or development of capabilities; or the training of persons who carry out, or are likely to carry out, the selection of material derived from bulk equipment interference.

Section 102: Power to issue warrants to intelligence services: the Secretary of State

300 This section sets out the circumstances in which the Secretary of State has the power to issue a warrant under Part 5 of the Bill, establishing the process and requirements for equipment interference warrants that are applied for, by or on behalf of and issued to a director of one of the intelligence services – i.e. MI5, SIS, and GCHQ.

301 Subsection (1)(a) sets out that equipment interference warrants issued to the intelligence services must be necessary for one of three statutory purposes, detailed in subsection (5). This means a warrant can only be issued if it is in the interests of national security, for the purpose 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).

302 Subsection (1) also requires that 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, if the Secretary of State considers that appropriate safeguards are in place and, unless considered urgent, the decision to issue the warrant has been approved by a Judicial Commissioner.

303 Subsections (2) and (4) makes clear that the Secretary of State may not issue a warrant under this section if it relates to serious crime activity in Scotland or the subject of the warrant is in, or believed to be in, Scotland. In such circumstances the warrant will be issued by the Scottish Ministers (see section 103).

304 Subsection (7) makes it clear that it is not sufficient to establish that a warrant is necessary on the grounds set out in subsection (5) only on the basis that the information that would be obtained relates to trade union activity in the British Islands.

Section 103: Power to issue warrants to intelligence services: the Scottish Ministers

305 This section provides that the Scottish Ministers may issue a warrant under this Part where they consider that the warrant is necessary for the prevention or detection of serious crime, and proportionate to what is sought to be achieved. Unless it is considered urgent, the decision of the Scottish Ministers to issue the warrant must be approved by a Judicial Commissioner before the warrant can be issued.

306 The Scottish Ministers may only consider applications for targeted equipment interference

warrants made by or on behalf of the head of an intelligence service, which relate only to equipment in or believed to be in Scotland. The Scottish Ministers may only consider applications for targeted examination warrants, which relate only to the protected material of a person in, or reasonably believed to be in, Scotland.

307 A warrant cannot be considered necessary only on the basis that the information that would be obtained relates to trade union activity in the British Islands.

Section 104: Power to issue warrants to the Chief of Defence Intelligence

308 This section sets out the circumstances in which the Secretary of State can issue a targeted equipment interference warrant to the Chief of Defence Intelligence. Such warrants work in the same way as warrants issued to the intelligence services by the Secretary of State, with approval dependent upon consideration of necessity and proportionality. Warrants issued to the Chief of Defence Intelligence can only be issued if it is necessary in the interests of national security. Unless it is considered urgent, the decision to issue the warrant must be approved by a Judicial Commissioner.

309 Subsection (2) makes it clear that it is not sufficient to establish that a warrant is necessary only on the basis that the information that would be obtained relates to trade union activity in the British Islands.

Section 105: Decision to issue warrants under sections 102 to 104 be taken personally by Ministers

310 Subsection (1) requires the decision to issue a warrant under sections 102, 103 or 104 to be taken personally by the Secretary of State or a member of the Scottish Government. Subsection (3) requires the warrant to be signed by the person who has taken the decision to issue the warrant. Where that is not reasonably practicable, the warrant may be signed by a senior official designated by a Secretary of State or member of the Scottish Government but the Secretary of State or member of the Scottish Government must personally and expressly authorise the issuing of the warrant. Wherever the Act refers to "a member of the Scottish Government" this is a reference to one of the Scottish Ministers. It does not refer to an official or any other person.

Section 106: Power to issue warrants to law enforcement officers

311 This section sets out the circumstances in which a law enforcement chief can issue a targeted equipment interference warrant to an appropriate law enforcement officer, establishing the process and requirements.

312 Subsection (1) sets out the conditions that must be met for a law enforcement chief to issue a targeted equipment interference warrant, where they consider that the warrant is necessary for the purpose of preventing or detecting serious crime and that the conduct authorised is proportionate. Unless considered urgent, a decision to issue a warrant must be approved by a Judicial Commissioner before the warrant is issued. A law enforcement chief must also be satisfied that appropriate safeguards are in place (as detailed in sections 129 and 130).

313 Subsection (2) makes it clear that it is not sufficient to establish that a warrant is necessary, only on the basis that the information that would be obtained relates to trade union in the British Islands.

314 Subsection (3) sets out the conditions that must be met for the law enforcement chiefs, specified at Part 1 of the table at Schedule 6, to issue a targeted equipment interference warrant for purposes other than serious crime. Warrants under this subsection must be considered necessary for the purpose of preventing death or any injury or damage to a person's physical or mental health, or of mitigating any injury or damage to a person's

physical or mental health. The conduct must be considered proportionate to what is sought be gained and, unless considered urgent, the decision to issue the warrant must be approved by a Judicial Commissioner before the warrant is issued. In practice, warrants issued under this section would permit the specified law enforcement agencies to use equipment interference to locate and ensure the safety of vulnerable people, such as missing children.

315 Subsection (4) permits 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 only be delegated in an urgent case where it is not reasonably practical for a law enforcement chief to consider the application and issue the warrant. Schedule 6 sets out the appropriate delegates in each law enforcement agency that can issue an equipment interference warrant in these circumstances.

316 Subsections (6) to (13) set out variations or restrictions on the permitted purposes of targeted equipment interference warrants that may be issued by specified law enforcement chiefs. These variations and restrictions ensure that equipment interference can only be used in appropriate circumstances in relation to the purpose of each agency. For example, immigration officers may only be issued with an equipment interference warrant if the respective law enforcement chief considers that the warrant is necessary for the prevention or detection of serious crime which are related to an immigration or nationality offence (all the other requirements of subsection (1) must still be met).

Schedule 6: Issue of warrants under section 106 etc: table

317 This table sets out the law enforcement chiefs (and their delegates in urgent cases) who may issue targeted equipment interference warrants, and the appropriate law enforcement officer who may apply for such warrants.

318 Paragraph 1 defines collaborative force and collaborative agreement in relation to a police force for the purpose of understanding the first three entries in the table.

319 Paragraph 2 of the Schedule defines collaborative police force in relation to the NCA and provides that equipment interference can be carried out by police forces and the NCA who enter into collaboration agreements, enabling applications from police officers to the NCA and from NCA officers to Chief Constables.

Section 107: Restriction on issue of warrants to certain law enforcement officers

320 This section establishes the jurisdiction of equipment interference warrants for law enforcement agencies. A number of agencies may not be issued with a targeted equipment interference warrant if there is not a connection to the British Islands.

321 Subsection (2) lists the law enforcement chiefs that may only issue a targeted equipment interference warrant where they consider there is a connection to the British Islands. Subsection (3) also extends this restriction to collaborative forces led by the National Crime Agency.

322 Subsection (4) defines a British Islands connection, establishing that there will be such a connection in circumstances where:

a. any of the proposed conduct would take place in the British Islands (regardless of where the equipment to be interfered with is located);

b. it is believed that the equipment to be interfered with is or may be located in the British Islands at some point during the interference taking place. For example, a computer could 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 communications sent to or from a person believed to be in the British Islands and any associated equipment data or information relating to an individual whom is believed to be in the British Islands.

323 Subsection (5) provides that the law enforcement chiefs listed in Schedule 6 but not specified at subsection (2), are not subject to this restriction and are able to issue equipment interference warrants under section 106 whether or not there is a connection to the British Islands.

Section 108: Approval of warrants by Judicial Commissioners

324 This section sets out the test that the Judicial Commissioner must apply when considering whether to approve a decision to issue a warrant. He or she must review the conclusion the issuing authority came to regarding the necessity and proportionality of the warrant. In doing so the Judicial Commissioner must apply the same principles that a court would apply on an application for judicial review. The Judicial Commissioner must review the conclusion as to necessity and proportionality with sufficient care to comply with the general privacy duties set out in section 2.

325 Subsection (4) makes clear that where a Commissioner refuses to approve a warrant he or she must set out written reasons for the 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.

326 Subsection (5) sets out that a person seeking to issue a warrant under this Part 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 right of appeal and the warrant cannot be issued.

Section 109: Approval of warrants issued in urgent cases

327 This section sets out the process for issuing an equipment interference warrant in urgent cases. If the person issuing the warrant deems the warrant to be urgent then it can be issued without the approval of a Judicial Commissioner. Subsection (2) requires a Judicial Commissioner must be notified that the urgent warrant has been issued. Subsection (3) provides that the Commissioner must decide whether to approve the decision to issue the warrant within three working days.

328 If the Judicial Commissioner refuses to approve the urgent warrant within the three day period then subsection (4) provides that the warrant ceases to have effect and may not be renewed. The Investigatory Powers Commissioner cannot be asked to reconsider a Judicial Commissioner's decision to refuse an urgent warrant.

Section 110: Failure to approve warrant issued in urgent case

329 If a Judicial Commissioner refuses to approve the decision to issue a warrant, those exercising powers under the warrant must, as far and as quickly as they can, stop any activity being undertaken.

330 A Judicial Commissioner can determine what can happen to any material obtained under an urgent warrant that has not been approved. Subsection (5) provides for representations to be made to the Judicial Commissioner by the person who issued the urgent warrant or the authority who applied for it.

331 Subsection (3) provides that a Judicial Commissioner has the power to authorise additional equipment interference after refusing to approve a warrant, where such interference is necessary to ensure any ongoing interference ceases as soon as possible.

332 Subsections (7) and (8) provide for the person who issued an urgent warrant to ask the Investigatory Powers Commissioner to review a Judicial Commissioner's decision as to what can happen to any material obtained under an urgent warrant that the Commissioner refused to approve. The Investigatory Powers Commissioner can confirm the Judicial Commissioner's decision or make a fresh determination.

333 Subsection (9) provides that the urgent warrant being cancelled does not mean that anything already done under the warrant is unlawful, this is also the case for anything that it is not reasonably practicable to stop doing.

Section 111: Members of Parliament etc.

334 Subsections (1) to (3) of this section require the Secretary of State to obtain the approval of the Prime Minister (as well as a Judicial Commissioner) before issuing a targeted equipment interference or examination warrant where the purpose is to obtain the communications or private information of a person who is a Member of Parliament, a Member of the European Parliament representing the United Kingdom, or a member of one of the devolved legislatures.

335 Subsections (4) to (7) provide an equivalent requirement for warrants issued by law enforcement chiefs under section 106, who must obtain approval from both the Secretary of State and Prime Minister (as well as a Judicial Commissioner) before issuing a targeted equipment interference warrant in these circumstances. Subsection (5) provides that this requirement does not apply if the law enforcement chief believes that the only equipment to which the interference relates is located in Scotland.

Section 112: Items subject to legal privilege

336 This section sets out the safeguards which apply to targeted equipment interference or selection for examination of legally privileged material authorised under this Chapter. Further detail is provided in the Equipment Interference Code of Practice.

337 Where the purpose, or one of the purposes, of a warrant is to obtain items subject to legal privilege the warrant application must make that clear. The person issuing the warrant must consider the public interest in the confidentiality of items subject to privilege. That person must be satisfied that there are exceptional and compelling circumstances which make the acquisition or selection for examination of these items necessary, and that there are specific arrangements in place for how these items will be handled, retained, used and destroyed. Subsection (5) provides that a warrant for the purpose of protecting the interests of the economic well-being of the UK so far as those interests are also relevant to national security cannot be issued with the purpose of targeting legally privileged material. Subsection (6) provides further detail on what may constitute exceptional and compelling circumstances.

338 Where an agency applies for a targeted equipment interference warrant and believes that it is likely that they will obtain items subject to legal privilege, this must be made clear in the warrant application, including an assessment of the likelihood of obtaining such items. The person authorising the warrant may do so only if they are satisfied that there are specific arrangements in place for how such items would be handled, retained, used and destroyed. If the agency wishes to retain the items they have acquired, the Investigatory Powers Commissioner must be informed as soon as possible.

339 Subsections (11) to (13) set out the safeguards which apply when the purpose of a targeted equipment interference or examination warrant is to acquire or select for examination items that, if they were not made with the intention of furthering a criminal purpose, would be items subject to privilege. They provide that in those circumstances the warrant application must set out the reasons for believing the communications or items of information are likely to

be made, created or held with the intention of furthering a criminal purpose, and the person authorising the warrant may only do so if they consider that the communications or items of information are likely to be made, created or held with the intention of furthering a criminal purpose.

Section 113: Confidential Journalistic Material

340 This section sets out the additional safeguards which apply when the purpose, or one of the purposes of a targeted equipment interference or examination warrant is to authorise or require the interference with equipment for the purpose of obtaining communications or other items of information which the agency believes will contain confidential journalistic material, or selection for examination of such communications or other items of information. It provides that the warrant application must include a statement that the purpose or one of the purposes of the warrant is to identify or confirm a source of journalistic information. In addition, specific arrangements must be in place for the handling, retention, use and destruction of communications or other items of information containing confidential journalistic material. The definition of "journalistic material" and "confidential journalistic material" is provided in section 264.

Section 114: Sources of Journalistic Information

341 This section sets out the additional safeguards which apply when an agency applies for a targeted equipment interference warrant and the purpose, or one of the purposes of the warrant is to identify or confirm a journalist's source. It provides that the warrant application must make clear that this is the purpose or one of the purposes. In addition, specific arrangements must be in place for the handling, retention, use and destruction of material that identifies sources of journalistic information.

Section 115: Requirements which must be met by warrants

342 This section details the information that must be included in targeted equipment interference warrants and targeted examination warrants.

343 The table at subsection (3) sets out the matters to which a warrant can relate and the details that must be included in targeted equipment interference warrant. These requirements aim to ensure consistency in warrant applications, ensuring the information provided is comprehensive. Subsection (4) also requires that the warrant describes the type of equipment that is to be interfered with and the conduct (the equipment interference technique/s) that the warrant recipient is authorised to take.

344 A separate table is provided at subsection (5) which provides an equivalent to subsection (3) for targeted examination warrants. In contrast to targeted equipment interference warrants, examination warrants must describe the subject in terms of individuals rather than equipment.

345 The code of practice provides further detail, making clear that a warrant should be specific about the technique and the circumstances in which the warrant is to be used.

Section 116: Duration of warrants

346 This section deals with the duration of a Part 5 warrant. An equipment interference warrant will last for six months (unless it is cancelled earlier). If the warrant is not renewed it will cease to have effect after that period. Urgent warrants last for five working days, unless renewed.

Section 117: Renewal of warrants

347 Subsections (1), (2) and (3) provide that a warrant may be renewed by the Secretary of State,

member of the Scottish Government or law enforcement chief where relevant. In order to be renewed, a warrant must remain necessary and proportionate, applying the same tests as for issuing a warrant. As with an application for an equipment interference warrant, the decision to renew the warrant must also be approved by a Judicial Commissioner. The additional protections for Members of Parliament, etc. (see section 111), for legally privileged material (section 112) for confidential journalistic material (section 113), and for sources of journalistic information (section 114) apply when renewing warrants as they do when issuing warrants. A warrant may not be renewed more than 30 days in advance of the warrant ceasing to have effect.

Section 118: Modifications of warrants issued by the Secretary of State or Scottish Ministers

348 This section sets out the modifications which may be made to a targeted equipment interference or examination warrant, issued by the Secretary of State or the Scottish Ministers.

349 Subsection (2) details the only modifications that may be made to such a warrant. This includes adding or removing a matter to which the warrant relates, adding, varying or removing a name or description included in the warrant and adding, varying or removing a description of the types of equipment included in the warrant.

350 Subsection (3) provides that a warrant relating to the interference with equipment belonging to, used by or in the possession of a single person or organisation or in a single location, cannot be modified to add, vary or remove a person, organisation or location.

351 A decision to modify a warrant must be taken personally by the person making the modification, and the modification instrument must be signed by that person.

Section 119: Persons who may make modifications under section 118

352 This section sets out who is able to make modifications under section 118. The effect of this provision is that modifications may be made by the Secretary of State or Scottish Minister (where relevant) or a senior official acting on their behalf.

353 Subsection (2) provides that, in urgent cases, modifications may be made by a person to whom the warrant is addressed or a person holding a senior position in the same organisation.

354 However, what section 119 says is subject to special rules when the additional safeguards in sections 111 to 114 apply.

Section 120: Further provision about modifications under section 118

355 A modification which adds a name or description to a warrant, or which adds a factor to a warrant, can only be made if the modification is necessary and the conduct authorised by the modification is proportionate to what is sought to be achieved. This means that adding something to a warrant is subject to the same necessity and proportionality test as issuing a warrant. This section also sets out that the additional protections for Members of Parliament, etc. (section 111), items subject to legal privilege (section 112), items containing confidential journalistic material (section 113) and material that identifies a journalist's source (section 114) apply in relation to a decision to make a modification of a warrant as apply in relation to a decision to issue a warrant.

356 Subsection (4) makes clear that a modification which relates to a Member of Parliament or member of another relevant legislature can only be made by a Secretary of State and only has effect after the decision to make the modification has been approved by the Judicial Commissioner. Subsection (5) provides that a modification in relation to items subject to legal

privilege, items containing confidential journalistic material and material that identifies a journalist's source can only be made by a Secretary of State (or a member of the Scottish Government for warrants issued by the Scottish Minister) or in an urgent case, a senior official acting on their behalf, Such modifications must be approved by a Judicial Commissioner before they have effect, except where the person making the modification considers that there is an urgent need to make it. Subsections (7) and (8) provide for circumstances where the Secretary of State has taken a decision to modify a warrant but it is not reasonably practicable for them to sign the instrument. The rules in subsections (7) and (8) are the same as for issuing of warrants.

Section 121: Notification of modifications

357 This section provides that a Judicial Commissioner must be notified as soon as is reasonably practicable that a modification has been made and the reason for it. This notification requirement does not apply in circumstances where the Judicial Commissioner is required to approve the modification before it has effect, such as where it relates to Members of Parliament, items subject to legal privilege, items containing confidential journalistic material and material that identifies a journalist's source. It also does not apply to urgent modifications where a different procedure applies (see section 122).

358 Where a modification 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 informed.

Section 122: Approval of modifications under section 118 made in urgent cases

359 This section sets out the process for approving a modification to a warrant which has been made urgently. In most cases the fact that a modification was made urgently means that the modification could be made by a person holding a senior position in the equipment interference agency, rather than by a senior official acting on behalf of the Secretary of State or the Scottish ministers. The urgent modification must then be approved within three working days by a senior official designated by the Secretary of State or the Scottish Ministers.

360 Where the additional safeguards in sections 112 to 114 apply, the case being urgent means that the warrant may be modified without the prior approval of a Judicial Commissioner. The modification must then be approved within three working days by a Judicial Commissioner.

361 Where a designated senior official takes a decision, a Judicial Commissioner and either the Secretary of State or the Scottish Ministers must be informed. Where the decision on whether or not to approve the modification is taken by a Judicial Commissioner, the Secretary of State or a member of the Scottish Government will have to be informed courtesy of section 121, which is why that notification requirement is not dealt with in this section.

362 If the designated senior officer or the Judicial Commissioner refuses to approve the modification, the warrant (unless it no longer has effect) has effect as if the modification had not been made and 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 by virtue of that modification stops as soon as possible. The designated official or the Judicial Commissioner may then, if required, authorise further interference for the purpose of enabling the person to whom the warrant is addressed to secure that anything in the process of being done by virtue of the modification stops as soon as possible. In this case, subsection (9) ensures that the Secretary of State or member of the Scottish Government must be informed of the authorised interference.

Section 123: Modification of warrants issued by law enforcement chiefs

363 This section sets out the modifications which may be made to a targeted equipment interference warrant, issued by a law enforcement chief or appropriate delegate.

364 Subsection (2) details the only modifications that may be made to such a warrant. This includes adding or removing a matter to which the warrant relates, adding, varying or removing a name or description included in the warrant and adding, varying or removing a description of the types of equipment included in the warrant.

365 Subsection (3) provides that a warrant relating to the interference with equipment belonging to, used by or in the possession of a single person or organisation or in a single location, cannot be modified to add, vary or remove a person, organisation or location.

366 The decision to make any modifications under this section must be made by the law enforcement chief or appropriate delegate that issued the warrant. Such modifications must be approved by a Judicial Commissioner before they have effect, except where the person making the modification considers that there is an urgent need to make it (see section 124).

367 This section also sets out that the additional protections provided for in sections 111 to 114 apply (additional protections for Members of Parliament etc., items subject to legal privilege, items containing confidential journalistic material and sources of journalistic information) in relation to any modification as they apply in relation to the issuing of a warrant, except where the modification is only removing any matter, name or description from the warrant.

Section 124: Approval of modifications under section 123 in urgent cases

368 This section provides that once an urgent modification has been made by a law enforcement chief or an appropriate delegate a Judicial Commissioner must be informed.

369 The Judicial Commissioner must decide whether to approve the modification and notify the person who made the modification of their decision within three working days. If the urgent modification is refused the modification will cease to have effect and 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 by virtue of that modification stops as soon as possible. The Judicial Commissioner may then, if required, authorise further interference for the purpose of enabling the person to whom the warrant is addressed to secure that anything in the process of being done by virtue of the modification stops as soon as possible.

Section 125: Cancellation of warrants

370 This section provides that a Secretary of State, a member of the Scottish Government, a senior official acting on their behalf or a law enforcement chief (or appropriate delegate) may cancel a warrant at any time. They must do so if the warrant if it is no longer necessary on any relevant grounds, or if the conduct authorised by the warrant is no longer proportionate to what is sought to be achieved.

Section 126: Implementation of warrants

371 This section provides that the person who has obtained the warrant (i.e. the head of the equipment interference agency) may require other persons to assist in giving effect to a targeted equipment interference warrant. Subsections (2), (3) and (5) 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 the warrant may be served by providing a copy of the warrant itself or one or more of the schedules contained in the warrant. Subsection (4) sets out that the provision of assistance includes the disclosure of anything obtained under the warrant.

Section 127: Service of warrants

372 This section sets out the process for serving a targeted equipment interference warrant under section 126(2). Subsection (2) provides that a warrant must be served in such a way as to bring its contents to the attention of the person who is to be required to give effect to it. Subsections (3) and (4) set out the ways a warrant may be served on a person outside the United Kingdom.

Section 128: Duty of telecommunications operators to assist with implementation

373 This section provides that a telecommunications operator served with a targeted equipment interference warrant is required to take steps to give effect to it.

374 This duty only applies in respect of an equipment interference warrant issued to agencies – which are also permitted to apply for a targeted interception warrant. In all cases the Secretary of State or the Scottish Ministers will approve the proposed steps which the telecommunication operator is required to take, even if the normal warrantry process would not require their involvement. This means that targeted equipment interference warrants issued to the law enforcement officers listed at subsection (3) will be reviewed by the Secretary of State or the Scottish Ministers before a requirement can be imposed on a telecommunications operator

375 This section does not require a relevant telecommunications operator to take any steps which are not reasonably practicable to take. If the relevant telecommunications operator has previously been served with a notice to maintain a permanent technical capability then the steps required to comply with the notice should be considered when determining if the steps required by the warrant are reasonably practicable.

376 Subsection (7) provides that the duty to comply with a warrant is enforceable by civil proceedings brought by the Secretary of State against a person within the United Kingdom.

Section 129: Safeguards relating to retention and disclosure of material

377 This section sets out that the issuing authority must ensure that arrangements are in force for securing that certain requirements are met relating to retention and disclosure of material obtained under the warrant. The number of persons who see the material, the extent of disclosure and the number of copies made of any material must be kept to the minimum necessary for the authorised purposes. Subsection (3) sets out the circumstances in which something is necessary for the authorised purposes, for example where it is necessary for the functions of the Secretary of State or a Judicial Commissioner under the Act.

378 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. Subsection (8) requires that the Investigatory Powers Commissioner must be informed where confidential journalistic material or material which identifies a source of journalistic material is retained for purposes other than destruction.

379 The requirements in this section do not apply to material, or copies of material, handed over to an overseas authority. Section 130 applies instead.

Section 130: Safeguards relating to disclosure of material overseas

380 This section sets out the safeguards which apply when disclosing material acquired by virtue of an equipment interference warrant to an overseas authority. It provides that the issuing authority (defined in section 129(11)) must be satisfied that safeguards equivalent to those required by section 129 are in place, to the extent that the issuing authority considers appropriate.

Section 131: Additional safeguards for items subject to legal privilege

381 This section sets out the safeguards which apply when an item subject to legal privilege is

retained for purposes other than its destruction. The Investigatory Powers Commissioner must be informed as soon as is reasonably practicable. The Commissioner has the power to order that the item subject to legal privilege is destroyed, or to impose conditions as to the use or retention of the material.

382 The Investigatory Powers Commissioner must consider that the public interest in retaining the items outweighs the public interest in the confidentiality of items subject to privilege, and that retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury. If that test is not met, the Commissioner must exercise the power to order destructions or impose conditions. Even if the test is met, the Investigatory Powers Commissioner may still impose any conditions the Commissioner thinks necessary to protect the public interest in the confidentiality of items subject to privilege.

383 Subsections (4) and (5) provide that the Commissioner may require the person who issued the warrant and the person to whom the warrant is addressed to make representations to the Commissioner about the retention of items or the conditions that might be imposed and provides that the Commissioner must have regard to those representations, and any representation which those person choose to make, if not required to do so.

Section 132: Duty not to make unauthorised disclosures

384 This section places a duty on those persons listed in subsection (3) not to disclose the existence or details of an equipment interference warrant, or the material obtained under such a warrant. Subsection (4) sets out the matters which, if disclosed, would constitute unauthorised disclosure.

Section 133: Section 132: meaning of "excepted disclosure"

385 This section provides that in certain situations the duty not to make an unauthorised disclosure in section 132 does not apply. Disclosures made in such circumstances are called "excepted disclosures". Excepted disclosures are grouped into 4 heads.

386 Head 1 includes disclosure authorised by the warrant. It also includes disclosure which is necessary for the purpose of providing assistance in giving effect to a warrant. Head 2 allows for disclosure made to or authorised by a Judicial Commissioner, or a disclosure to the Independent Police Complaints Commission or the Intelligence and Security Committee of Parliament. Head 3 allows for disclosure in contemplation of, or in connection with, legal proceedings except where such a disclosure is made with the intention of furthering a criminal purpose. Head 4 allows for the disclosure of statistical information by a telecommunications operator, subject to any requirements imposed by regulations made by the Secretary of State, and for the disclosure of information by any person about warrants in general. This does not provide for disclosure of any particular warrant issued under Part 5.

Section 134: Offence of making unauthorised disclosure

387 This section provides that it is an offence knowingly to disclose any matter in breach of the duty in section 132(1) and sets out the penalties for such disclosures.

Section 135: Part 5: Interpretation

388 This section provides definitions for certain terms used in this Part.

Part 6: Bulk warrants

Chapter 1: Bulk interception warrants

Section 136: Bulk interception warrants

389 This section describes a bulk interception warrant and sets out the two conditions that a warrant issued under this chapter must meet.

390 The main purpose for which a bulk interception warrant may be issued is limited to intercepting overseas-related communications or obtaining secondary data from such communications. This prevents a bulk interception warrant being issued for the primary purpose of obtaining communications between individuals in the British Islands.

391 Subsection (3) defines "overseas-related communications" as communications that are sent or received by individuals outside the British Islands.

392 A bulk interception warrant may authorise the interception of overseas-related communications, the obtaining of secondary data and the selection for examination of intercepted content or secondary data obtained under the warrant.

393 Subsection (5) sets out the additional conduct that a bulk interception warrant authorises, where it is necessary or unavoidable to do what is required by the warrant. For example, 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. It also permits an interception warrant to authorise activity for obtaining secondary data.

> Example:
> A bulk warrant is sought for the interception of communications. The primary objective of the warrant is to obtain the communications of individuals 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 individuals in the UK will also be intercepted. In order to select for examination the content of those communications, a targeted examination warrant must be sought. This will need to be issued by the Secretary of State and approved by a Judicial Commissioner.

Section 137: Obtaining secondary data

394 This section describes secondary data which can be obtained under a bulk interception warrant. Secondary data means systems data or identifying data associated with or attached to the communications being transmitted. In order to be secondary data, identifying data must be capable of being separated from the communication in such a way that, when separated, it would not reveal the meaning (if any) of the content of the communication.

395 Systems data is defined in section 263 as data which enables or otherwise facilitates, or identifies or describes anything connected with enabling or facilitating, the functioning of any postal service, telecommunications system or any telecommunications service provided by means of that system. Anything that is systems data is not content.

396 Identifying data is defined in section 263 as data which can identify, or assist in identifying, any person, apparatus, telecommunication system or telecommunications service, or which identifies an event, or may be used to identify the location of any person, event or thing.

397 Secondary data obtained under a bulk interception warrant will be subject to the relevant safeguards set out in Chapter 1 of Part 6.

398 Secondary data could include:

a. messages sent between items of network infrastructure to enable the system to manage the flow of communications;

b. router configurations or firewall configurations;

c. software operating system (including the version of that system);

d. the period of time a router has been active on a network;

e. the location of a meeting in a calendar appointment;

f. photograph information - such as the time/date and location it was taken; and

g. contact 'mailto' addresses within a webpage.

Section 138: Power to issue bulk interception warrants

399 This section sets out the power to issue bulk interception warrants. The Secretary of State may issue a bulk interception warrant only where it is necessary and proportionate, for one or more specified statutory purposes. Subsection (1) makes clear that the interests of national security must always be one of those purposes.

400 Subsection (1) also requires that the Secretary of State must consider that each of the operational purposes specified in the warrant is a purpose for which the examination of intercepted content or secondary data is or may be necessary. Operational purposes limit the purposes for which data collected under a warrant can be selected for examination and no official is permitted to select data for examination other than as permitted by these purposes. Section 142 sets out more detail about operational purposes.

401 This subsection makes clear that the operational purposes specified on a warrant must relate to one or more of the statutory grounds specified on the warrant. For example, if a bulk interception warrant is issued in the interests of national security and for the purpose of preventing and detecting serious crime, every operational purpose specified on that warrant must be necessary for one or both of these broader statutory grounds.

402 In addition, subsection (1) makes clear that the Secretary of State's decision to issue the warrant must be approved by a Judicial Commissioner.

403 An application for a bulk interception warrant may only be made by one of the three intelligence services.

Section 139: Additional requirements in respect of warrants affecting overseas operators

404 This section outlines the requirements relating to warrants where the Secretary of State believes that giving effect to the warrant, if issued, is likely to require the assistance of a telecommunications operator who is based outside the United Kingdom.

405 Subsection (2) requires that the Secretary of State must consult the relevant telecommunications operator before issuing the warrant.

406 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.

Section 140: Approval of warrants by Judicial Commissioners

407 This section sets out the test that a Judicial Commissioner must apply when considering

whether to approve a decision to issue a bulk interception warrant. He or she must review the conclusion the Secretary of State came to regarding the necessity and proportionality of the warrant. The Judicial Commissioner must also review the Secretary of State's conclusion as to the necessity of the operational purposes specified on the warrant, and any matters taken into account in relation to warrants affecting overseas operators.

408 In determining these matters, the Judicial Commissioner must apply the same principles that a court would apply on an application for judicial review. The Judicial Commissioner must review the Secretary of State's conclusions with sufficient care to comply with the general privacy duties set out in section 2.

409 Where a Judicial Commissioner refuses to approve a warrant, subsection (3) makes clear that the Commissioner must set out written reasons for the 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 Judicial Commissioner.

410 Subsection (4) makes clear that the Secretary of State 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 right of appeal and the warrant cannot be issued.

Section 141: Decisions to issue warrants to be taken personally by Secretary of State

411 Subsection (1) requires the decision to issue a warrant under Chapter 1 to be taken personally by the Secretary of State, and subsection (2) makes clear the warrant must be signed by the Secretary of State before it is issued.

Section 142: Requirements that must be met by warrants

412 This section sets out the information, which must be specified on a bulk interception warrant.

413 Subsection (3) requires that a warrant must set out the operational purposes for which any intercepted content or secondary data obtained under the warrant may be selected for examination.

414 Subsection (4) makes clear that any operational purpose specified on a bulk interception warrant must also be included on a separate, central list of all operational purposes to be maintained by the heads of the intelligence services. The maintenance of this list will assist the intelligence services in identifying new operational purposes that may need to be added to bulk warrants over time, such as where a new threat to national security has developed.

415 Subsection (5) makes clear that a bulk interception warrant may specify however many operational purposes for which it is considered the examination of content and secondary data obtained under the warrant will, or may, be necessary. This may include all of the operational purposes that are included on the central list maintained by the heads of the intelligence services. Given the global nature of internet communications and reflecting the fact that bulk interception is primarily an intelligence gathering tool, bulk interception warrants are likely to specify all operational purposes from the central list.

416 Subsections (6) to (10) set out the processes by which the central list of operational purposes will be regulated and overseen. The addition of any operational purpose to the central list must be approved by the Secretary of State. These subsections also make clear that it is not sufficient for an operational purpose to use the wording of one of the statutory purposes: the Secretary of State must be satisfied that the purpose includes more detail before it may be added to the list. This ensures that intercepted content or secondary data may only be selected for examination for specific reasons.

417 These subsections also specify that the central list of operational purposes must be shared with the Intelligence and Security Committee every three months and must also be reviewed at least annually by the Prime Minister.

Section 143: Duration of warrants

418 This section sets out that a bulk interception warrant (unless cancelled) lasts for six months from the date of issue or, in the case of a renewed warrant, from the day after it would otherwise have expired.

Section 144: Renewal of warrants

419 This section provides for the renewal of a bulk interception warrant. The decision to renew a bulk interception warrant must be taken personally by the Secretary of State.

420 Subsection (2) sets out the conditions that must be met for a warrant to be renewed. The Secretary of State must believe that the warrant continues to be necessary and proportionate in relation to relevant statutory purpose(s), and that the operational purposes specified on the warrant continue to be necessary. The decision to renew the warrant must also be approved by a Judicial Commissioner.

421 A warrant may not be renewed more than 30 days in advance of the warrant ceasing to have effect.

Section 145: Modification of warrants

422 This section sets out the modifications which may be made to a bulk interception warrant.

423 The only modifications that may be made are adding, varying or removing any operational purpose specified in the warrant, or providing that the warrant no longer provides for the interception of communications covered by the warrant or the obtaining of secondary data from those communications.

424 Subsections (4) and (5) require that any modification to add or vary an operational purpose (a major modification) must be made by the Secretary of State and, except in urgent cases, approved by a Judicial Commissioner.

425 Subsection (6) provides that a senior official, acting on behalf of the Secretary of State, may make a modification to remove an operational purpose or to cancel the interception of communications (a minor modification). Subsection (12) provides that where a warrant is modified to cancel the interception of communications it remains a bulk interception warrant. Where a minor modification is made by a senior official, the Secretary of State must be personally notified of the modification, as well as the reasons for making it.

426 Subsection (8) places an obligation on the Secretary of State, or senior official acting on their behalf, to remove an operational purpose where selection for examination of content or secondary data for that purpose is no longer necessary.

427 Subsection (10) provides that where there is a need to make a major modification, but it is not reasonably practicable for the Secretary of State to sign the instrument making the modification, it can be signed by a senior official acting on behalf of the Secretary of State, but the modification must be personally authorised by the Secretary of State. Such a modification is not an urgent modification and must still be approved by a Judicial Commissioner before taking effect.

Section 146: Approval of major modifications by Judicial Commissioners

428 This section sets out the test that a Judicial Commissioner must apply when considering whether to approve the making of a major modification to a bulk interception warrant.

429 The Judicial Commissioner must review the Secretary of State's decision as to whether making the modification is necessary. In doing so, the Judicial Commissioner must apply the same principles that a court would apply on an application for judicial review. The Judicial Commissioner must review the Secretary of State's conclusions with sufficient care to comply with the general privacy duties set out in section 2.

430 Where a Judicial Commissioner refuses to approve the making of a modification, subsection (3) requires that they must set out written reasons for their refusal to the Secretary of State.

431 Subsection (4) provides that the Secretary of State may ask the Investigatory Powers Commissioner to reconsider a decision to make a modification that a Judicial Commissioner has refused. Should the Investigatory Powers Commissioner also refuse the decision to make the modification there is no right of appeal and the modification cannot be made.

Section 147: Approval of major modifications made in urgent cases

432 This section sets out the process for the approval of a major modification to a bulk interception warrant, which has been made urgently by the Secretary of State without the approval of a Judicial Commissioner.

433 The Secretary of State must inform a Judicial Commissioner that the modification has been made.

434 The Judicial Commissioner has three working days from the date of the modification in which to decide whether to approve the decision to modify the warrant, and to notify the Secretary of State of that decision.

435 If the Judicial Commissioner refuses to approve the decision to make the modification, subsection (4) makes clear that the warrant has effect as if the modification had not been made, and anything done as a result of that modification must stop as soon as possible.

436 In an urgent case where a Judicial Commissioner refuses to approve the decision to make a major modification, the Secretary of State may not refer the case to the Investigatory Powers Commissioner for a review.

Section 148: Cancellation of warrants

437 This section sets out the circumstances under which a bulk interception warrant must be cancelled.

438 Where the Secretary of State or a senior official decides the warrant is no longer necessary or proportionate, or that the examination of intercepted content and secondary data collected is no longer necessary for any of the operational purposes specified on the warrant, he or she must cancel it. A warrant may be cancelled by the Secretary of State or a senior official at any time.

Section 149: Implementation of warrants

439 This section sets out the requirements for giving effect to a bulk interception warrant. These replicate the provisions relating to the implementation of a targeted interception warrant, in sections 41, 42 and 43.

Section 150: Safeguards relating to retention and disclosure of material

440 This section sets out the general safeguards which apply to bulk interception warrants. These replicate the general safeguards which apply to the handling of targeted interception warrants in section 53.

Section 151: Safeguards relating to disclosure of material overseas

441 This section sets out the safeguards relating to the disclosure overseas of material obtained under a bulk interception warrant. The Secretary of State must be satisfied that, to the extent appropriate, the overseas authority with whom material is being shared has in place safeguards in relation to retention, disclosure and examination that correspond to those in the Act.

Section 152: Safeguards relating to examination of material

442 This section sets out the safeguards relating to the examination of intercepted content and secondary data which has been acquired under a bulk interception warrant. Subsections (1) and (2) require that intercepted content and secondary data may only be selected for examination for the operational purposes specified in the warrant and that selection for examination must be necessary and proportionate in all the circumstances.

443 Subsection (4) places a prohibition on selecting intercepted content for examination if any criteria used for the selection of that content refer to an individual known to be currently in the British Islands. A targeted examination warrant under Part 2 of the Bill, issued by the Secretary of State and approved by a Judicial Commissioner, must be in place before any such examination can take place.

> ### 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 Judicial Commissioner.

444 Subsections (5) to (7) deal with cases in which there is a change of circumstances such that an individual believed to be outside the British Islands, whose communications' content is 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 working days. Subsection (8) provides that the senior official must inform the Secretary of State that the selection is being carried out. Any selection after five working days 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 of the content of his communications. This authorisation only lasts for five working days, after which the selection for examination must cease or a targeted examination warrant must be sought. This will need to be issued by the Secretary of State and the decision to issue the warrant approved by a Judicial Commissioner before any further selection is permitted.

Section 153: Additional safeguards for items subject to legal privilege

445 This section sets out the safeguards, which apply when the use of certain criteria to select intercepted content for examination is either intended or likely to result in the acquisition of items subject to legal privilege. In this case, the use of those criteria must be approved by a senior official acting on behalf of the Secretary of State. That senior official may only give their approval if they are satisfied that there are exceptional and compelling circumstances which make the use of the criteria necessary, if the intention is specifically to acquire items subject to legal privilege, or, where the acquisition of such items is likely, specific arrangements are in place for how these items will be handled, retained, used and destroyed.

446 This section also sets out safeguards which apply when an item subject to legal privilege is retained for purposes other than destruction, following its selection for examination. Subsection (9) requires that the Investigatory Powers Commissioner must be informed as soon as reasonably practicable in these circumstances.

447 Subsection (10) provides that the Commissioner may direct that the item is destroyed or impose conditions as to the use or disclosure of the item.

Section 154: Additional safeguard for confidential journalistic material

448 This section sets out an additional safeguard in circumstances where a communication containing confidential journalistic material has been intercepted under a bulk interception warrant and is retained for purposes other than destruction following its selection for examination. In such circumstances, the person to whom the warrant is addressed must inform the Investigatory Powers Commissioner as soon as reasonably practicable.

Section 155: Offence of breaching safeguards relating to examination of material under bulk interception warrants

449 Subsection (1) creates a criminal offence for the deliberate selection for examination of material collected under a bulk interception warrant, where a person knows or believes that selection is in breach of the examination safeguards at sections 152 and 153.

450 Subsection (2) sets out the penalties for a person found guilty of this offence.

451 Proceedings in relation to an offence under this section may only be instituted by or 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.

Section 156: Application of other restrictions in relation to warrants

452 This section sets out that the exclusion of matters from legal proceedings set out in section 56, and the exceptions set out in Schedule 3, also apply to bulk interception warrants. The duty not to make unauthorised disclosures in section 57, the exceptions in section 58 and the associated offence in section 59 also apply to bulk interception warrants.

Section 157: Chapter 1: interpretation

453 This section defines various terms relating to bulk interception warrants which are used in this chapter.

Chapter 2: Bulk acquisition warrants

Section 158: Power to issue bulk acquisition warrants

454 Subsection (1) sets out the power for the Secretary of State to issue a bulk acquisition warrant. A warrant may be issued only where it is necessary and proportionate for one or more specified statutory purposes. The interests of national security must always be one of those

purposes. The decision to issue the warrant must be approved by a Judicial Commissioner. A warrant may only be issued to the three intelligence agencies.

455 Subsection (1) also requires that the Secretary of State must consider that each of the operational purposes specified in the warrant is a purpose for which the examination of material obtained under the warrant is or may be necessary. Operational purposes limit the purposes for which data collected under a warrant can be selected for examination and no official is permitted to select data for examination other than as permitted by these purposes. Section 161 sets out more detail about operational purposes.

456 This subsection makes clear that the operational purposes specified on a warrant must relate to one or more of the statutory grounds specified on the warrant. For example, if a bulk acquisition warrant is issued in the interests of national security and for the purpose of preventing and detecting serious crime, every operational purpose specified on that warrant must be necessary for one or both of these broader statutory grounds.

457 Subsection (4) makes explicit that legitimate trade union activity would never be sufficient grounds, of itself, for a bulk acquisition warrant to be considered necessary.

458 Subsection (6) sets out that a bulk acquisition warrant may authorise one or more of: requiring a telecommunications operator to disclose specified communications data in its possession or to obtain and disclose communications data which is not in its possession; the selection for examination of the data obtained under the warrant; and the disclosure of data described in the warrant.

459 Subsection (7) provides that a bulk acquisition warrant also authorises conduct necessary to do what is required by the warrant.

460 Subsection (8) provides that a bulk acquisition warrant may be issued in a relation to data which will come into existence in the future.

Section 159: Approval of warrants by Judicial Commissioners

461 This section sets out the test that a Judicial Commissioner must apply when considering whether to approve a decision to issue a bulk acquisition warrant. He or she must review the conclusions the Secretary of State came to regarding the necessity and proportionality of the warrant. The Judicial Commissioner must also review the Secretary of State's conclusions as to the necessity of the operational purposes specified on the warrant.

462 In determining these matters the Judicial Commissioner must apply the same principles that a court would apply on an application for judicial review. The Judicial Commissioner must review the Secretary of State's conclusions with sufficient care to comply with the general privacy duties set out in section 2 of the Act.

463 Where a Judicial Commissioner refuses to approve a warrant, subsection (3) makes clear that the Commissioner must set out written reasons for the 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 Judicial Commissioner.

464 Subsection (4) makes clear that the Secretary of State 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 then there is no right of appeal and the warrant cannot be issued.

Section 160: Decisions to issue warrants to be taken personally by Secretary of State

465 Subsection (1) requires the decision to issue a warrant to be taken personally by the Secretary of State, and subsection (2) makes clear the warrant must be signed by the Secretary of State

before it is issued.

Section 161: Requirements that must be met by warrants

466 This section sets out the information which must be specified on a bulk acquisition warrant.

467 Subsection (3) requires that a warrant must set out the operational purposes for which any communications data obtained under the warrant may be selected for examination.

468 Subsection (4) makes clear that any operational purpose specified on a bulk acquisition warrant must also be included on a separate, central list of all operational purposes to be maintained by the heads of the intelligence services. The maintenance of this list will assist the intelligence services in identifying new operational purposes that may need to be added to bulk warrants over time, such as where a new threat to national security has developed.

469 Subsection (5) makes clear that a bulk acquisition warrant may specify however many operational purposes for which it is considered the examination of data obtained under the warrant will, or may, be necessary. This may include all of the operational purposes that are included on the central list maintained by the heads of the intelligence services. As a bulk acquisition warrant may lead to the collection of communications data that is relevant to a range of operational purposes, bulk acquisition warrants are likely to specify all operational purposes from the central list.

470 Subsections (6) to (10) set out the processes by which the central list of operational purposes will be regulated and overseen. The addition of any operational purpose to the central list must be approved by the Secretary of State. These subsections also make clear that it is not sufficient for an operational purpose to use the wording of one of the statutory purposes: the Secretary of State must be satisfied that the purpose includes more detail before it may be added to the list. This ensures that intercepted content or secondary data may only be selected for examination for specific reasons.

471 These subsections also specify that the central list of operational purposes must be shared with the Intelligence and Security Committee every three months and must also be reviewed at least annually by the Prime Minister.

Section 162: Duration of warrants

472 This section sets out that a bulk acquisition warrant (unless cancelled) lasts for six months from the date of issue or, in the case of a renewed warrant, from the day after it would otherwise have expired.

Section 163: Renewal of warrants

473 This section provides for the renewal of a bulk acquisition warrant. The decision to renew a bulk acquisition warrant must be taken personally by the Secretary of State.

474 Subsection (2) sets out the conditions that must be met for a warrant to be renewed. The Secretary of State must believe that the warrant continues to be necessary and proportionate in relation to relevant statutory purpose(s) and that the operational purposes specified on the warrant continue to be necessary. The decision to renew the warrant must also be approved by a Judicial Commissioner.

475 A warrant may not be renewed more than 30 days in advance of the warrant ceasing to have effect.

Section 164: Modification of warrants

476 This section sets out the modifications that may be made to a bulk acquisition warrant.

477 The only modifications that may be made are adding, varying or removing any operational purpose specified in the warrant or providing that the warrant no longer provides for the acquisition of data covered by the warrant.

478 Subsections (4) and (5) require that any modification to add or vary an operational purpose (a major modification) must be made by the Secretary of State and, except in urgent cases, approved by a Judicial Commissioner.

479 Subsection (6) provides that a senior official, acting on behalf of the Secretary of State, may make a modification to remove an operational purpose or to cancel the collection of data (a minor modification). Where a minor modification is made by a senior official, the Secretary of State must be personally notified of the modification, as well as the reasons for making it.

480 Subsection (8) places an obligation on the Secretary of State, or senior official acting on their behalf, to remove an operational purpose where selection for examination of data for that purpose is no longer necessary.

481 Subsection (10) provides that where there is a need to make a major modification, but it is not reasonably practicable for the Secretary of State to sign the instrument making the modification, it can be signed by a senior official acting on behalf of the Secretary of State, but the modification must be personally authorised by the Secretary of State. Such a modification is not an urgent modification and must still be approved by a Judicial Commissioner before taking effect.

Section 165: Approval of major modifications by Judicial Commissioners

482 This section sets out the test that a Judicial Commissioner must apply when considering whether to approve the making of a major modification to a bulk acquisition warrant.

483 The Judicial Commissioner must review the Secretary of State's decision as to whether making the modification is necessary. In doing so, the Judicial Commissioner must apply the same principles that a court would apply on an application for judicial review. The Judicial Commissioner must review the Secretary of State's conclusions with sufficient care to comply with the general privacy duties set out in section 2.

484 Where a Judicial Commissioner refuses to approve the making of a modification, subsection (3) requires that they must set out written reasons for their refusal to the Secretary of State.

485 Subsection (4) provides that the Secretary of State may ask the Investigatory Powers Commissioner to reconsider a decision to make a modification that a Judicial Commissioner has refused. Should the Investigatory Powers Commissioner also refuse the decision to make the modification there is no right of appeal and the modification cannot be made.

Section 166: Approval of major modifications made in urgent cases

486 This section sets out the process for the approval of a major modification to a bulk acquisition warrant, which has been made urgently by the Secretary of State without the approval of a Judicial Commissioner.

487 The Secretary of State must inform a Judicial Commissioner that the modification has been made.

488 The Judicial Commissioner has three working days from the date of the modification in which to decide whether to approve the decision to modify the warrant, and to notify the Secretary of State of that decision.

489 If the Judicial Commissioner refuses to approve the decision to make the modification, subsection (4) makes clear that the warrant has effect as if the modification had not been

made, and anything done as a result of that modification must stop as soon as possible.

490 In an urgent case where a Judicial Commissioner refuses to approve the decision to make a major modification, the Secretary of State may not refer the case to the Investigatory Powers Commissioner for a review.

Section 167: Cancellation of warrants

491 This section sets out the circumstances under which a bulk acquisition warrant must be cancelled.

492 Where the Secretary of State or a senior official decides the warrant is no longer necessary or proportionate, or that the examination of data collected under the warrant is no longer necessary for any of the operational purposes specified on the warrant, he or she must cancel the warrant.

493 The Secretary of State or a senior official may also cancel a warrant at any time.

Section 168: Implementation of warrants

494 This section sets out the requirements for giving effect to a bulk acquisition warrant, and provides that the person who has obtained the warrant (i.e. the head of the relevant intelligence agency) may require other persons to assist in giving effect to it.

495 Subsections (2), (3) and (5) make clear: that a copy of a warrant may be served on any person who the intelligence agency 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 the warrant may be served by providing a copy of the warrant itself or one or more of the schedules contained in the warrant. Subsection (4) sets out that the provision of assistance includes the disclosure of communications data obtained under the warrant.

Section 169: Service of warrants

496 This section sets out the process for serving a bulk acquisition warrant. Subsection (2) provides that a warrant must be served in such a way as to bring its contents to the attention of the person who it is considered will be able to give effect to it. Subsections (3) and (4) set out the ways a warrant may be served on a person outside the United Kingdom.

Section 170: Duty of operators to assist with implementation

497 This section requires a telecommunications operator to take whatever steps are necessary to give effect to a bulk acquisition warrant. Subsection (2) clarifies that this section applies whether or not the provider is in the UK. An operator is not required to take steps which are not reasonably practicable. Subsection (4) provides that, where a technical capability notice under Part 9 has been given to the operator, the requirements placed on the operator are relevant to the consideration of what is reasonable.

498 Subsection (5) provides that the duty is enforceable against a person in the UK by the Secretary of State by civil proceedings for an injunction, or for the specific performance of a statutory duty or for any other appropriate relief.

Section 171: Safeguards relating to the retention and disclosure of data

499 This section sets out the safeguards which apply to communications data acquired under a bulk acquisition warrant. Subsection (2) requires the Secretary of State to ensure arrangements are in place to limit the disclosure of data to the minimum necessary for the authorised purposes. Data must be held securely and destroyed when there are no longer grounds for retaining it. Subsection (9) provides that the Secretary of State must be satisfied that, to the extent possible, any overseas authority with whom data is shared has in place retention,

disclosure and examination safeguards that correspond with those in the Bill.

Section 172: Safeguards relating to examination of data

500 This section provides that data obtained under a warrant may only be selected for examination in accordance with the operational purposes specified in the warrant and only when that selection is necessary and proportionate.

Section 173: Offence of breaching safeguards relating to examination of data

501 Subsection (1) creates a criminal offence for the deliberate selection for examination of material collected under a bulk acquisition warrant, where the person knows or believes that selection is in breach of the examination safeguards in section 172.

502 Subsection (2) sets out the penalties for a person found guilty of this offence.

503 Proceedings in relation to an offence under this section may only be instituted by or 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.

Section 174: Offence of making unauthorised disclosure

504 This section makes it an offence for persons specified in subsection (1) to make a disclosure to another person of the existence or contents of a bulk acquisition warrant, without reasonable excuse. Subsection (2) provides that it is a reasonable excuse where the disclosure is authorised by the Secretary of State. Subsection (3) sets out the maximum penalties for the offence.

Section 175: Chapter 2: interpretation

505 This section defines the terms used in this Chapter.

Chapter 3: Bulk equipment interference warrants

Section 176: Bulk equipment interference warrants: general

506 This section describes a bulk equipment interference warrant and sets out the two conditions that a warrant issued under this chapter must meet.

507 The main purpose for which a bulk equipment interference warrant may be issued is limited to interference with equipment to obtain overseas-related communications, overseas-related information or overseas-related equipment data. This prevents a bulk equipment interference warrant being issued where the primary purpose is obtaining communications between individuals in the British Islands or the information of individuals in the British Islands.

508 Subsection (2) defines "overseas-related communications" and "overseas-related information". Subsection (3) sets out when equipment data is "overseas-related".

509 A bulk equipment interference warrant must authorise the obtaining of communications, equipment data and other information to which the warrant relates, and may also authorise the selection for examination of material obtained under the warrant. Subsection (5) sets out that a bulk equipment interference warrant also authorises additional conduct necessary to do what is required by the warrant.

510 Subsection (6) provides that a bulk equipment interference warrant may not permit the acquisition of communications (other than stored communications) in circumstances where an interception warrant is required.

> **Example:**
> A bulk equipment interference warrant is sought. The primary objective of the warrant is to obtain the communications and other information 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 and information, it is inevitable that some communications and information of persons in the UK will also be acquired. In order to examine the content of those communications or any private information a targeted examination warrant must be sought. This will need to be issued by the Secretary of State and approved by a Judicial Commissioner.

Section 177: Meaning of "equipment data"

511 This section describes equipment data which can be obtained under a bulk equipment interference warrant. Equipment data means systems data or identifying data. In order to be equipment data, identifying data must be capable of being separated from the communication or item of information in such a way that, when separated, it would not reveal the meaning (if any) of the content of the communication or the meaning (if any) of an item of information (disregarding any inferred meaning).

512 Systems data is defined in section 263 as data which enables or otherwise facilitates, or identifies or describes anything connected with enabling or facilitating, the functioning of any postal service, telecommunications system or any telecommunications service provided by means of the system or any other relevant system or service provided by means of that relevant system.

513 Identifying data is defined in section 263 as data which can identify, or assist in identifying, any person, apparatus, telecommunication system or telecommunications service, or which identifies an event, or may be used to identify the location of any person, event or thing.

514 Equipment data obtained under a bulk equipment interference warrant will be subject to the relevant safeguards set out in Chapter 3 of Part 6.

515 Equipment data may also be obtained under a targeted equipment interference warrant. Secondary data comprising systems data and identifying data may be obtained pursuant to an interception warrant.

516 Equipment data could include:

a. messages sent between items of network infrastructure to enable the system to manage the flow of communications;

b. router configurations or firewall configurations;

c. software operating system (version);

d. the period of time a router has been active on a network;

e. the location of a meeting in a calendar appointment;

f. photograph information - such as the time/date and location it was taken; and

g. contact 'mailto' addresses within a webpage.

Section 178: Power to issue bulk equipment interference warrants

517 This section sets out the power to issue bulk equipment interference warrants. The Secretary of State may issue a bulk equipment interference warrant only where it is necessary and proportionate for one or more specified statutory purposes. Subsection (1) makes clear that the interests of national security must always be one of those purposes. Except in urgent cases, the decision to issue a warrant must also be approved by a Judicial Commissioner.

518 Subsection (1) also requires that the Secretary of State must consider that each of the operational purposes specified in the warrant is a purpose for which the examination of intercepted content or secondary data is or may be necessary. Operational purposes limit the purposes for which data collected under a warrant can be selected for examination and no official is permitted to select data for examination other than as permitted by these purposes. Section 183 sets out more detail about operational purposes.

519 This subsection makes clear that the operational purposes specified on a warrant must relate to one or more of the statutory purposes specified on the warrant. For example, if a bulk equipment interference warrant is issued in the interests of national security and for the purpose of preventing and detecting serious crime, every operational purpose specified on that warrant must be necessary for one or both of these broader purposes.

520 In addition, subsection (1) makes clear that the Secretary of State's decision to issue the warrant must be approved by a Judicial Commissioner.

521 Subsection (4) makes clear that an application for a bulk equipment interference warrant may only be made by one of the three intelligence services.

Section 179: Approval of warrants by Judicial Commissioners

522 This section sets out the test that the Judicial Commissioner must apply when considering whether to approve a decision to issue a bulk equipment interference warrant. He or she must review the conclusion the Secretary of State came to regarding the necessity and proportionality of the warrant. The Judicial Commissioner must also review the Secretary of State's conclusions as to the necessity of the operational purposes specified on the warrant.

523 In determining these matters, the Judicial Commissioner must apply the same principles that a court would apply on an application for judicial review. The Judicial Commissioner must review the Secretary of State's conclusions with sufficient care to comply with the general privacy duties set out in section 2.

524 Where a Judicial Commissioner refuses to approve a warrant, subsection (3) makes clear that 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 Judicial Commissioner.

525 Subsection (4) makes clear that the Secretary of State 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 right of appeal and the warrant cannot be issued.

Section 180: Approval of warrants issued in urgent cases

526 This section sets out the process for issuing a bulk equipment interference warrant in urgent cases. If the Secretary of State deems the warrant to be urgent then it can be issued without the approval of a Judicial Commissioner. Subsection (2) requires a Judicial Commissioner must be notified that the urgent warrant has been issued. Subsection (3) provides that the Commissioner must decide whether to approve the decision to issue the warrant within three

working days.

527 If the Judicial Commissioner refuses to approve the urgent warrant within the three day period then subsection (4) provides that the warrant ceases to have effect and may not be renewed. The Investigatory Powers Commissioner cannot be asked to reconsider a Judicial Commissioner's decision to refuse an urgent warrant.

Section 181: Failure to approve warrant issued in urgent case

528 If a Judicial Commissioner refuses to approve the decision to issue a bulk equipment interference warrant in an urgent case, those exercising powers under the warrant must, as far and as quickly as they can, stop any activity being undertaken. A Judicial Commissioner can determine what can happen to any material obtained under an urgent warrant that he or she has declined to approve.

529 Subsection (3) explains that a Judicial Commissioner has the power to authorise additional equipment interference after refusing to approve a warrant, where such interference is necessary to ensure any ongoing or future interference ceases as soon as possible.

530 Subsection (5) provides for representations to be made to the Judicial Commissioner by the Secretary of State or the person to whom the warrant is addressed.

531 Subsections (6) and (7) provide for the Secretary of State who issued an urgent warrant to ask the Investigatory Powers Commissioner to review a decision of a Judicial Commissioner to direct that material is destroyed or restrictions are imposed upon its use. The Investigatory Powers Commissioner can confirm the Judicial Commissioner's decision or make a fresh determination.

532 Subsection (8) provides that any activity carried out before the Judicial Commissioner refused to authorise the warrant remains lawful, as is anything that it is not reasonably practicable to stop doing.

Section 182: Decisions to issue warrants to be taken personally by Secretary of State

533 Subsection (1) requires the decision to issue a bulk equipment interference warrant to be taken personally by the Secretary of State, and subsection (2) makes clear the warrant must be signed by the Secretary of State before it is issued. Where that is not reasonably practicable, the warrant may be signed by a senior official designated by the Secretary of State but the Secretary of State must personally and expressly authorise the issuing of the warrant.

Section 183: Requirements that must be met by warrants

534 This section sets out the information, which must be specified on a bulk equipment interference warrant.

535 Subsection (4) requires that a warrant must set out the operational purposes for which any material obtained under the warrant may be selected for examination.

536 Subsection (5) makes clear that any operational purpose specified on a bulk equipment interference warrant must also be included on a separate, central list of all operational purposes to be maintained by the heads of the intelligence services. The maintenance of this list will assist the intelligence services in identifying new operational purposes that may need to be added to bulk warrants over time, such as where a new threat to national security has developed.

537 Subsection (6) makes clear that a bulk equipment interference warrant may specify however many operational purposes for which it is considered the examination of content and secondary data obtained under the warrant will, or may, be necessary. This may include all of

the operational purposes that are included on the central list maintained by the heads of the intelligence services. Given the global nature of internet communications and reflecting the fact that bulk equipment interference is primarily an intelligence gathering tool, bulk equipment interference warrants are likely to specify all operational purposes from the central list.

538 Subsections (7) to (11) set out the processes by which the central list of operational purposes will be regulated and overseen. These subsections make clear that the addition of any operational purpose to the central list must be approved by the Secretary of State. They also make clear that it is not sufficient for an operational purpose to use the wording of one of the statutory purposes: the Secretary of State must be satisfied that the purpose includes more detail before it may be added to the list. This ensures that material may only be selected for examination for specific reasons.

539 These subsections also specify that the central list of operational purposes must be shared with the Intelligence and Security Committee every three months and must also be reviewed at least annually by the Prime Minister.

Section 184: Duration of warrants

540 This section sets out that a bulk equipment interference warrant lasts for six months (unless cancelled) from the date of issue or, in the case of a renewed warrant, from the day after it would otherwise have expired. An exception applies for warrants issued in an urgent case, which last for five working days, unless renewed.

Section 185: Renewal of warrants

541 This section provides for the renewal of a bulk equipment interference warrant. The decision to renew a bulk equipment interference warrant must be taken personally by the Secretary of State.

542 Subsection (2) sets out the conditions that must be met for a warrant to be renewed. The Secretary of State must believe that the warrant continues to be necessary and proportionate in relation to relevant statutory purpose(s) and that the operational purposes specified on the warrant continue to be necessary. The decision to renew the warrant must also be approved by a Judicial Commissioner.

543 A warrant may not be renewed more than 30 days in advance of the warrant ceasing to have effect.

Section 186: Modification of warrants

544 This section sets out the modifications which may be made to a bulk equipment interference warrant. There are two types of modification that may be made to a bulk equipment interference warrant: minor and major modifications.

545 A major modification is a modification to add or vary an operational purpose or a description of conduct, accordingly, any element of the warrant may be modified. Major modifications follow the same authorisation process as a new warrant application, they must be made by the Secretary of State and, unless urgent, have effect only if the decision to make the modification is approved by a Judicial Commissioner. Where it is not reasonably practicable for an instrument making a major modification to be signed by the Secretary of State, the instrument making the modification can be signed by a senior official designated by the Secretary of State to do so. The modification must still be personally authorised by the Secretary of State. Such a modification is not an urgent modification and must still be approved by a Judicial Commissioner before taking effect.

546 A minor modification is one which removes an operational purpose or any description of conduct from a bulk equipment interference warrant. Minor modifications may be made by the Secretary of State or a senior official acting on their behalf and do not require approval from a Judicial Commissioner. If a minor modification is made by a senior official the Secretary of State must be personally notified of the modification and the reasons for making it.

547 Subsection (9) places an obligation on the Secretary of State, or senior official acting on their behalf, to remove an operational purpose where it is no longer necessary.

548 Subsection (13) provides that elements of a bulk equipment interference warrant may be modified so as to effectively cancel the ability to continue to acquire material under the warrant, whilst maintaining the ability to examine material already acquired under the warrant.

Section 187: Approval of major modifications by Judicial Commissioners

549 This section sets out the test that a Judicial Commissioner must apply when deciding whether to approve the making of a major modification to a bulk equipment interference warrant.

550 The Judicial Commissioner must review the Secretary of State's decision as to whether making the modification is necessary and, in the case of modifications adding or varying conduct, proportionate. In doing so, the Judicial Commissioner must apply the same principles that a court would apply on an application for judicial review. The Judicial Commissioner must review the Secretary of State's conclusions with sufficient care to comply with the general privacy duties set out in section 2.

551 Where a Judicial Commissioner refuses to approve the making of a modification, subsection (3) makes clear that they must set out written reasons for their refusal to the Secretary of State.

552 Subsection (4) provides that the Secretary of State may ask the Investigatory Powers Commissioner to reconsider a decision to make a modification that a Judicial Commissioner has refused. Should the Investigatory Powers Commissioner also refuse the decision to make the modification there is no right of appeal and the modification cannot be made.

Section 188: Approval of major modifications made in urgent cases

553 This section sets out the process for the approval of a major modification to a bulk equipment interference warrant, which has been made urgently by the Secretary of State without the approval of the Judicial Commissioner.

554 The Secretary of State must inform a Judicial Commissioner that the modification has been made.

555 The Judicial Commissioner has three working days from the date of the modification in which to decide whether to approve the decision to modify the warrant, and to notify the Secretary of State of that decision.

556 If the Judicial Commissioner refuses to approve the decision to make the modification, subsection (4) makes clear that the warrant has effect as if the modification had not been made, and anything done as a result of that modification must stop as soon as possible. If the Commissioner refuses to approve the modification, the activity authorised by that modification must cease as far as reasonably practicable. Subsection (5) explains that a Judicial Commissioner has the power to authorise additional equipment interference after refusing to approve the decision to issue an urgent warrant, where such interference is necessary to ensure any ongoing or future interference ceases as soon as possible.

557 In an urgent case where a Judicial Commissioner refuses to approve the decision to make a

major modification, the Secretary of State may not refer the case to the Investigatory Powers Commissioner for a review.

558 Subsection (6) clarifies that if the decision to make an urgent modification is not approved, the actions carried out whilst the warrant was active by virtue of the modification are not made invalid or unlawful by the ceasing of the warrant.

Section 189: Cancellation of warrants

559 This section sets out the circumstances under which a bulk equipment interference warrant may be cancelled.

560 Where the Secretary of State or a senior official decides the warrant is no longer necessary or proportionate, or that the examination of material is no longer necessary for any of the operational purposes specified on the warrant, he or she must cancel it. A warrant may be cancelled by the Secretary of State or a senior official at any time.

Section 190: Implementation of warrants

561 This section sets out the requirements for giving effect to a bulk equipment interference warrant. These replicate the provisions relating to the implementation of a targeted equipment interference warrant, in sections 126, 127 and 128.

Section 191: Safeguards relating to retention and disclosure of material

562 This section sets out the general safeguards which apply to bulk equipment interference warrants. These replicate the general safeguards which apply to the handling of targeted equipment interference warrants in section 129.

Section 192: Safeguards relating to disclosure of material overseas

563 This section sets out the safeguards relating to the disclosure overseas of material obtained under a bulk equipment interference warrant. The Secretary of State must be satisfied that, to the extent appropriate, the overseas authority with whom material is being shared has in place safeguards in relation to retention, disclosure and examination that correspond to those in the Act.

Section 193: Safeguards relating to examination of material etc.

564 This section sets out the safeguards relating to the examination material which has been acquired under a bulk equipment interference warrant. Subsections (1) and (2) require that material may only be selected for examination for the operational purposes specified in the warrant and that selection for examination must be necessary and proportionate in all the circumstances.

565 Subsection (4) places a prohibition on selecting protected 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. A targeted examination warrant under Part 5 of the Act, issued by the Secretary of State and approved by a Judicial Commissioner, must be in place before any such examination can take place.

> ### Example:
> A member of an intelligence service is investigating an international terrorist group and one member 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 she 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 Judicial Commissioner.

566 Subsections (5) to (7) deal with cases in which there is a change of circumstances such that an individual believed to be outside the British Islands, whose protected material is 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 working days. Subsection (8) provides that the senior official must inform the Secretary of State that the selection is being carried out. Any selection after five working days 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 of protected material. This authorisation only lasts for five working days, after which the selection for examination must cease or a targeted examination warrant must be sought. This will need to be issued by the Secretary of State and the decision to issue the warrant approved by a Judicial Commissioner before any further selection is permitted.

Section 194: Additional safeguards for items subject to legal privilege

567 This section sets out the safeguards, which apply when the use of certain criteria to select material for examination is either intended or likely to result in the acquisition of items subject to legal privilege. In this case, the use of those criteria must be approved by a senior official acting on behalf of the Secretary of State. That senior official may only give their approval if they are satisfied that there are exceptional and compelling circumstances which make the use of the criteria necessary, if the intention is specifically to acquire items subject to legal privilege, or, where the acquisition of such items is likely, specific arrangements are in place for how these items will be handled, retained, used and destroyed.

568 This section also sets out safeguards, which apply when an item subject to legal privilege is retained for purposes other than destruction, following its selection for examination. Subsection (9) requires that the Investigatory Powers Commissioner must be informed as soon as reasonably practicable in these circumstances.

569 Subsection (10) provides that the Commissioner may direct that the item is destroyed or impose conditions as to the use or disclosure of the item.

Section 195: Additional safeguard for confidential journalistic material

570 This section sets out an additional safeguard in circumstances where confidential journalistic material has been acquired under a bulk equipment interference warrant and is retained following its selection for examination. In such circumstances, the person to whom the warrant is addressed must inform the Investigatory Powers Commissioner as soon as reasonably practicable.

Section 196: Offence of breaching safeguards relating to examination of material

571 Subsection (1) creates a criminal offence for the deliberate selection for examination of material collected under a bulk equipment interference warrant, where a person knows or believes that selection is in breach of the examination safeguards at sections 193 and 194.

572 Subsection (2) sets out the penalties for a person found guilty of this offence.

573 Proceedings in relation to an offence under this section may only be instituted by or 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.

Section 197: Application of other restrictions in relation to warrants

574 This section sets out that the duty not to make unauthorised disclosures in sections 132, the exceptions in section 133 and the associated offence in section 134, also apply to bulk interception warrants.

Section 198: Chapter 3: interpretation

575 This section defines various terms relating to bulk equipment interference warrants which are used in this chapter.

Part 7: Bulk personal dataset warrants

Section 199: Bulk personal datasets: interpretation

576 Subsection (1) sets out the circumstances in which, for the purposes of this Bill, an intelligence service retains a bulk personal dataset. An intelligence service is defined in the general definitions section of the Act to mean MI5, SIS or GCHQ. The safeguards set out in this Part must be followed if these circumstances are met. A bulk personal dataset is a set of information that includes personal data relating to a number of individuals, the majority of whom are not, and are unlikely to become, of interest to the service in the exercise of its functions.

577 Subsection (2) defines personal data. The definition is the same 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 ensures that, where the bulk personal datasets retained or retained and examined by an intelligence service include data relating to deceased persons, the same safeguards will apply to all the data contained in those datasets.

Section 200: Requirement for authorisation by warrant: general

578 This section specifies that an intelligence service may not exercise a power to retain or examine a bulk personal dataset without a warrant. Subsection (3) describes the two types of warrant provided for under this Part of the Act – a 'class BPD warrant' and a 'specific BPD warrant'.

Section 201: Exceptions to section 200(1) and (2)

579 This section explains when the general requirements listed in the previous section do not apply. Subsection (1) states that a warrant under this Part is not required if the bulk personal dataset has been obtained under another regime outlined in this Act – for example if it is obtained by interception, carried out under an interception warrant.

580 Subsection (2) clarifies that a bulk personal dataset can be retained or examined to enable the information contained in it to be destroyed. If a warrant is cancelled or a specific warrant is not approved, it will not always be possible for the intelligence service to delete the applicable dataset immediately from its systems. This provision allows the service to hold the dataset

while it is ensuring that the relevant data is entirely removed from its systems and ensure that it is legally compliant.

581 Subsection (3) explains that other exceptions to section 200(1) and (2) are contained in sections 210(8), 219(8) and 220(5).

Section 202: Restriction on use of class BPD warrants

582 This section explains when a class BPD warrant cannot be used. It explains that a class BPD warrant cannot be used if the bulk personal dataset that the intelligence service wishes to retain, or retain and examine, is a dataset that includes or consists of "protected data" or health records, or if a substantial proportion of the bulk personal dataset consists of sensitive personal data. This section also states that a class BPD warrant cannot be used if the nature of the dataset or the circumstances in which it was created raise novel or contentious issues which ought to be considered by the Secretary of State and Judicial Commissioner.

Section 203: Meaning of "protected data"

583 This section defines "protected data" as any data contained in a bulk personal dataset other than data which is one or more of the following: systems data (as defined in section 263(4)); data which is not private information (so in other words, private information is protected data); or identifying data which is capable of being logically separated from the dataset and, if it were so separated, would not reveal anything which could reasonably be considered the meaning of the rest of the data which would remain in the dataset.

584 Systems data is essentially data that enables or facilitates the functioning of any system or service. Identifying data may help to identify persons, systems, services, locations or events. If the data cannot be classified either as systems data or identifying data, then it will fall within the definition of protected data so long as it is private information. The term private information includes information relating to a person's private or family life. Data which may not fall within the definition of private information could include that which is publicly available, such as information from books, newspapers, TV and radio broadcasts or data that is freely available on-line. Protected data in a bulk personal dataset may therefore include, for example, the contents of letters, e-mails or other documents.

Section 204: Class BPD warrants

585 This section explains how the class BPD warrant authorisation process works. A class BPD warrant will authorise the retention and examination of datasets that can be said to fall into a class because they are of a similar type and raise similar considerations (for instance in relation to the degree of intrusion and sensitivity, and the proportionality of using the data). This would, for example, allow the Secretary of State to authorise a class of dataset relating to travel where these conditions were met.

586 Subsection (2) specifies what an application for a class BPD warrant must include – a description of the class of bulk personal datasets and the operational purposes for which it is proposed to examine datasets of that class.

587 Subsection (3) explains that a Secretary of State can issue a class BPD warrant (thus enabling the retention and examination of datasets of that class) if he or she believes that the warrant is necessary (for the standard reasons of national security etc.) and proportionate, and that satisfactory handling measures (protective security measures, for example) are in place. The Secretary of State must also consider that each operational purpose specified in the warrant is one for which the examination of bulk personal datasets to which the application relates is or may be necessary, and that the examination of those datasets for such an operational purpose is necessary for the statutory purposes set out in subsection (3)(a). In addition, a Judicial

Commissioner must have approved the Secretary of State's decision to issue a warrant before the warrant can be issued.

588 Subsection (4) makes clear that the fact that the information that would be retained or retained and examined under the warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on the grounds on which warrants may be issued by the Secretary of State.

Section 205: Specific BPD warrants

589 This section explains how the specific BPD warrant authorisation process works. The Act provides for two cases in which an intelligence service may seek a specific BPD warrant. These are set out in subsections (2) and (3). A specific BPD warrant would cover a specific dataset rather than a class of datasets.

590 Subsection (2) describes the first case where a specific BPD warrant may be applied for. This is where the dataset does not fall within a class described by an existing class BPD warrant. An example of this could be if it is a new or novel type of dataset.

591 Subsection (3) describes the second case where a specific BPD warrant may be applied for. This is when a dataset falls within a class BPD warrant, but either section 202 prevents the intelligence service from relying on a BPD class warrant or, for any reason, the service believes that it would be appropriate to seek a specific BPD warrant.

592 The information that must be included in the application is set out in subsection (4) – a description of the specific dataset and the operational purposes for which the dataset is to be examined. Where a specific BPD warrant is sought because the section 202 restrictions on the use of class BPD warrants apply, then the application must include an explanation of why that section applies.

593 Subsection (6) describes the conditions which must be met before a specific BPD warrant can be issued by the Secretary of State. They are the same as for a class BPD warrant: the Secretary of State can issue a specific warrant if he or she believes that it is necessary for specified purposes and proportionate, and that adequate handling arrangements (protective security measures, for example) are in place. The Secretary of State must also consider that each operational purpose specified in the warrant is one for which the examination of the bulk personal dataset to which the application relates is or may be necessary, and that the examination of the dataset for such an operational purpose is necessary for the statutory purposes set out in subsection (5)(a). In addition, except in urgent cases (on which see section 209), a Judicial Commissioner must have approved the Secretary of State's decision to issue a warrant before the warrant can be issued.

594 Subsection (7) makes clear that the fact that the information that would be retained or retained and examined under the warrant relates to the activities in the British Islands of a trade union is not, of itself, sufficient to establish that the warrant is necessary on the grounds on which warrants may be issued by the Secretary of State.

595 Subsection (8) provides that a warrant can authorise the use of a replacement dataset. This is intended to allow updated versions of the authorised dataset to be retained and used without the need for a separate warrant. For example, a dataset may be updated on a weekly or monthly basis, and in those circumstances the necessity and proportionality case and operational purposes for which the dataset may be examined may be unchanged. Subsection (8) allows the agencies to retain and examine this updated data under the existing authorisation and without the need for a new specific BPD warrant.

Section 206: Additional safeguards for health records

596 This section explains the process that must be followed if an intelligence service wishes to apply for a specific BPD warrant relating to health records. Subsections (1) to (3) provide that if an intelligence service applies for such a specific BPD warrant, and the purpose or one of the purposes is to authorise the retention and examination of health records, the application must contain a statement to this effect. They also provide that the warrant can only be issued if the Secretary of State considers that there are exceptional and compelling circumstances that mean it is necessary to authorise the warrant. Subsections (4) and (5) apply when a bulk personal dataset includes or is likely to include health records, but the purpose of the warrant is not to retain or retain and examine such records. In such circumstances, the application must include a statement that the dataset includes or is likely to include health records and in the latter case how likely this is. Subsections (6) and (7) define 'health record' in this context.

Section 207: Protected data: power to impose conditions

597 This section states that where the Secretary of State decides to issue a specific BPD warrant, the Secretary of State may impose conditions which must be satisfied before protected data retained in reliance on the warrant may be selected for examination on the basis of criteria which are referable to an individual known to be in the British Islands at the time of selection. If an intelligence service has a dataset which it knows to contain protected data, this allows the Secretary of State, if he or she is not satisfied that the selection for examination safeguards set out in section 221 would be sufficient on their own, to set conditions that must be met before any searches of that dataset take place for information relating to individuals who are known to be in the British Islands.

Section 208: Approval of warrants by Judicial Commissioners

598 This section explains the process by which the Judicial Commissioner will consider whether to approve the Secretary of State's decision to issue the class or specific BPD warrant. It is consistent with the role of Judicial Commissioners in the rest of the Act (e.g. in authorising interception warrants). Amongst other things, it specifies that in reviewing the Secretary of State's conclusions, a Judicial Commissioner must apply judicial review principles, and must consider the Secretary of State's conclusions with sufficient care to ensure that the Commissioner complies with the requirements of section 2 of the Act (general duties in relation to privacy).

Section 209: Approval of specific BPD warrants issued in urgent cases

599 This section applies to specific BPD warrants only. If the Secretary of State considers that there is an urgent need to issue it, a specific BPD warrant may be issued without the approval of the Judicial Commissioner. If this happens, a Judicial Commissioner must be informed that an urgent warrant has been issued and, within three working days, decide whether to approve the issue of that warrant and notify the Secretary of State of the decision. This is the same approach as for urgent targeted interception warrants (for example). Subsection (4) explains that if the Judicial Commissioner refuses to approve the decision to issue the warrant, it ceases to have effect.

Section 210: Failure to approve specific BPD warrant issued in urgent case

600 This section explains the process if a Judicial Commissioner refuses to approve a specific BPD warrant that was issued under the urgency procedure above. Subsection (2) states that anything being done under that warrant should stop as soon as possible. Subsection (3) explains that if a Judicial Commissioner refuses to approve the warrant, he or she may determine what may be done with the material that was retained under that warrant. He or she may direct that the material is destroyed or impose conditions as to the use or retention of any of the material.

601 Subsections (4) and (5) explain that the Judicial 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.

602 Subsection (8) makes clear that an intelligence service is not in breach of the requirement for a warrant under subsections (1) and (2) of section 200 if it retains or examines a bulk personal dataset as a result of directions allowing this made by the Judicial Commissioner under subsection (3)(b). Subsection (9) makes it clear that nothing in this section or section 209 affects the lawfulness of 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.

Section 211: Decisions to issue warrants to be taken personally by Secretary of State

603 This section specifies that the decision to issue a class or specific BPD warrant must be taken personally by the Secretary of State and the warrant must be signed by the Secretary of State. In the case of specific warrants only, a designated senior official may sign the warrant if it is not reasonably practicable for the Secretary of State to sign it. In such a case, the warrant must contain a statement that it is not reasonably practicable for the warrant to be signed by the Secretary of State, and that the Secretary of State has personally and expressly authorised the issue of the warrant.

Section 212: Requirements that must be met by warrants

604 This section explains that a warrant under this Part must state that it is a class BPD warrant or a specific BPD warrant, be addressed to the intelligence service concerned, describe the class or specific dataset authorised and specify the operational purposes for which data contained in the bulk personal dataset or datasets can be selected for examination. This section makes clear that the operational purposes must be ones specified in a list maintained by the heads of the intelligence services. An operational purpose may only be specified on the list with the approval of the Secretary of State. Every three months, the list of operational purposes must be copied to the Intelligence and Security Committee of Parliament. The Prime Minister must review the list at least once a year. It is not sufficient for operational purposes to use the wording of one of the statutory purposes set out in subsection (3)(a) of section 204 or subsection (6)(a) of section 205: the Secretary of State must be satisfied that the purpose as specified includes a greater level of detail before it may be added to the list. This ensures that data may only be selected for examination for specific reasons.

Section 213: Duration of warrants

605 This section sets out that a specific or class BPD warrant (unless cancelled) lasts for six months from the date of issue or, in the case of a renewed warrant, from the day after it would otherwise have expired. An urgent warrant has effect for five working days after the day on which it was issued. These durations are consistent with other forms of warrants in the Act.

Section 214: Renewal of warrants

606 This section provides for the renewal of a class or specific BPD warrant. The decision to renew a warrant must be taken personally by the Secretary of State.

607 Subsection (2) sets out the conditions that must be met for a warrant to be renewed. The Secretary of State must believe that the warrant continues to be necessary and proportionate in relation to relevant statutory purpose(s), that the operational purposes specified on the warrant continue to be necessary, and that the examination of datasets for such an operational purpose is necessary for the statutory purposes. The decision to renew the warrant must also be approved by a Judicial Commissioner.

608 A non-urgent warrant may not be renewed more than 30 days in advance of the warrant ceasing to have effect. An urgent warrant may be renewed at any point before its expiry date.

Section 215: Modification of warrants

609 This section explains the process by which class or specific BPD warrants can be modified, what constitutes a major or minor modification to a warrant and who is authorised to make or approve those modifications. The only modification that can be made to any warrant is to add, vary or remove an operational purpose. A major modification adds or varies an operational purpose; a minor modification removes one. This section also provides for major modifications in urgent circumstances. These provisions are consistent with equivalent sections in Part 6 of the Act.

610 Subsection (11) provides that where it is not reasonably practicable for an instrument making a major modification to be signed by the Secretary of State, the instrument making the modification can be signed by a senior official designated by the Secretary of State to do so. But subsection (12) requires in such a case that the modification must be personally authorised by the Secretary of State. Such a modification is not an urgent modification and must still be approved by a Judicial Commissioner before taking effect.

Section 216: Approval of major modifications by Judicial Commissioners

611 This section sets out the test that a Judicial Commissioner must apply when deciding whether to approve the making of a major modification to a class or specific BPD warrant. It is consistent with the role of Judicial Commissioners in Part 6 of the Act (e.g. in authorising major modifications of bulk interception warrants).

Section 217: Approval of major modifications made in urgent cases

612 This section explains the approval process for urgent major modifications. If the Secretary of State believes that there is an urgent need to make a major modification to a warrant, this may be made without the approval of the Judicial Commissioner. If this happens, a Judicial Commissioner must be informed that the warrant has been modified and, within three working days, decide whether to approve the modification of that warrant and notify the Secretary of State of the decision. This is the same approach as for urgent modifications of targeted interception warrants, and is consistent with equivalent sections in Part 6 of the Act. Subsection (4) explains that if the Commissioner refuses to approve the decision to modify the warrant, the modification ceases to have effect.

Section 218: Cancellation of warrants

613 This section sets out that a Secretary of State or senior official designated by the Secretary of State can cancel a warrant at any time, and must do so if the warrant is no longer necessary or proportionate.

Section 219: Non-renewal or cancellation of BPD warrants

614 This section sets out the process if a class or specific BPD warrant is not renewed or is cancelled and in particular what must be done with the material that was retained under that warrant. The material may be destroyed – section 201(2) ensures retention or examination of the material for the purpose of destroying the material is lawful. But depending on the reasons why the warrant has been cancelled or not renewed, the relevant intelligence service may consider it necessary and proportionate to retain some or all of the material that had been retained under the authority of that warrant. Section 219 therefore includes bridging provisions to ensure any retention and examination of the material in question is lawful pending any authorisation via a new warrant. Subsection (2) specifies that, within five days of the cancellation or non-renewal, the intelligence service can either apply for a new specific or

class BPD warrant to cover the whole, or part, of the material covered under the previous warrant or, if further consideration is needed as to whether to apply for a new warrant, can apply to the Secretary of State for a bridging authorisation to retain or retain and examine all or part of this dataset while this is decided.

615 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 for up to three months. This may be the case if, for example, the Secretary of State no longer believes that an entire class of bulk personal dataset should be retained, but that it is necessary and proportionate to retain a subset or subsets of that material. Subsection (4) specifies that in deciding whether to approve the Secretary of State's decision, a Judicial Commissioner must apply judicial review principles, and must take sufficient care to ensure that the Commissioner complies with the requirements of section 2 of the Act (general duties in relation to privacy).

616 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 (5)). Subsection (6) 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.

617 Subsection (7) states that the intelligence service must apply for the fresh specific or class BPD warrant as soon as reasonably practicable and before the end of the period specified by the Secretary of State if it decides to apply for such a warrant. Subsection (8) sets out the time limits in relation to this section, and provides that if those time limits are adhered to then the retention and examination of the data throughout the process remains lawful.

Section 220: Initial examinations: time limits

618 This section explains the process of, and sets time limits for, the initial examination of a bulk personal dataset. Subsection (1) states that this section applies when an intelligence service obtains a bulk personal dataset, i.e. a set of information it believes includes or may include personal data relating to a number of individuals, the majority of whom are not, or unlikely to become of interest to the service in the exercise of its functions.

619 Subsection (2) outlines the steps that the intelligence service must take, and requires these steps to be taken with a set period. These steps are: an initial examination to determine whether it is a bulk personal dataset; reaching a decision whether to retain the dataset; and making an application for a specific BPD warrant (unless the dataset is authorised by a class BPD warrant).

620 Subsections (3) and (4) define the beginning and end of the set period during which the steps must be taken. The period begins when the intelligence service first forms the belief outlined in subsection (1). The period ends after three months where the set of information was created in the UK or after six months where the set of information was created outside the UK. Subsection (5) makes clear that it remains lawful for an intelligence service to retain a bulk personal dataset for the period between deciding to apply for a specific BPD warrant and the determination of that application, and that it is lawful for the intelligence service to examine the bulk personal dataset during that period if the examination is necessary for the purpose of applying for the warrant.

Section 221: Safeguards relating to the examination of bulk personal datasets

621 This section outlines safeguards relating to the examination of bulk personal datasets under a class or specific BPD warrant. It requires the Secretary of State to ensure that arrangements are

in force for securing that data can only be selected for examination from the bulk personal dataset for an operational purpose specified in the warrant, and the selection of that data must be necessary and proportionate. If a specific BPD warrant includes conditions relating to protected data, the Secretary of State must also ensure that arrangements are in force for securing that the selection for examination of data in relation to individuals known to be in the British Islands at the time of the selection are in accordance with those conditions.

Section 222: Additional safeguards for items subject to legal privilege: examination

622 This section outlines additional safeguards where protected data retained under a specific BPD warrant is to be selected for examination, and the purpose or one of the purposes of using the criteria used for selection ('the relevant criteria') is to identify items subject to legal privilege or the use of the relevant criteria is likely to identify such items. If the relevant criteria are referable to an individual known to be in the British Islands at the time of selection, the data may only be selected for examination if the Secretary of State has approved those criteria, with the approval of a Judicial Commissioner. Subsection (3) states that in any other case the approval for the criteria may come from a senior official acting on behalf of the Secretary of State.

623 Subsections (5) and (6) specify that approval may only be given if there are specific handling arrangements in place for items subject to legal privilege, there are exceptional and compelling circumstances making it necessary to authorise the use of the relevant criteria, and the approver has regard to the public interest in the confidentiality of items subject to legal privilege. Subsection (7) states that there cannot be exceptional and compelling circumstances unless the public interest in obtaining the information outweighs the public interest in the confidentiality of the items subject to legal privilege, there are no other means by which the information may reasonably be obtained, and obtaining the information is necessary in the interests of national security or for the purpose of preventing death or significant injury.

624 Subsection (8) explains the process by which a Judicial Commissioner will consider whether to approve the Secretary of State's decision to issue the warrant. It is consistent with the role of Judicial Commissioners in the rest of the Act. Subsections (9) to (13) outline the procedure if protected data is to be selected for examination for the purpose of identifying data that, if the data or any underlying material were not created or held with the intention of furthering a criminal purpose, would otherwise be subject to legal privilege.

Section 223: Additional safeguards for items subject to legal privilege: retention following examination

625 This section explains the process that must be followed if an item subject to legal privilege is to be retained following examination. If an item is to be retained for purposes other than destruction, the Investigatory Powers Commissioner must be informed as soon as is reasonably practicable. Unless (i) the public interest in retaining the item outweighs the public interest in the confidentiality of items subject to legal privilege and (ii) retaining the item is necessary in the interests of national security or for the purpose of preventing death or significant injury, the Commissioner must direct that the item is destroyed or impose conditions as to the use or retention of that item. Even if criteria (i) and (ii) are met, the Commissioner can impose conditions he or she thinks are necessary to protect the public interest in the confidentiality of items subject to legal privilege. The Commissioner may require representations from the Secretary of State or the person to whom the warrant is addressed about the exercise of the Commissioner's functions to direct the destruction of the item or impose conditions on its use or retention, and must have regard to any representations received.

Section 224: Offence of breaching safeguards relating to examination of material

626 This section creates a criminal offence of deliberately selecting for examination data retained in reliance on a class or specific BPD warrant where a person knows or believes that selection is in breach of: (i) the requirement that the selection is necessary for the operational purposes specified in the warrant in accordance with section 212; (ii) the requirement that the selection is necessary and proportionate; or (iii) in the case of protected data, any conditions imposed under section 207.

627 This section also sets out the penalties for a person found guilty of this offence, and makes clear that proceedings in relation to an offence under this section may only be instituted by or 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.

Section 225: Application of Part to bulk personal datasets obtained under this Act

628 This section relates to bulk personal datasets obtained by an intelligence service using a capability for which a warrant or other authorisation was issued or given under the Act, other than a bulk acquisition warrant under Part 6 of this Act. The general rule is that Part 7 of the Act does not apply to bulk personal datasets acquired pursuant to such a warrant or authorisation, as a result of the exception set out in section 201(1). Instead, any provisions from the regime governing the original acquisition ('the original acquisition regime') that are relevant to the bulk personal dataset will apply. However, under this section the intelligence service can apply to the Secretary of State for a direction which has the effect of applying the Part 7 regime to the bulk personal dataset, thereby displacing the exception in 201(1).

629 The direction will allow: the intelligence service to retain and examine the bulk personal dataset under the Part 7 regime; that any other power to do so ceases to apply; and that any associated regulatory provision (as defined in subsection (14)) arising by virtue of the original acquisition regime will cease to apply (subsection (3)). In most cases, the expectation is that the regulatory provisions applicable under the acquiring regime will be disapplied in full. However, subsection (5) specifies that if appropriate, the direction may provide for the continued application of specified associated regulatory provisions in their original or modified form. Subsection (6) makes clear that in the case of a bulk personal dataset obtained by interception which identifies itself as the product of interception, such a direction may not disapply the provisions in section 56 of and Schedule 3 to the Act, which prevent such material from being disclosed in legal proceedings or Inquiries Act proceedings. Subsection (6) also makes clear that a direction may not disapply sections 57 or 59 of the Act. These sections together mean that it is an offence to make unauthorised disclosure of the existence of an intercept warrant or any intercepted material. This ensures that the prohibition on disclosure of intercept material could never be disapplied by the Secretary of State.

630 Such a direction can only be given with the approval of a Judicial Commissioner (subsection (7)). The effect of such a direction will be that a Part 7 warrant is required to retain and examine the bulk personal dataset, and subsection (13) allows the intelligence service to apply for, and the Secretary of State to issue, a specific BPD warrant at the same time as the direction. A specific BPD warrant will be required where retention and examination is not authorised under a class BPD warrant.

631 A Judicial Commissioner must apply judicial review principles when deciding whether to approve a decision by the Secretary of State to give such a direction (subsection (8)). Where a Judicial Commissioner refuses to approve such a decision, he or she must give written reasons for this (subsection (9)). 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 (subsection

(10)). Subsection (7) states that a direction may be varied to allow the alteration or removal of any provisions included in the direction under subsection (5). Subsections (7) to (10) apply to such a variation.

Section 226: Part 7: interpretation

632 This section defines specific terms used in this Part.

Part 8: Oversight arrangements

Chapter 1: Investigatory Powers Commissioner and other Judicial Commissioners

Section 227: Investigatory Powers Commissioner and other Judicial Commissioners

633 This section establishes the office of the Investigatory Powers Commissioner, who is supported in carrying out functions by other Judicial Commissioners. No-one may be appointed as the IPC or as a Judicial Commissioner unless they have held a judicial position at least as senior as a high court judge. Appointments to these positions are made by the Prime Minister. The Prime Minister may only appoint someone to the post of IPC after receiving a joint recommendation from the Lord Chief Justice of England and Wales, the Lord President of Scotland, the Lord Chief Justice of Northern Ireland and the Lord Chancellor. In order for the Prime Minister to appoint someone to the position of Judicial Commissioner the Investigatory Powers Commissioner must also jointly recommend the candidate. The Prime Minister must then consult the Scottish Ministers before the appointment is made. When making appointments and consulting with the Scottish Ministers the prime Minister must have regard to a memorandum of understanding agreed with the Scottish Ministers.

634 To allow them to work effectively, the IPC may delegate functions to the other Judicial Commissioners. The IPC cannot delegate the duty to make a joint recommendation to the Prime Minister about the appointment of a Judicial Commissioner or the duty to appoint members to the TAP. That a function has been delegated does not prevent the IPC from exercising that function.

635 Subsection 11 provides that a function that may be exercised by a Judicial Commissioner may be exercised by any Judicial Commissioner. The reason for this provision can best be explained using the example of section 25. That section requires that a Judicial Commissioner be notified when an urgent warrant has been issued and that the Commissioner must then do certain things. This subsection means that where a particular Judicial Commissioner is informed that an urgent warrant has been issued, the resulting tasks can be performed by any of the Judicial Commissioners. This subsection is subject to the exception that certain functions can only be performed by the IPC or by a Judicial Commissioner to whom the IPC has chosen to delegate specific functions.

636 The IPC is a Judicial Commissioner, so where the Act or these Explanatory Notes refers to a Judicial Commissioner this includes the IPC.

Section 228: Terms and conditions of appointment

637 The Judicial Commissioners will be appointed for fixed terms of three years and can be re-appointed. Subsections (4) to (5) ensure the independence of the Judicial Commissioners by limiting the circumstances in which they can be removed from office. Judicial Commissioners 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.

Section 229: Main oversight functions

638 This section gives the IPC a broad remit to keep under review the use of investigatory powers. This section does not list each individual function that the Commissioner is to oversee. Instead it gives the Commissioner a wide remit to oversee the way public authorities intercept communications, acquire or retain communications data or carry out equipment interference. This section then lists additional matters not caught by that starting point, such as the acquisition, retention, use or disclosure of bulk personal data sets. The IPC will undertake, with the assistance of the Judicial Commissioners and staff, the functions currently undertaken by the Intelligence Services Commissioner, the Interception of Communications Commissioner and the Surveillance Commissioners. The IPC and other Judicial Commissioners will have discretion as to how they must fulfill their functions, but this must include audits, inspections and investigations.

639 Subsection (4) explains that, to prevent inefficiency and duplication of oversight, the IPC will not oversee particular areas that are already subject to oversight by other individuals or bodies. The IPC 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 IPC will not oversee matters which are overseen by the Information Commissioner or the Investigatory Powers Commissioner for Northern Ireland.

640 Subsection (6) and (7) 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. The Judicial Commissioners will have to decide for themselves if their proposed activity would, for example, prejudice national security or impede the effectiveness of operations. These duty not to act in a way that would have such an impact does not apply to the functions listed in subsection (8). Those are the functions which may be described as 'judicial functions' such as the authorisation functions of the Commissioners, deciding whether to approve the issuing, renewing or modification of a warrant.

Section 230: Additional directed oversight functions

641 As the policies, capabilities and practices of the security and intelligence agencies change with time, subsections (1) to (3) allow the Prime Minister to direct the IPC to oversee new areas. This is to ensure that independent oversight keeps pace with developments within the security and intelligence agencies. The Intelligence and Security Committee of Parliament may request that the Prime Minister gives a direction to the IPC.

642 Subsection (4) sets out that the Prime Minister must publish any direction that they give to the IPC to ensure that there is transparency about the Commissioner's 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, for example, the capabilities of an intelligence service, to the extent that it has a detrimental impact, such as causing damage to national security.

Section 231: Error reporting

643 This section provides for a process through which people can be informed of serious relevant error in the use of investigatory powers that relates to them. A relevant error means an error made by a public authority in complying with any requirement over which the Investigatory Powers Commissioner has oversight.

644 The IPC must inform the person affected by a relevant error if the error is serious and if it is in the public interest for the person to be informed. An error can only be considered serious if it has caused significant prejudice or harm to the person concerned. In deciding whether informing the person is in the public interest, the Commissioner 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.

645 If the IPC decides that the person should be informed, that person must also be informed of any right they have to bring a claim in the Investigatory Powers Tribunal. 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.

646 The IPC's annual report (see section 234) must include details regarding errors, including the number of errors the Commissioner becomes aware of, and the number of times a person has been informed of an error.

Section 232: Additional functions under this Part

647 This section sets out that a Judicial Commissioners must give the Investigatory Powers Tribunal any documents, information and other assistance the Tribunal may require, including the Commissioner's opinion on anything the Tribunal has to decide. This allows the Tribunal to take advantage of the IPC's expertise and the expertise of their office when reaching a decision.

648 Subsection (2) allows the IPC 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 damaging to one of the things listed, including national security, the Commissioner must consult the Secretary of State first. If the advice or guidance relates to matters that are the responsibility of the Scottish Ministers then the Scottish Ministers must also be consulted. The Commissioner does not have to consult the Secretary of State or Scottish Ministers before providing information to the Investigatory Powers Tribunal.

Section 233: Functions under other Parts and other enactments

649 This section amends other enactments so that functions of the Intelligence Services Commissioner, Interception of Communications Commissioner and the Surveillance Commissioners are instead carried out by the IPC and Judicial Commissioners.

Section 234: Annual and other reports

650 Subsection (1) means that the IPC must report to the Prime Minister on an annual basis about their work and subsection (2) lists matters which must be included in that report. The Prime Minister may require additional reports. The IPC may report at any time on any matter the Commissioner has oversight of. The IPC's reports can include any recommendations the Commissioner thinks appropriate.

651 Subsections (6) and (7) state that upon receipt of an annual report from the IPC 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 IPC before deciding to redact anything from the report. The Prime Minister must additionally consult the Scottish Ministers before redacting anything relating to Part 3 of the Police Act 1997. Reports that are laid before Parliament must be sent to the Scottish Ministers to be laid before the Scottish Parliament.

652 If the Commissioner has carried out an investigation, inspection or audit following a referral from the Intelligence and Security Committee of Parliament, then the Prime Minister must share a copy of any resulting report with the Committee, so long as the report relates to

matters which are within the statutory remit of the Committee.

Section 235: Investigation and information powers

653 This section ensures that the Judicial Commissioners have access to the information necessary to carry out the Commissioners' oversight role effectively. The section does this by requiring people to provide a Judicial Commissioner with all the information and documents that the Commissioner may need. People must also provide the Commissioner with any assistance they may need when carrying out investigations, inspections or audits. This section does not limit what such assistance may include, but makes clear that it includes providing access to technical systems.

654 The duties to provide information and assistance applies very widely. The persons to whom these obligations apply include anyone working for a public authority, telecommunications and postal operators who are subject to obligations under this Act and anyone who is or may be required to provide assistance under the Act.

Section 236: Referrals by the Intelligence and Security Committee of Parliament

655 This section provides that if the Intelligence and Security Committee of Parliament refers an issue to the IPC with the intention that the Commissioner should carry out an investigation, inspection or audit, then the IPC must inform the Committee of their decision as to whether to do so.

Section 237: Information gateway

656 This section allows people to provide information to a Judicial Commissioner, regardless of any other legal restrictions that might exist. This right extend to anyone working for a public authority, a communications service provider or indeed any member of the general public. This means that, for example, someone whose work relates to the use of investigatory powers may tell a Judicial Commissioner about their work, and any concerns they may have, without being censured for doing so. An exception to this is that the protections in the Data Protection Act 1998 still apply when information is provided to the IPC.

Section 238: Funding, staff and facilities

657 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.

658 Subsection (2) requires the Secretary of State to provide the IPC with the staff, accommodation, equipment, facilities and services that the Secretary of State considers necessary. It is intended that the resources afforded to the IPC ensure that the office is fully staffed with administrative, 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 must consult with the IPC. Treasury approval is required as to the number of staff. However, it is for the IPC to hire such staff and procure such services as they feel are necessary. Should the IPC believe that the resources afforded to them are insufficient, then they may publicly report the fact in their Annual Report or raise the matter with the Intelligence and Security Committee of Parliament.

659 This section also allows the Scottish Ministers to provide funding for the work done by Judicial Commissioners in relation to the exercise of devolved functions by Scottish public authorities. This might include, for example, Judicial Commissioners approving a decision by the chief constable of the Police Service of Scotland to issue an equipment interference warrant.

660 Subsections (5) to (7) allow the IPC and other Judicial Commissioners to delegate some of

their functions to staff. It also allows delegation to other people acting on their behalf, which might include contractors. "Functions" include powers and duties (see the definition in section 246(1)) so, for example, the power to require the provision of assistance may be delegated. This will mean that inspectors carrying out inspections, investigations or audits on behalf of the Judicial Commissioners may have conferred on them the right to receive exactly the same levels of co-operation, access and assistance that the Commissioners themselves would receive. Certain judicial functions and functions relating to appointments cannot be delegated to members of staff.

Section 239: Power to modify functions

661 This section allows the functions of the IPC to be changed by regulations. Such regulations 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. However, this power cannot be used to change the Judicial Commissioners' functions to approve, quash or cancel an authorisation or warrant.

Section 240: Abolition of existing oversight bodies

662 The IPC replaces the commissioners who provided oversight of investigatory powers before this Act: the Interception of Communications Commissioner, the Surveillance Commissioners (including Assistant Surveillance Commissioners) and the Intelligence Services Commissioner. The abolition of the Chief Surveillance Commissioner and Assistant Surveillance Commissioners includes those appointed by the Scottish Ministers for the purposes of RIPSA. Accordingly, this section abolishes those offices.

663 This section provides for a power to make regulations abolishing the Investigatory Powers Commissioner of Northern Ireland and providing for that Commissioner's functions to be given to the IPC. Such regulations can only be made with the consent of the Northern Ireland Assembly.

Chapter 2: Other arrangements

Section 241: Codes of practice

664 This section provides for the Secretary of State to issue codes of practice concerning the use of powers under the Act, as outlined in Schedule 7.

Schedule 7: Codes of practice

665 Paragraph 1 requires the Secretary of State to issues codes of practice in respect of the exercise of functions under the Act, but not in relation to any functions conferred on certain persons where this would not be appropriate, such as the Technical Advisory Board, courts and tribunals or oversight bodies.

666 Paragraph 2 specifies that each code of practice must include provisions designed to protect the confidentiality of journalistic sources. The codes must also set out particular considerations which should be applied to data relating to a member of a profession which would regularly hold legally privileged or other confidential information, such as medical professionals, those in the legal profession or parliamentarians. A code about targeted interception or equipment interference and bulk interception or equipment interference, must contain detail about what circumstances are to be regarded as "exceptional and compelling" in the context of such circumstances allowing items subject to legal privilege to be deliberately obtained or selected for examination. The IPC must keep such detail contained in the codes under review.

667 Paragraph 3 requires the code of practice concerning the functions in Part 3 of the Act to include provisions about communications data acquired under that Part and held by public authorities. The code of practice must provide, in particular, for why, how, and where the data is held, who may access the data, disclosure of the data, and the processing and destruction of the data.

668 Paragraph 4 sets out the procedural requirements which must be followed by the Secretary of State in making a code of practice. The Secretary of State must consult on any draft code of practice and may modify a code on the basis of representations made after its publication in daft. The Secretary of State must specifically consult the IPC on all draft codes, and the Information Commissioner on a code of practice concerning Part 4. A code will come into force in accordance with regulations made by the Secretary of State, which must be laid in draft before Parliament and approved by each House. Paragraph 5 allows the Secretary of State to make revisions to a code of practice, and sets out the procedural requirements for doing so, which reflect those for making a new code of practice.

669 Paragraph 6 sets out the effect of a code of practice issued by the Secretary of State. Any person exercising any function to which a code relates must have regard to the code. Failure to comply with the code does not, of itself, make a person liable to criminal or civil proceedings, but the code is 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. The IPC, Information Commissioner and the Investigatory Powers Tribunal can also take into account such a failure.

Section 242: Right of appeal from the Tribunal

670 Prior to this Act there was no domestic route of appeal from a decision or determination of the Investigatory Powers Tribunal, with claimants having to pursue appeals to the European Court of Human Rights if they wish to challenge a decision. This section amends RIPA to introduce a domestic appeal route from decisions and determinations of the Investigatory Powers Tribunal on a point of law, to the Court of Appeal in England and Wales or the Court of Session. This section contains a regulation making power so that, with the consent of the Northern Ireland Assembly, the Court of Appeal of Northern Ireland can be added to the Courts in which such appeals can be heard. Regulations will detail the criteria to be considered by the Investigatory Powers Tribunal when determining the relevant appellate court.

671 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, this decision may be reviewed by the appeal court.

672 The Tribunal or appellate court must not give permission to appeal on a point of law unless 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, such as that it would be in the wider public interest.

673 This section also amends RIPA to say that the Investigatory Powers Tribunal must notify all parties to proceedings when they have reached a decision or determination, including decisions on permission to appeal. There is an exception for circumstances where the Tribunal is prevented from doing so by its procedural rules, for example where the decision relates to closed proceedings.

Section 243: Functions of Tribunal in relation to this Act

674 This section amends sections 64 to 67 of RIPA, which deal with the jurisdiction of the Investigatory Powers Tribunal, in consequence of the Act. The result is that the Investigatory

Powers Tribunal will have jurisdiction regarding claims brought against public authorities in respect of all the powers provided for in the Act.

Section 244: Oversight by Information Commissioner in relation to Part 4

675 The Information Commissioner must audit requirements or restrictions concerning data retained subject to a retention notice under Part 4 of the Act, for example, to ensure the data is retained securely. This is distinct from the IPC's role in respect of the acquisition of communications data.

Section 245: Technical Advisory Board

676 This section provides for the continued existence of the Technical Advisory Board, established under RIPA. Its make-up will be prescribed by the Secretary of State in regulations and must include a balanced representation of the interests of communications service providers and of those people able to apply for warrants or authorisations under the Bill. The regulations made under this section may also set out how many members must be present for the Board to carry out its functions.

Section 246: Technology Advisory Panel

677 This section creates a panel which will provide advice to the IPC, the Secretary of State and the Scottish Ministers about the impact of changing technology on the exercise of investigatory powers and the availability and development of techniques to use such powers while minimising interference with privacy. The panel is required to provide an annual report to the IPC which must be copied to the Secretary of State and, where appropriate, the Scottish Ministers.

Section 247: Members of the Panel

678 This section provides for members of the Technology Advisory Panel to be appointed by the IPC. The same duties to provide information to the Judicial Commissioner in section 235 apply in relation to providing information to members of the Panel.

Part 9: Miscellaneous and general provisions

Chapter 1: Miscellaneous

Section 248: Combination of warrants and authorisations

679 This section explains that Schedule 8 allows for the combination of targeted interception and equipment interference warrants with other warrants or authorisations. This builds on the provisions in RIPA allowing for certain warrants and authorisations to be combined. RIPA allows authorisations that combine property interference under ISA and intrusive surveillance under RIPA.

Schedule 8: Combination of warrants

680 This Schedule allows for certain different warrants and authorisations to be applied for in combination with each other. It may be that a single operation or investigation will involve conduct that needs to be authorised under a number of different warrants or authorisations. This Schedule means that one application can be made covering all of the authorisations and warrants that are needed. This has the advantage of avoiding duplication. It also means that the person who has to take the decision to issue the warrant, and a Judicial Commissioner reviewing that decision, has sight of all of the conduct that is being authorised. However, the public authority applying for warrants and authorisations is not obliged to apply for them in

combination with each other. Nothing in this Schedule prevents warrants and authorisations that are related to each other being applied for individually.

681 Where warrants are applied for in combination, the resulting warrant is referred to as a "combined warrant". A combined warrant is a single warrant, though it may be made up of a number of other warrants and authorisations that would otherwise be issued individually.

682 Part 1 of the Schedule explains the warrants and authorisations that may be issued in combination with a targeted interception warrant. It does this by first listing the combinations that can be issued by the Secretary of State (paragraphs 1 to 3) and then the combinations that can be issued by the Scottish Ministers (paragraphs 4 to 7). Part 2 of the Schedule repeats this, but for warrants and authorisations that can be issued in combination with a targeted equipment interference warrant. Part 2 is divided up into the combined warrants that can be issued by the Secretary of State, the Scottish Ministers and by the heads of law enforcement bodies. Part 3 of the Schedule provides for one further combined warrant: a combination of a targeted examination warrant issued under Part 2 of the Act with a targeted examination warrant issued under Part 5 of the Act.

683 In some circumstances, the effect of Parts 1 to 3 will be that a person will be given the power to issue a combined warrant including an authorisation that the person would not normally be able to issue. This would occur, for example, if the National Crime Agency wanted a combined warrant made up of a targeted interception warrant and a targeted equipment interference warrant. The National Crime Agency would apply to the Secretary of State (or the Scottish Ministers) who may issue the combined warrant, even though they would not normally issue a targeted equipment interference warrant to the National Crime Agency. That is because the Director General of the National Crime Agency would normally issue such a warrant.

684 Paragraph 19 provides that where one of the warrants or authorisations that can make up a combined warrant is referred to anywhere in legislation, that reference includes that type of warrant when it is part of a combined warrant.

685 Paragraph 20 sets out that for certain matters, the rules that apply to a warrant will apply to the relevant part of a combined warrant. This includes, for example, the conditions that must exist before a warrant can be issued. Take the example of a combined warrant that is made up of a targeted interception warrant and an authorisation under section 93 of the Police Act 1997. The rules regarding when a targeted interception warrant can be issued will apply to the targeted interception warrant part of the combined warrant. The paragraph lists all the matters for which this principle applies.

686 However, paragraphs 21 to 23 create an exception to paragraph 20. When a combined warrant including a targeted interception warrant is issued, the rules regarding the procedure for issuing a targeted interception warrant applies to the whole combined warrant. And likewise, when a combined warrant includes a targeted equipment interference warrant, the combined warrant will be issued using the procedure for a targeted equipment interference warrant. This means that the double-lock applies to the whole combined warrant. So, for example, a combined warrant made up of a targeted interception warrant and an authorisation for intrusive surveillance could only be issued with the approval of a Judicial Commissioner, even though such approval would not normally be needed for an authorisation for intrusive surveillance. The exception specified in paragraphs 21(3) and 22(3) is where part of the combined warrant includes a warrant issued under section 5 of ISA. Judicial Commissioner approval is not required for the part containing the section 5 warrant.

687 Paragraph 24 provides that certain rules in the Police Act 1997 will not apply to an authorisation under section 93 of the Police Act 1997 when it is issued as part of a combined

warrant. For example, section 96 of the Police Act 1997 requires authorisations to be notified to a Judicial Commissioner. But if the authorisation is part of a combined warrant, a Judicial Commissioner will be required to approve the issuing of the warrant, and the rule in section 96 of the Police Act 1997 is not needed.

688 Paragraphs 25 and 26 are similar to paragraph 24, except they provide that certain rules in RIPA and RIPSA do not apply to authorisations for intrusive or directed surveillance when they are part of a combined warrant.

689 Some of the warrants and authorisations that can be combined have different durations. The normal rule, which is set out in paragraph 27, is that the shortest of the durations will apply. So, where an authorisation lasting 3 months is combined with one that lasts 6 months, the combined warrant lasts 3 months. However, there is one exception to this. When one of the intelligence services is issued with a combined warrant including an authorisation for directed surveillance, the warrant can last 6 months.

690 The effects of paragraphs 28 and 29 are that if a Judicial Commissioner refuses to approve the decision to issue a combined warrant that was issued urgently, the power for a Judicial Commissioner to determine what may be done with any material already obtained applies to the targeted interception or targeted equipment interference parts of the combined warrant.

691 The effect of paragraph 30 is that the rules about the service of warrants and requiring people to provide assistance in order to give effect to a warrant that apply to warrants under Part 2 or Part 5 of the Act apply to the part of a combined warrant that is made up of those warrants. For example, where a combined warrant includes a targeted interception warrant, the part of the combined warrant that is a targeted interception warrant can be served in the same way as a targeted interception warrant that was issued individually.

692 Section 56 provides that certain matters relating to interception warrants cannot be referred to or relied on in legal proceedings. The effect of paragraph 31 is that this rule applies to warrants under Part 2 of the Act that are issued as part of a combined warrant, but with one difference. The rules in section 56 mean that (subject to certain exceptions) it is not possible to reveal that a warrant under Part 2 was issued. The effect of paragraph 31 is that it will be possible to disclose the existence of a combined warrant, but only if doing so does not reveal that it included a warrant under Part 2. The effect of paragraph 32 is that one of the exceptions to the rules against disclosure, the ability to obtain legal advice, applies to advice about this Schedule.

Section 249: Payments towards certain compliance costs

693 This section requires the Secretary of State to ensure that there are arrangements in force to ensure that communications service providers receive an appropriate contribution towards the costs of complying with this 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 Part 9 must specify the level of contribution to be made.

Section 250: Power to develop compliance systems etc.

694 This section enables the Secretary of State to develop, provide, maintain or improve apparatus, systems, facilities and services to help the Secretary of State, another public authority or any other person to comply with the Act.

695 This power could be used, for example, to develop systems to be used by telecommunication operators in complying with obligations under the act or systems to be used by public authorities to acquire communications data. Such systems can operate in respect of multiple powers under the Act.

696 This section also allows the Secretary of State to achieve the same thing by entering into financial arrangements with any other, such as providing financial assistance.

Section 251: Amendments of the Intelligence Services Act 1994

697 Section (3)(1)(a) of ISA gives GCHQ the function of monitoring or interfering with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information. This section amends that provision to say that GCHQ can also "make use of" such emissions and equipment. This clarifies that GCHQ may, in the performance of its functions, make use of telecommunications 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.

698 Section (3)(1)(b) of ISA gives GCHQ the functions of providing advice and assistance about the protection of information to the armed forces, the Government and to certain organisations. This section amends that provision so that GCHQ may provide such advice to organisations, persons or the general public, both in the UK or abroad. This will enable GCHQ to provide information assurance advice to a wide audience on issues, such as cyber security, which affect not just the Government but also business and the public in general.

699 Subsection (3) amends section 5 of ISA to remove the restriction preventing the Secretary of State from issuing GCHQ and SIS with a property warrant relating to their function of supporting the prevention and detection of serious crime where the property is in the British Islands. The security and intelligence agencies have a remit to support law enforcement to help prevent and detect serious crime.

Section 252: National security notices

700 This section provides for the Secretary of State to give a national security notice to any telecommunications operator in the UK requiring the operator to take steps appearing to the Secretary of State to be necessary in the interests of national security. A national security notice may only be given if the conduct required by the notice is necessary and proportionate, and where the decision to give a notice has been approved by a Judicial Commissioner.

701 The section does not list the things that a national security notice might require an operator to do, but subsection (3) gives examples of the types of things. A notice can, for example, require an operator to provide services or facilities to help the intelligence service carry out its functions more effectively or more safely.

702 Subsection (5) stipulates that the notice cannot be used for the primary purpose of requiring an operator to do something for which a warrant or authorisation is required under this Act or any of the other Acts listed. The other Acts are ones that provide for investigatory powers. Where a notice requires the taking of steps for which a warrant or authorisation would otherwise be required, such a warrant or authorisation is needed regardless of the notice. This means that a national security notice cannot be used to avoid the need for a warrant or authorisation.

Section 253: Maintenance of technical capability

703 This section allows the Secretary of State to give an operator a notice which imposes obligations on the operator. A technical capability notice may only be given where the conduct required by the notice is necessary and proportionate, and where the decision to give the notice has been approved by a Judicial Commissioner. A notice may be given to a postal operator, a telecommunications operator or a person proposing to become either.

704 Subsection (4) provides for the Secretary of State to make regulations specifying the obligations that may be imposed upon relevant operators under a notice. The Secretary of

State may specify an obligation only if he or she believes the obligations are a reasonable way of ensuring that operators are able to comply with any warrant under Part 2, 5 or 6, or any authorisation or notice given under Part 3.

705 Subsection (5) gives examples of the sorts of obligations that may be included in the regulations. The regulations could include, for example, obligations to provide communications facilities to support the implementation of warrants, ensuring the security of facilities, or ensuring that staff who handle classified material are appropriately vetted.

706 Subsection (6) requires the Secretary of State to consult a number of people before making the regulations provided for at subsection (3). These include persons with statutory functions affecting providers of communications services, such as the IPC.

707 Subsection (8) confirms that a technical capability notice can be given to persons outside the United Kingdom. A notice may relate to conduct outside of the United Kingdom.

Section 254: Approval of notices by Judicial Commissioners

708 This section sets out the test to be applied by Judicial Commissioners when deciding whether to approve the Secretary of State's decision to give a national security notice or a technical capability notice. The Judicial Commissioner must review the Secretary of State's conclusions regarding the necessity of the notice and the proportionality of the conduct required by the notice, applying the same principles as would be applied by a court on an application for judicial review. The Judicial Commissioner must consider a decision with a sufficient degree of care as to ensure the Commissioner complies with the duties imposed by section 2.

709 Should a Judicial Commissioner refuse to approve the Secretary of State's decision to give a notice, subsection (4) requires the Judicial Commissioner to provide written reasons for the refusal. Where a Judicial Commissioner has refused to approve a notice, subsection (5) allows the Secretary of State to ask the IPC to decide whether to approve the decision to give a notice.

Section 255: Further provision about notices under section 252 or 253

710 Subsection (2) requires the Secretary of State to consult the operator before giving either a national security notice or technical capability notice. Subsection (3) sets out considerations the Secretary of State must take into account before giving a notice. Subsection (4) makes clear that the Secretary of State must give specific consideration to the technical feasibility and likely cost of complying with obligations that relate to the removal of encryption.

711 Subsection (6) set out two mechanisms by which a notice may be given to a person outside the United Kingdom, though a notice can be given in any other way. Subsection (8) makes clear that any person to whom a technical capability notice is given, or any person employed or engaged for the purposes of that person's business, cannot disclose the existence or the contents of that notice to any person without the permission of the Secretary of State.

712 Subsection (9) requires a person to whom a notice is given to comply with it. Subsection (12) makes clear that in relation to national security notices, a person must give effect to obligations imposed by a national security notice, notwithstanding any requirements imposed on them by the listed provisions in the Communications Act 2003. This replicates a provision previously provided for in the Telecommunications Act 1984 (as amended by the Communications Act 2003) and removes any ambiguity about how the obligations set out in a national security notice relate to those provided for in relevant parts of the Communications Act 2003.

713 Subsection (10) outlines that the Secretary of State may bring civil proceedings to enforce both a national security and technical capability notice in relation to 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 interception warrants or an authorisation or notice given under Part 3.

Section 256: Variation and revocation of notices

714 This section requires the Secretary of State to keep a technical capability notice or national security notice under review. It allows the Secretary of State to vary or revoke a notice, but only if the variation is necessary and the conduct as varied is proportionate to what is sought to be achieved. If the variation would impose further requirements on an operator, the decision to vary a notice must be approved by a Judicial Commissioner.

715 Where Judicial Commissioner approval is required, subsection (8) means that the Commissioner employs the same test as when deciding whether to approve a decision to give a notice. Subsection (9) means that the obligations to consult operators and to take certain matters into account apply when varying a notice as they do when giving a notice.

Section 257: Review by the Secretary of State

716 This section permits the recipient of a notice to refer the notice, or part of the notice, back to the Secretary of State for review. The person does not have to comply with the notice, or part of the notice, until it has been reviewed. The Secretary of State must consult both the Technical Advisory Board and a Judicial Commissioner. Subsection (8) requires the Commissioner and the Technical Advisory Board to consult the person to whom the notice has been given and the Secretary of State, and report their conclusions to both parties.

717 After consideration of the conclusions of the Commissioner and Board, the Secretary of State may decide to vary the notice or revoke it, or give a notice to the person confirming its effect. The Secretary of State can only vary a notice or give a notice confirming its effect with the approval of the IPC.

Section 258: Approval of notices following review under section 257

718 This section makes provision for the IPC to decide whether to approve the Secretary of State's decision to either vary a notice or give a notice confirming the effect of a notice.

719 Subsection (2) requires the IPC to consider whether the notice as varied or confirmed by the Secretary of State is necessary and whether the conduct as varied is proportionate to what is sought to be achieved by that conduct. The test applied by the IPC is the same as a Judicial Commissioner would apply when deciding whether to approve the decision to give a notice.

Section 259: Amendments of the Wireless Telegraphy Act 2006

720 This section amends the Wireless Telegraphy Act 2006 so that Act 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 Act provides for such interception.

Chapter 2: General

Section 260: Review of operation of Act

721 This section provides for the Secretary of State to prepare a report on the operation of the Act after five years and six months. The Secretary of State is obliged, in preparing the report, to take into account any report made by a Select Committee of either Houses of Parliament, or by a Joint Committee of both Houses.

Section 261: Telecommunications definitions

722 This section provides relevant definitions in relation to telecommunication systems, services and operators.

723 The Act defines communications data in respect of telecommunications systems, services and operators to provide for technologically neutral, modernised definitions. Communications data is data held by a telecommunications operator or available directly from the network which identifies a person or device on the network, ensures that a communication reaches its intended destination, describes how a person has been using a service or is about the architecture of the telecommunication system itself. Communications data is divided into entities data and events data.

724 Subsection (2) defines a telecommunication. It includes communications between persons, between a person and a machine and between machines.

725 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 or objects.

726 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.

727 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; or 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; or the destination IP address that an individual has connected to online.

728 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, for example, the telephone call.

729 Subsection (6)(b) makes clear that anything which meets the definitions of systems data within section 264 is not content.

730 Subsections (8) to (14) define communication service providers and systems for the purpose of the Act.

Section 262: Postal definitions

731 Subsection (3) defines what is meant by communications data in the postal context. Subsection (3)(a) includes data that ensures a postal item reaches its destination – such as an address on an envelope. Subsection 3(b) includes data about the use of a postal service, for example it could indicate whether a mail redirection is in place. Subsection 3(c) includes information about a person to whom a postal service is provided – for example the contact details for a person who holds a postal account. Subsection (4) makes clear than anything on the outside of a postal item which relates to its transmission or identifies the sender or recipient is

communications data.

732 Subsection (5) defines a postal item. This does not include containers or any other form of freight. The provisions of the Act do not apply to freight.

733 Subsections (6) to (8) define communication service providers and systems for the purpose of the Act.

Section 263: General definitions

734 Subsection (1) defines terms used throughout the Act. The definition of serious crime in this subsection is subject to the transitional provision in paragraph 6 of schedule 9.

735 Subsections (2) to (4) set out the definitions of systems data and identifying data. Systems data is data which enables or facilitates, or otherwise relates to, the functioning of a postal service, telecommunications system or telecommunications service, or of any other relevant system (or service provided by means of that system). A communication or item of information may include data which may be used:

a. to identify, or assist in identifying, any person, apparatus, system or service;

b. to identify any event; or

c. to identify the location of any person, event or thing.

736 In most cases this data will be systems data, however, there will be cases where this information does not enable or otherwise facilitate the functioning of a service or system and therefore is not systems data. Where such data, can be logically separated from the remainder of the communication or item of information and does not, once separated, reveal the meaning (if any) of any communication or item of information it is identifying data.

Section 264: General definitions: "journalistic material"

737 This provides a definition of journalistic material and confidential journalistic material. It makes clear that material is not to be regarded as created or acquired for the purposes of journalism if it is created or acquired with the intention of furthering a criminal purpose.

Section 265: Index of defined expressions

738 This provision is self-explanatory.

Section 266: Offences by bodies corporate etc.

739 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. If the offence is committed with the consent or connivance of a senior officer, or is caused by that person's neglect, that person (as well as the body corporate or partnership) may be found guilty of the offence.

Section 267: Regulations

740 This section sets out the parliamentary procedures to which the various delegated legislative powers under the Act are subject. It sets out which parliamentary procedure applies to which power, and provides that regulations subject to certain procedures may be combined.

Section 268: Enhanced affirmative procedure

741 This section sets out the enhanced affirmative procedure to which certain regulations under the Act are subject, including regulations which provide for additional authorities to be able to acquire communications data. The enhanced affirmative procedure is a process for making secondary legislation that allows for greater scrutiny than the affirmative procedure. It allows

for scrutiny by a committee of either House of Parliament.

Section 269: Financial provisions

742 This provision is self-explanatory.

Section 270: Transitional, transitory or saving provision

743 This section introduces Schedule 9 and gives the Secretary of State power to make any transitional, transitory or saving provisions considered appropriate in connection with the coming into force of the provisions in the Act. This standard power enables the changes made the Act to be implemented in an orderly manner.

Schedule 9: Transitional, transitory and saving provision

744 Schedule 9 contains transitional, transitory and saving provisions for the Act. In particular, paragraph 1 provides that an agreement designated under section 1(4) of RIPA as an international mutual assistance agreement shall be treated as if they had been designated as such under section 11(3) of this Act.

745 Paragraphs 3 to 5 sets out transitional arrangements for the retention of communications data. Retention notices given under DRIPA will remain in force, and be treated as retention notices given under Part 4 of the Act, until six months after section 1(1) of DRIPA is repealed. However, during this six month transitional period, certain provisions in Part 4 of the Act will not apply to such notices. For example, the provisions requiring Judicial Commissioner approval will not apply.

746 Paragraph 4 anticipates the possibility of Section 87 of the Act being brought into force without any requirement that the giving, varying or confirming of a notice requires the approval of a Judicial Commissioner. This may occur if section 87 of the Act is brought into force before the Judicial Commissioners, provided for in Part 8 of the Act, have been appointed. Paragraph 4 provides that a notice given, varied or confirmed will cease to have effect 3 months after the requirement for approval etc. comes into force.

747 The definition of "serious crime" and "other relevant crime" is dependent on the sentence someone could receive for an offence at the age of 18 in England and Wales, or at the age of 21 in Northern Ireland and Scotland. The definitions are to be read as if the relevant age was 21 in England and Wales until paragraph 211 of Schedule 7 to the Criminal Justice and Court Service Act 2000 (which would amend an equivalent definition in RIPA) comes into force.

Section 271: Minor and consequential provision

748 This section introduces Schedule 10 and gives the Secretary of State power to make regulations to make such provision as the Secretary of State considers appropriate in consequence of this Act, including by amending legislation. Subsection (4) makes clear that this provision cannot be used to modify any primary legislation made after the end of the Session in which this Act is passed.

Schedule 10: Minor and consequential provision

749 Schedule 10 makes minor and consequential amendments to other enactments. The explanatory notes will provide an overview of these amendments, and will highlight the most significant, but will not explain every amendment in detail.

750 Often pieces of legislation refer to other pieces of legislation. One of the things this Schedule does is make sure that these references work despite the other changes made by the Act. The Schedule also updates certain definitions, including some in RIPA, to refer to the definitions in the Act. For example, in RIPA, "postal service" is defined in relation to a section of that Act that is being repealed. As a consequence, paragraph 6(5) of this Schedule provides that in

RIPA "postal service" is given the definition that is in this Act.

751 The Schedule also provides that provisions in other legislation that refer to matters in RIPA will now apply to equivalent matters in the Act. For example, section 6(4) of the Justice and Security Act 2013 provides for courts seised of relevant civil proceedings to be able to make a declaration that the proceedings are such that an application for closed material proceedings may be made. A necessary precondition is that a party to the proceedings would be required to disclose sensitive material or would be required to disclose sensitive material were it not for certain prohibitions, including section 17 of RIPA. Paragraph 52 of the Schedule replaces the reference to section 17 of RIPA with the equivalent provision of the Act (section 56(1)). This means that the provision of the Justice and Security Act 2013 will continue to have the same effect, despite this Act replacing parts of RIPA.

752 The Schedule makes a number of very similar amendments. There are a number of places in legislation where disclosure provisions (either provisions that allow information to be disclosed or provisions that require certain information to be provided) are limited with reference to Part 1 of RIPA. This means that the restrictions on disclosure (including in section 19 of RIPA) override provisions that otherwise allow disclosure to be made. This Schedule means that in such instances disclosure provisions will be restricted by Parts 1 to 7 and Chapter 1 of Part 9 of the Act. Such amendments are made by Paragraphs 7 and 8, 11 to 13, 15 to 27, 29 to 33 and 35 of this Schedule.

753 Paragraphs 2 and 42 amend Schedules 2 and 3 of the Northern Ireland Act 1998. Those Schedules list the matters that are excepted and reserved, and consequently determine what matters have been devolved to the Northern Ireland Assembly. The amendments made in paragraphs 2 and 42 maintain the position before this Act, so that anything excepted or reserved continues to be excepted or reserved. A similar amendment is made to the Scotland Act 1998 by paragraph 41.

754 Paragraph 6A of the Crime and Courts Act 2013 provides that an NCA officer requires the consent of the Chief Constable of the Police Service of Northern Ireland before that officer can carry out certain investigatory activity in Northern Ireland. The amendment made by paragraph 70 of this Schedule means that consent will be required before an NCA officer interferes with equipment that is known to be in Northern Ireland.

755 Part 5 of the Schedule makes a number of amendments in consequence of the IPC and the Judicial Commissioners replacing the Intelligence Services Commissioner, Interception of Communications Commissioner and Surveillance Commissioners. This is in addition to the amendments made by Section 233 and provides that the Judicial Commissioners will have the same powers and functions as the Commissioners that they are replacing. For example, the Protection of Freedoms Act 2012 includes a duty to consult the Chief Surveillance Commissioner when preparing a code of practice under section 28. This is amended so that it will be necessary to consult the IPC instead. In some places, rules regarding the existing Commissioners have been omitted because they replicate matters dealt with in the Act. For example, section 40 of RIPA concerns information that must be provided to the Surveillance Commissioners. This is no longer necessary as the duty to provide information to the Judicial Commissioners (see section 235) will apply.

Section 272: Commencement, extent and short title

756 This section makes provision for the Act to come into force on a certain day or different days as appointed by the Secretary of State in regulations.

757 Subsections (2) and (3) say when certain of the provisions of the Act come into force.

758 Subsections (4) to (7) set out the territorial extent of the Act. Subsection (7) provides for the

Act to be extended to (with or without modifications) to the Isle of Man or any of the British overseas territories, by Order in Council.

Commencement

759 Sections 260 to 269, 270(2), 271(2) to (4) and 272 commence on Royal Assent. Sections 227 and 228 come into force two months after Royal Assent. The remaining provisions of the Act will be brought into force by means of regulations made by the Secretary of State.

Related documents

760 The following documents are relevant to the Act and can be read at the stated locations:

Reports informing the draft Bill

- Privacy and Security – a report by the Intelligence and Security Committee of Parliament: http://isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt(web).pdf#
- A Question of Trust: Report of the Investigatory Powers Review by David Anderson QC: https://www.gov.uk/government/publications/a-question-of-trust-report-of-the-investigatory-powers-review
- A Democratic Licence to Operate: Report of the Independent Surveillance Review by the Royal United Services Institute for Defence and Security Studies: https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf

Pre-legislative scrutiny

- Oral statement and debate: Draft Investigatory Powers Bill
    - House of Commons Hansard Vol. 601 Col. 969-992 (http://hansard.parliament.uk/pdf/Commons/2015-11-04)
    - House of Lords Hansard Vol. 765 Col. 1652-1666 (http://hansard.parliament.uk/pdf/Lords/2015-11-04)
- Joint Committee report on the draft Investigatory Powers Bill: http://www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/93.pdf
- Intelligence and Security Committee Report on the draft Investigatory Powers Bill: http://isc.independent.gov.uk/files/20160209_ISC_Rpt_IPBill(web).pdf
- House of Commons Science and Technology Committee – Investigatory Powers Bill: technology issues: http://www.publications.parliament.uk/pa/cm201516/cmselect/cmsctech/573/573.pdf
- Government response to pre-legislative scrutiny reports: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504174/54575_Cm_9219_WEB.PDF

Other reports

- Report of the Bulk Powers Review: https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2016/08/Bulk-Powers-Review-final-report.pdf
- Joint Committee on Human Rights Legislative Scrutiny: Investigatory Powers Bill: http://www.publications.parliament.uk/pa/jt201617/jtselect/jtrights/104/104.pdf
- Delegated Powers and Regulatory Reform Committee second report of session 2016-17, published 8 July 2016, including Investigatory Powers Bill: http://www.publications.parliament.uk/pa/ld201617/ldselect/lddelreg/21/2104.htm
- Select Committee on the Constitution third report of session 2016-17, published 11 July 2016, Investigatory Powers Bill: http://www.publications.parliament.uk/pa/ld201617/ldselect/ldconst/24/2402.htm

Government legal memoranda

- European Convention on Human Rights memorandum: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/506171/ECHR_Memo_-_Introduction.pdf
- Delegated Powers Memorandum: http://www.parliament.uk/documents/lords-committees/delegated-powers/Investigatory-Powers-Bill-DPM.pdf
- Supplementary Delegated Powers Memorandum: http://www.parliament.uk/documents/lords-committees/delegated-powers/Investigatory-Powers-Bill-SDPM.pdf

Legislative consent of the Scottish Parliament

- Legislative consent memorandum: http://www.parliament.uk/documents/commons-public-bill-office/2016-17/legislative-consent-resolutions/Investigatory-Powers-Bill-LCM1-251016.pdf
- Letter from the Clerk of the Scottish Parliament to the Clerk of the House of Commons confirming legislative consent: http://www.parliament.uk/documents/commons-public-bill-office/2016-17/legislative-consent-resolutions/Investigatory-Powers-Bill-LCM2-251016.pdf
- Extract of minutes of proceedings of the Scottish Parliament, 6 October 2016: http://www.parliament.uk/documents/commons-public-bill-office/2016-17/legislative-consent-resolutions/Investigatory-Powers-Bill-LCM3-251016.pdf

Court judgments and opinions

- European Court Judgment: Judgment of 8.4. 2014 – Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Others: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0293&from=EN

- Advocate-General's Opinion on DRIPA Judicial Review: http://curia.europa.eu/juris/document/document.jsf?docid=181841&doclang=EN

Previous editions of the Bill

- Bill 143: http://www.publications.parliament.uk/pa/bills/cbill/2015-2016/0143/16143.pdf
- Bill 2: http://www.publications.parliament.uk/pa/bills/cbill/2016-2017/0002/17002.pdf
- HL Bill 40: http://www.publications.parliament.uk/pa/bills/lbill/2016-2017/0040/17040.pdf
- HL Bill 62: http://www.publications.parliament.uk/pa/bills/lbill/2016-2017/0062/17062.pdf
- HL Bill 66: http://www.publications.parliament.uk/pa/bills/lbill/2016-2017/0066/17066.pdf

Annex A - Glossary

BPD	Bulk personal dataset
DRIPA	Data Retention and Investigatory Powers Act 2014
GCHQ	Government Communications Headquarters
IP address	Internet Protocol address
IPC	Investigatory Powers Commissioner
IPT	Investigatory Powers Tribunal
ISA	Intelligence Services Act 1994
ISC	Intelligence and Security Committee
MI5	Security Service
MI6	Secret Intelligence Service (SIS)
NCA	National Crime Agency
Ofcom	Office of Communications
RIPA	Regulation of Investigatory Powers Act 2000
RIPSA	Regulation of Investigatory Powers (Scotland) Act 2000
SIS	Secret Intelligence Service (MI6)
SPoC	single point of contact
TAP	Technology Advisory Panel

Annex B - Territorial extent and application

Provision	England	Wales		Scotland		Northern Ireland	
	Extends to E & W and applies to England?	**Extends to E & W and applies to Wales?**	**Legislative Consent Motion required?**	**Extends to Scotland?**	**Legislative Consent Motion required?**	**Extends to Northern Ireland?**	**Legislative Consent Motion required?**
Part 1: General privacy Protections							
Section 1	Yes	Yes	No	Yes	No	Yes	No
Section 2	Yes	Yes	No	Yes	Yes	Yes	No
Sections 3 to 13	Yes	Yes	No	Yes	No	Yes	No
Schedule 1	Yes	Yes	No	Yes	No	Yes	No
Schedule 2	Yes	Yes	No	Yes	No	Yes	No
Section 14	Yes	Yes	No	Yes	Yes	Yes	No
Part 2: Lawful interception of communications							
Sections 15 to 20	Yes	Yes	No	Yes	No	Yes	No
Sections 21 to 25	Yes	Yes	No	Yes	Yes	Yes	No
Section 26	Yes	Yes	No	Yes	No	Yes	No
Sections 27 to 30	Yes	Yes	No	Yes	Yes	Yes	No
Sections 31 and 32	Yes	Yes	No	Yes	No	Yes	No
Sections 33 to 39	Yes	Yes	No	Yes	Yes	Yes	No
Sections 40 to 48	Yes	Yes	No	Yes	No	Yes	No
Sections 49 and 50	Yes	Yes	No	Yes	Yes	Yes	No
Sections 51 and 52	Yes	Yes	No	Yes	No	Yes	No
Sections 53 to 55	Yes	Yes	No	Yes	Yes	Yes	No
Section 56	Yes	Yes	No	Yes	No	Yes	No
Schedule 3	Yes	Yes	No	Yes	No	Yes	No
Section 57	Yes	Yes	No	Yes	Yes	Yes	No

Sections 58 to 60	Yes	Yes	No	Yes	No	Yes	No
Part 3: Authorisations for obtaining communications data							
Sections 61 to 86	Yes	Yes	No	Yes	No	Yes	No
Schedule 4	Yes	Yes	No	Yes	No	Yes	No
Schedule 5	Yes	Yes	No	Yes	No	Yes	No
Part 4: Retention of communications data							
Sections 87 to 98	Yes	Yes	No	Yes	No	Yes	No
Part 5: Equipment interference							
Sections 99 to 102	Yes	Yes	No	Yes	No	Yes	No
Section 103	No	No	No	Yes	Yes	No	No
Section 104	Yes	Yes	No	Yes	No	Yes	No
Sections 105 to 110	Yes	Yes	No	Yes	Yes	Yes	No
Schedule 6	Yes	Yes	No	Yes	Yes	Yes	No
Section 111	Yes	Yes	No	Yes	No	Yes	No
Sections 112 to 114	Yes	Yes	No	Yes	Yes	Yes	No
Section 115	Yes	Yes	No	Yes	No	Yes	No
Section 116	Yes	Yes	No	Yes	No	Yes	No
Sections 117 to 125	Yes	Yes	No	Yes	Yes	Yes	No
Sections 126 to 128	Yes	Yes	No	Yes	No	Yes	No
Sections 129 to 132	Yes	Yes	No	Yes	Yes	Yes	No
Sections 133 to 135	Yes	Yes	No	Yes	No	Yes	No
Part 6: Bulk warrants							
Sections 136 to 198	Yes	Yes	No	Yes	No	Yes	No
Part 7: Bulk personal dataset warrants							
Sections 199 to 226	Yes	Yes	No	Yes	No	Yes	No
Part 8: Oversight arrangements							
Section 227	Yes	Yes	No	Yes	Yes	Yes	No
Section 228	Yes	Yes	No	Yes	No	Yes	No
Section 229	Yes	Yes	No	Yes	Yes	Yes	No

Section 230	Yes	Yes	No	Yes	No	Yes	No
Sections 231 to 235	Yes	Yes	No	Yes	Yes	Yes	No
Sections 236 to 238	Yes	Yes	No	Yes	No	Yes	No
Sections 239 and 240	Yes	Yes	No	Yes	Yes	Yes	No
Section 241	Yes	Yes	No	Yes	No	Yes	No
Schedule 7	Yes	Yes	No	Yes	No	Yes	No
Sections 242 and 243	Yes	Yes	No	Yes	Yes	Yes	No
Sections 244to 247	Yes	Yes	No	Yes	No	Yes	No
Part 9: Miscellaneous and general provisions							
Section 248	Yes	Yes	No	Yes	Yes	Yes	No
Schedule 8	Yes	Yes	No	Yes	Yes	Yes	No
Sections 249 to 270	Yes	Yes	No	Yes	No	Yes	No
Schedule 9	Yes	Yes	No	Yes	No	Yes	No
Sections 271 and 272	Yes	Yes	No	Yes	Yes	Yes	No
Schedule 10	Yes	Yes	No	Yes	Yes	Yes	No

761

Annex C - Hansard References

762 The following table sets out the dates and Hansard references for each stage of the Act's passage through Parliament.

Stage	Date	Hansard Reference
House of Commons		
Introduction	1 March 2016	Vol. 606 Col. 836
Second Reading	15 March 2016	Vol. 607 Col. 812-909
Public Bill Committee	24 March 2016 12 April 2016 14 April 2016 19 April 2016 21 April 2016 26 April 2016 28 April 2016 3 May 2016	First sitting; Second sitting Third sitting; Fourth sitting Fifth sitting; Sixth sitting Seventh sitting; Eighth sitting Ninth sitting; Tenth sitting Eleventh sitting; Twelfth sitting Thirteenth sitting; Fourteenth sitting Fifteenth sitting; Sixteenth sitting
Report and Third Reading	6 June 2016	Vol. 611 Col. 868-1006
House of Lords		
Introduction	8 June 2016	Vol. 773 Col. 747
Second Reading	27 June 2016	Vol. 773 Col. 1359-1379 and 1401-1464
Grand Committee	11 July 2016 13 July 2016 19 July 2016 5 September 2016 7 September 2016 12 September 2016	Vol. 774 Col. 13-33, 50-81 and 95-116 Vol. 774 Col. 220-281 Vol. 774 Col. 536-601 and 621-636 Vol. 774 Col. 856-873 and 901-913 Vol. 774 Col. 1042-1090 and 1105-1122 Vol. 774 Col. 1310-1321
Report	11 October 2016 17 October 2016 19 October 2016	Vol. 774 Col. 1789-1858 Vol. 774 Col. 2119-2161 and 2170-2201 Vol. 774 Col. 2346-2422
Third Reading	31 October 2016	Vol. 776 Col. 433-451
Ping pong		
Consideration of Lords amendments	1 November 2016	House of Commons Vol. 616 Col. 813-859
Consideration of Commons reasons	2 November 2016	House of Lords Vol. 776 Col. 642-660
Consideration of Lords message	15 November 2016	House of Commons Vol. 617 Col. 154-172
Consideration of Commons reasons	16 November 2016	House of Lords Vol. 776 Col. 1430-1436
Royal Assent	29 November 2016	House of Commons Vol. 617 Col. 1377 House of Lords Vol. 777 Col. 85

Annex D - Progress of Bill Table

763 This Annex shows how each section and Schedule of the Act was numbered during the passage of the Bill through Parliament.

Section of the Act	Bill as Introduced in the Commons	Bill as amended in Committee in the Commons	Bill as introduced in the Lords	Bill as amended in Committee in the Lords	Bill as amended on Report in the Lords
Section 1	Clause 1	Clause 1	Clause 1	Clause 1	Clause 1
Section 2			Clause 2	Clause 2	Clause 2
Section 3	Clause 2	Clause 2	Clause 3	Clause 3	Clause 3
Section 4	Clause 3	Clause 3	Clause 4	Clause 4	Clause 4
Section 5	Clause 4	Clause 4	Clause 5	Clause 5	Clause 5
Section 6	Clause 5	Clause 5	Clause 6	Clause 6	Clause 6
Section 7	Clause 6	Clause 6	Clause 7	Clause 7	Clause 7
Section 8			Clause 8	Clause 8	Clause 8
					Clause 9
Section 9	Clause 7	Clause 7	Clause 9	Clause 9	Clause 10
Section 10	Clause 8	Clause 8	Clause 10	Clause 10	Clause 11
Section 11	Clause 9	Clause 9	Clause 11	Clause 11	Clause 12
Section 12	Clause 10	Clause 10	Clause 12	Clause 12	Clause 13
Section 13	Clause 11	Clause 11	Clause 13	Clause 13	Clause 14
Section 14	Clause 12	Clause 12	Clause 14	Clause 14	Clause 15
Section 15	Clause 13	Clause 13	Clause 15	Clause 15	Clause 16
Section 16	Clause 14	Clause 14	Clause 16	Clause 16	Clause 17
Section 17	Clause 15	Clause 15	Clause 17	Clause 17	Clause 18
Section 18	Clause 16	Clause 16	Clause 18	Clause 18	Clause 19
Section 19	Clause 17	Clause 17	Clause 19	Clause 19	Clause 20
Section 20	Clause 18	Clause 18	Clause 20	Clause 20	Clause 21
Section 21	Clause 19	Clause 19	Clause 21	Clause 21	Clause 22
Section 22	Clause 20	Clause 20	Clause 22	Clause 22	Clause 23
Section 23	Clause 21	Clause 21	Clause 23	Clause 23	Clause 24
Section 24	Clause 22	Clause 22	Clause 24	Clause 24	Clause 25
Section 25	Clause 23	Clause 23	Clause 25	Clause 25	Clause 26
Section 26	Clause 24	Clause 24	Clause 26	Clause 26	Clause 27
Section 27	Clause 25	Clause 25	Clause 27	Clause 27	Clause 28
Section 28					Clause 29
Section 29					Clause 30
Section 30	Clause 26	Clause 26	Clause 28	Clause 28	Clause 31

Section 31	Clause 27	Clause 27	Clause 29	Clause 29	Clause 32
Section 32	Clause 28	Clause 28	Clause 30	Clause 30	Clause 33
Section 33	Clause 29	Clause 29	Clause 31	Clause 31	Clause 34
Section 34	Clause 30	Clause 30	Clause 32	Clause 32	Clause 35
Section 35			Clause 33	Clause 33	Clause 36
Section 36			Clause 34	Clause 34	Clause 37
Section 37			Clause 35	Clause 35	Clause 38
Section 38	Clause 31	Clause 31	Clause 36	Clause 36	Clause 39
Section 39	Clause 32	Clause 32	Clause 37	Clause 37	Clause 40
Section 40	Clause 33	Clause 33	Clause 38	Clause 38	Clause 41
Section 41	Clause 34	Clause 34	Clause 39	Clause 39	Clause 42
Section 42	Clause 35	Clause 35	Clause 40	Clause 40	Clause 43
Section 43	Clause 36	Clause 36	Clause 41	Clause 41	Clause 44
Section 44	Clause 37	Clause 37	Clause 42	Clause 42	Clause 45
Section 45	Clause 38	Clause 38	Clause 43	Clause 43	Clause 46
Section 46	Clause 39	Clause 39	Clause 44	Clause 44	Clause 47
Section 47	Clause 40	Clause 40	Clause 45	Clause 45	Clause 48
Section 48	Clause 41	Clause 41	Clause 46	Clause 46	Clause 49
Section 49	Clause 42	Clause 42	Clause 47	Clause 47	Clause 50
Section 50	Clause 43	Clause 43	Clause 48	Clause 48	Clause 51
Section 51	Clause 44	Clause 44	Clause 49	Clause 49	Clause 52
Section 52	Clause 45	Clause 45	Clause 50	Clause 50	Clause 53
Section 53	Clause 46	Clause 46	Clause 51	Clause 51	Clause 54
Section 54	Clause 47	Clause 47	Clause 52	Clause 52	Clause 55
Section 55					Clause 56
Section 56	Clause 48	Clause 48	Clause 53	Clause 53	Clause 57
Section 57	Clause 49	Clause 49	Clause 54	Clause 54	Clause 58
Section 58	Clause 50	Clause 50	Clause 55	Clause 55	Clause 59
Section 59	Clause 51	Clause 51	Clause 56	Clause 56	Clause 60
Section 60	Clause 52	Clause 52	Clause 57	Clause 57	Clause 61
Section 61	Clause 53	Clause 53	Clause 58	Clause 58	Clause 62
Section 62				Clause 59	Clause 63
Section 63	Clause 54	Clause 54	Clause 59	Clause 60	Clause 64
Section 64	Clause 55	Clause 55	Clause 60	Clause 61	Clause 65
Section 65	Clause 56	Clause 56	Clause 61	Clause 62	Clause 66
Section 66	Clause 57	Clause 57	Clause 62	Clause 63	Clause 67
Section 67	Clause 58	Clause 58	Clause 63	Clause 64	Clause 68

Section 68	Clause 59	Clause 59	Clause 64	Clause 65	Clause 69
Section 69	Clause 60	Clause 60	Clause 65	Clause 66	Clause 70
Section 70	Clause 61	Clause 61	Clause 66	Clause 67	Clause 71
Section 71	Clause 62	Clause 62	Clause 67	Clause 68	Clause 72
Section 72	Clause 63	Clause 63	Clause 68	Clause 69	Clause 73
Section 73	Clause 64	Clause 64	Clause 69	Clause 70	Clause 74
Section 74	Clause 65	Clause 65	Clause 70	Clause 71	Clause 75
Section 75	Clause 66	Clause 66	Clause 71	Clause 72	Clause 76
Section 76	Clause 67	Clause 67	Clause 72	Clause 73	Clause 77
Section 77	Clause 68	Clause 68	Clause 73	Clause 74	Clause 78
Section 78	Clause 69	Clause 69	Clause 74	Clause 75	Clause 79
Section 79	Clause 70	Clause 70	Clause 75	Clause 76	Clause 80
Section 80	Clause 71	Clause 71	Clause 76	Clause 77	Clause 81
Section 81	Clause 72	Clause 72	Clause 77	Clause 78	Clause 82
Section 82	Clause 73	Clause 73	Clause 78	Clause 79	Clause 83
Section 83	Clause 74	Clause 74	Clause 79	Clause 80	Clause 84
Section 84	Clause 75	Clause 75	Clause 80	Clause 81	Clause 85
Section 85	Clause 76	Clause 76	Clause 81	Clause 82	Clause 86
Section 86	Clause 77	Clause 77	Clause 82	Clause 83	Clause 87
Section 87	Clause 78	Clause 78	Clause 83	Clause 84	Clause 88
Section 88	Clause 79	Clause 79	Clause 84	Clause 85	Clause 89
Section 89					Clause 90
Section 90	Clause 80	Clause 80	Clause 85	Clause 86	Clause 91
Section 91					Clause 92
Section 92	Clause 81	Clause 81	Clause 86	Clause 87	Clause 93
Section 93	Clause 82	Clause 82	Clause 87	Clause 88	Clause 94
Section 94	Clause 83	Clause 83	Clause 88	Clause 89	Clause 95
Section 95	Clause 84	Clause 84	Clause 89	Clause 90	Clause 96
Section 96	Clause 85	Clause 85	Clause 90	Clause 91	Clause 97
Section 97	Clause 86	Clause 86	Clause 91	Clause 92	Clause 98
Section 98	Clause 87	Clause 87	Clause 92	Clause 93	Clause 99
Section 99	Clause 88	Clause 88	Clause 93	Clause 94	Clause 100
Section 100	Clause 89	Clause 89	Clause 94	Clause 95	Clause 101
Section 101	Clause 90	Clause 90	Clause 95	Clause 96	Clause 102
Section 102	Clause 91	Clause 91	Clause 96	Clause 97	Clause 103
Section 103	Clause 92	Clause 92	Clause 97	Clause 98	Clause 104
Section 104	Clause 93	Clause 93	Clause 98	Clause 99	Clause 105

Section 105	Clause 95	Clause 95	Clause 99	Clause 100	Clause 106
Section 106	Clause 96	Clause 96	Clause 100	Clause 101	Clause 107
Section 107	Clause 117	Clause 117	Clause 101	Clause 102	Clause 108
Section 108	Clause 97	Clause 97	Clause 102	Clause 103	Clause 109
Section 109	Clause 98	Clause 98	Clause 103	Clause 104	Clause 110
Section 110	Clause 99	Clause 99	Clause 104	Clause 105	Clause 111
Section 111			Clause 105	Clause 106	Clause 112
Section 112	Clause 100	Clause 100	Clause 106	Clause 107	Clause 113
Section 113					Clause 114
Section 114					Clause 115
Section 115	Clause 101	Clause 101	Clause 107	Clause 108	Clause 116
Section 116	Clause 102	Clause 102	Clause 108	Clause 109	Clause 117
Section 117	Clause 103	Clause 103	Clause 109	Clause 110	Clause 118
Section 118	Clause 104	Clause 104	Clause 110	Clause 111	Clause 119
Section 119			Clause 111	Clause 112	Clause 120
Section 120			Clause 112	Clause 113	Clause 121
Section 121			Clause 113	Clause 114	Clause 122
Section 122	Clause 105	Clause 105	Clause 114	Clause 115	Clause 123
Section 123	Clause 106	Clause 106	Clause 115	Clause 116	Clause 124
Section 124	Clause 107	Clause 107	Clause 116	Clause 117	Clause 125
Section 125	Clause 108	Clause 108	Clause 117	Clause 118	Clause 126
Section 126	Clause 109	Clause 109	Clause 118	Clause 119	Clause 127
Section 127	Clause 110	Clause 110	Clause 119	Clause 120	Clause 128
Section 128	Clause 111	Clause 111	Clause 120	Clause 121	Clause 129
Section 129	Clause 112	Clause 112	Clause 121	Clause 122	Clause 130
Section 130	Clause 113	Clause 113	Clause 122	Clause 123	Clause 131
Section 131					Clause 132
Section 132	Clause 114	Clause 114	Clause 123	Clause 124	Clause 133
Section 133	Clause 115	Clause 115	Clause 124	Clause 125	Clause 134
Section 134	Clause 116	Clause 116	Clause 125	Clause 126	Clause 135
Section 135	Clause 118	Clause 118	Clause 126	Clause 127	Clause 136
Section 136	Clause 119	Clause 119	Clause 127	Clause 128	Clause 137
Section 137	Clause 120	Clause 120	Clause 128	Clause 129	Clause 138
Section 138	Clause 121	Clause 121	Clause 129	Clause 130	Clause 139
Section 139	Clause 122	Clause 122	Clause 130	Clause 131	Clause 140
Section 140	Clause 123	Clause 123	Clause 131	Clause 132	Clause 141
Section 141	Clause 124	Clause 124	Clause 132	Clause 133	Clause 142

Section 142	Clause 125	Clause 125	Clause 133	Clause 134	Clause 143
Section 143	Clause 126	Clause 126	Clause 134	Clause 135	Clause 144
Section 144	Clause 127	Clause 127	Clause 136	Clause 136	Clause 145
Section 145	Clause 128	Clause 128	Clause 136	Clause 137	Clause 146
Section 146					Clause 147
Section 147	Clause 129	Clause 129	Clause 137	Clause 138	Clause 148
Section 148	Clause 130	Clause 130	Clause 138	Clause 139	Clause 149
Section 149	Clause 131	Clause 131	Clause 139	Clause 140	Clause 150
Section 150	Clause 132	Clause 132	Clause 140	Clause 141	Clause 151
Section 151	Clause 133	Clause 133	Clause 141	Clause 142	Clause 152
Section 152	Clause 134	Clause 134	Clause 142	Clause 143	Clause 153
Section 153	Clause 135	Clause 135	Clause 143	Clause 144	Clause 154
Section 154					Clause 155
Section 155					Clause 156
Section 156	Clause 136	Clause 136	Clause 144	Clause 145	Clause 157
Section 157	Clause 137	Clause 137	Clause 145	Clause 146	Clause 158
Section 158	Clause 138	Clause 138	Clause 146	Clause 147	Clause 159
Section 159	Clause 139	Clause 139	Clause 147	Clause 148	Clause 160
Section 160	Clause 140	Clause 140	Clause 148	Clause 149	Clause 161
Section 161	Clause 141	Clause 141	Clause 149	Clause 150	Clause 162
Section 162	Clause 142	Clause 142	Clause 150	Clause 151	Clause 163
Section 163	Clause 143	Clause 143	Clause 151	Clause 152	Clause 164
Section 164	Clause 144	Clause 144	Clause 152	Clause 153	Clause 165
Section 165					Clause 166
Section 166	Clause 145	Clause 145	Clause 153	Clause 154	Clause 167
Section 167	Clause 146	Clause 146	Clause 154	Clause 155	Clause 168
Section 168	Clause 147	Clause 147	Clause 155	Clause 156	Clause 169
Section 169	Clause 148	Clause 148	Clause 156	Clause 157	Clause 170
Section 170	Clause 149	Clause 149	Clause 157	Clause 158	Clause 171
Section 171	Clause 150	Clause 150	Clause 158	Clause 159	Clause 172
Section 172	Clause 151	Clause 151	Clause 159	Clause 160	Clause 173
Section 173					Clause 174
Section 174	Clause 152	Clause 152	Clause 160	Clause 161	Clause 175
Section 175	Clause 153	Clause 153	Clause 161	Clause 162	Clause 176
Section 176	Clause 154	Clause 154	Clause 162	Clause 163	Clause 177
Section 177	Clause 155	Clause 155	Clause 163	Clause 164	Clause 178
Section 178	Clause 156	Clause 156	Clause 164	Clause 165	Clause 179

Section 179	Clause 157	Clause 157	Clause 165	Clause 166	Clause 180
Section 180	Clause 158	Clause 158	Clause 166	Clause 167	Clause 181
Section 181	Clause 159	Clause 159	Clause 167	Clause 168	Clause 182
Section 182	Clause 160	Clause 160	Clause 168	Clause 169	Clause 183
Section 183	Clause 161	Clause 161	Clause 169	Clause 170	Clause 184
Section 184	Clause 162	Clause 162	Clause 170	Clause 171	Clause 185
Section 185	Clause 163	Clause 163	Clause 171	Clause 172	Clause 186
Section 186	Clause 164	Clause 164	Clause 172	Clause 173	Clause 187
Section 187					Clause 188
Section 188	Clause 165	Clause 165	Clause 173	Clause 174	Clause 189
Section 189	Clause 166	Clause 166	Clause 174	Clause 175	Clause 190
Section 190	Clause 167	Clause 167	Clause 175	Clause 176	Clause 191
Section 191	Clause 168	Clause 168	Clause 176	Clause 177	Clause 192
Section 192	Clause 169	Clause 169	Clause 177	Clause 178	Clause 193
Section 193	Clause 170	Clause 170	Clause 178	Clause 179	Clause 194
Section 194	Clause 171	Clause 171	Clause 179	Clause 180	Clause 195
Section 195					Clause 196
Section 196					Clause 197
Section 197	Clause 172	Clause 172	Clause 180	Clause 181	Clause 198
Section 198	Clause 173	Clause 173	Clause 181	Clause 182	Clause 199
Section 199	Clause 174	Clause 174	Clause 182	Clause 183	Clause 200
Section 200	Clause 175	Clause 175	Clause 183	Clause 184	Clause 201
Section 201	Clause 176	Clause 176	Clause 184	Clause 185	Clause 202
Section 202				Clause 186	Clause 203
Section 203					Clause 204
Section 204	Clause 177	Clause 177	Clause 185	Clause 187	Clause 205
Section 205	Clause 178	Clause 178	Clause 186	Clause 188	Clause 206
Section 206			Clause 187	Clause 189	Clause 207
Section 207					Clause 208
Section 208	Clause 179	Clause 179	Clause 188	Clause 190	Clause 209
Section 209	Clause 180	Clause 180	Clause 189	Clause 191	Clause 210
Section 210	Clause 181	Clause 181	Clause 190	Clause 192	Clause 211
Section 211	Clause 182	Clause 182	Clause 191	Clause 193	Clause 212
Section 212	Clause 183	Clause 183	Clause 192	Clause 194	Clause 213
Section 213	Clause 184	Clause 184	Clause 193	Clause 195	Clause 214
Section 214	Clause 185	Clause 185	Clause 194	Clause 196	Clause 215
Section 215	Clause 186	Clause 186	Clause 195	Clause 197	Clause 216

Section 216					Clause 217
Section 217	Clause 187	Clause 187	Clause 196	Clause 198	Clause 218
Section 218	Clause 188	Clause 188	Clause 197	Clause 199	Clause 219
Section 219	Clause 189	Clause 189	Clause 198	Clause 200	Clause 220
Section 220	Clause 190	Clause 190	Clause 199	Clause 201	Clause 221
Section 221	Clause 191	Clause 191	Clause 200	Clause 202	Clause 222
Section 222					Clause 223
Section 223					Clause 224
Section 224					Clause 225
Section 225	Clause 192	Clause 192	Clause 201	Clause 203	Clause 226
Section 226	Clause 193	Clause 193	Clause 202	Clause 204	Clause 227
Section 227	Clause 194	Clause 194	Clause 203	Clause 205	Clause 228
Section 228	Clause 195	Clause 195	Clause 204	Clause 206	Clause 229
Section 229	Clause 196	Clause 196	Clause 205	Clause 207	Clause 230
Section 230	Clause 197	Clause 197	Clause 206	Clause 208	Clause 231
Section 231	Clause 198	Clause 198	Clause 207	Clause 209	Clause 232
Section 232	Clause 199	Clause 199	Clause 208	Clause 210	Clause 233
Section 233	Clause 200	Clause 200	Clause 209	Clause 211	Clause 234
Section 234	Clause 201	Clause 201	Clause 210	Clause 212	Clause 235
Section 235	Clause 202	Clause 202	Clause 211	Clause 213	Clause 236
Section 236				Clause 214	Clause 237
Section 237	Clause 203	Clause 203	Clause 212	Clause 215	Clause 238
Section 238	Clause 204	Clause 204	Clause 213	Clause 216	Clause 239
Section 239	Clause 205	Clause 205	Clause 214	Clause 217	Clause 240
Section 240	Clause 206	Clause 206	Clause 215	Clause 218	Clause 241
Section 241	Clause 207	Clause 207	Clause 216	Clause 219	Clause 242
Section 242	Clause 208	Clause 208	Clause 217	Clause 220	Clause 243
Section 243	Clause 209	Clause 209	Clause 218	Clause 221	Clause 244
Section 244	Clause 210	Clause 210	Clause 219	Clause 222	Clause 245
Section 245	Clause 211	Clause 211	Clause 220	Clause 223	Clause 246
Section 246					Clause 247
Section 247					Clause 248
Section 248	Clause 212	Clause 212	Clause 221	Clause 224	Clause 249
Section 249	Clause 213	Clause 213	Clause 222	Clause 225	Clause 250
Section 250	Clause 214	Clause 214	Clause 223	Clause 226	Clause 251
Section 251	Clause 215	Clause 215	Clause 224	Clause 227	Clause 252
Section 252	Clause 216	Clause 216	Clause 225	Clause 228	Clause 253

Section 253	Clause 217	Clause 217	Clause 226	Clause 229	Clause 254
Section 254			Clause 227	Clause 230	Clause 255
Section 255	Clause 218	Clause 218	Clause 228	Clause 231	Clause 256
Section 256	Clause 219	Clause 219	Clause 229	Clause 232	Clause 257
Section 257	Clause 220	Clause 220	Clause 230	Clause 233	Clause 258
Section 258				Clause 234	Clause 259
Section 259	Clause 221	Clause 221	Clause 231	Clause 235	Clause 260
Section 260	Clause 222	Clause 222	Clause 232	Clause 236	Clause 261
Section 261	Clause 223	Clause 223	Clause 233	Clause 237	Clause 262
Section 262	Clause 224	Clause 224	Clause 234	Clause 238	Clause 263
Section 263	Clause 225	Clause 225	Clause 235	Clause 239	Clause 264
Section 264					Clause 265
Section 265	Clause 226	Clause 226	Clause 236	Clause 240	Clause 266
Section 266	Clause 227	Clause 227	Clause 237	Clause 241	Clause 267
Section 267	Clause 228	Clause 228	Clause 238	Clause 242	Clause 268
Section 268	Clause 229	Clause 229	Clause 239	Clause 243	Clause 269
Section 269	Clause 230	Clause 230	Clause 240	Clause 244	Clause 270
Section 270	Clause 231	Clause 231	Clause 241	Clause 245	Clause 271
Section 271	Clause 232	Clause 232	Clause 242	Clause 246	Clause 272
Section 272	Clause 233	Clause 233	Clause 243	Clause 247	Clause 273
Schedule 1	Schedule 1	Schedule 1	Schedule 1	Schedule 1	Schedule 1
Schedule 2	Schedule 2	Schedule 2	Schedule 2	Schedule 2	Schedule 2
Schedule 3	Schedule 3	Schedule 3	Schedule 3	Schedule 3	Schedule 3
Schedule 4	Schedule 4	Schedule 4	Schedule 4	Schedule 4	Schedule 4
Schedule 5	Schedule 5	Schedule 5	Schedule 5	Schedule 5	Schedule 5
Schedule 6	Schedule 6	Schedule 6	Schedule 6	Schedule 6	Schedule 6
Schedule 7	Schedule 7	Schedule 7	Schedule 7	Schedule 7	Schedule 7
Schedule 8	Schedule 8	Schedule 8	Schedule 8	Schedule 8	Schedule 8
Schedule 9	Schedule 9	Schedule 9	Schedule 9	Schedule 9	Schedule 9
Schedule 10	Schedule 10	Schedule 10	Schedule 10	Schedule 10	Schedule 10

Printed and published in the UK by The Stationery Office Limited under the authority and superintendence of Carol Tullo, Controller of Her Majesty's Stationery Office and Queen's Printer of Acts of Parliament.

tso
part of Williams Lea Tag

Published by TSO (The Stationery Office), part of Williams Lea Tag, and available from:

Online
www.tsoshop.co.uk

Mail, Telephone, Fax & E-mail
TSO
PO Box 29, Norwich, NR3 1GN
Telephone orders/General enquiries: 0333 202 5070
Fax orders: 0333 202 5080
E-mail: customer.services@tso.co.uk
Textphone: 0333 202 5077

TSO@Blackwell and other Accredited Agents

ISBN 978-0-10-560051-0
9 780105 600510