

INVESTIGATORY POWERS BILL

EXPLANATORY NOTES

What these notes do

These Explanatory Notes relate to the Investigatory Powers Bill as introduced in the House of Commons on 19 May 2016 (Bill 2).

- These Explanatory Notes have been produced by the Home Office in order to assist the reader of the Bill and to help inform debate on it. They do not form part of the Bill and have not been endorsed by Parliament.
- These Explanatory Notes explain what each part of the Bill will mean in practice; provide background information on the development of policy; and provide additional information on how the Bill will affect existing legislation in this area.
- These Explanatory Notes might best be read alongside the Bill. They are not, and are not intended to be, a comprehensive description of the Bill.

Table of Contents

| Subject | Page of these Notes |
|--|---------------------|
| Overview of the Bill | 7 |
| Policy background | 7 |
| Legal background | 10 |
| European law | 11 |
| Territorial extent and application | 12 |
| Commentary on provisions of Bill | 13 |
| Part 1: General Privacy Protections | 13 |
| Clause 1: Overview of the Act | 13 |
| Clause 2: Offence of unlawful interception | 13 |
| Clause 3: Definition of "interception" etc. | 13 |
| Clause 4: Conduct that is not interception | 14 |
| Clause 5: Definition of "lawful authority" | 14 |
| Clause 6: Monetary penalties for certain unlawful interceptions | 14 |
| Schedule 1: Monetary Penalty Notices | 15 |
| Clause 7: Restrictions on requesting interception by overseas authorities | 15 |
| Clause 8: Restriction on requesting assistance under mutual assistance agreements etc. | 15 |
| Clause 9: Offence of unlawfully obtaining communications data | 15 |
| Clause 10: Abolition or restriction of certain powers to obtain communications data | 15 |
| Schedule 2: Abolition of disclosure powers | 16 |
| Clause 11: Mandatory use of equipment interference warrants | 16 |
| Clause 12: Restriction on use of section 93 of the Police Act 1997 | 16 |
| Part 2: Lawful interception of communications | 16 |
| Chapter 1: Interception and examination with a warrant | 17 |
| Clause 13: Warrants that may be issued under this Chapter | 17 |
| Clause 14: Obtaining secondary data | 17 |
| Clause 15: Subject-matter of warrants | 18 |
| Clause 16: Persons who may apply for issue of a warrant | 18 |
| Clause 17: Power of Secretary of State to issue warrants | 18 |
| Clause 18: Grounds on which warrants may be issued by Secretary of State | 18 |
| Clause 19: Power of Scottish Ministers to issue warrants | 18 |
| Clause 20: "Relevant Scottish applications" | 19 |
| Clause 21: Approval of warrants by Judicial Commissioners | 19 |
| Clause 22: Approval of warrants issued in urgent cases | 19 |
| Clause 23: Failure to approve warrant issued in urgent case | 19 |
| Clause 24: Members of Parliament etc. | 20 |
| Clause 25: Items subject to legal privilege | 20 |
| Clause 26: Decisions to issue warrants to be taken personally by Ministers | 20 |
| Clause 27: Requirements that must be met by warrants | 20 |
| Clause 28: Duration of warrants | 21 |
| Clause 29: Renewal of warrants | 21 |
| Clause 30: Modification of warrants | 21 |

These Explanatory Notes relate to the Investigatory Powers Bill as introduced in the House of Commons on 19 May 2016 (Bill 2)

| | |
|---|-----------|
| Clause 31: Approval of major modifications made in urgent cases | 21 |
| Clause 32: Cancellation of warrants | 21 |
| Clause 33: Special rules for certain mutual assistance warrants | 21 |
| Clause 34: Implementation of warrants | 22 |
| Clause 35: Service of warrants outside the United Kingdom | 22 |
| Clause 36: Duty of operators to assist with implementation | 22 |
| Chapter 2: Other forms of lawful interception | 22 |
| Clause 37: Interception with the consent of the sender or recipient | 22 |
| Clause 38: Interception by providers of postal or telecommunication services | 23 |
| Clause 39: Interception by businesses etc. for monitoring and record-keeping purposes | 23 |
| Clause 40: Postal services: interception for enforcement purposes | 23 |
| Clause 41: Interception by OFCOM in connection with wireless telegraphy | 23 |
| Clause 42: Interception in prisons | 23 |
| Clause 43: Interception in psychiatric hospitals etc. | 24 |
| Clause 44: Interception in immigration detention facilities | 24 |
| Clause 45: Interception in accordance with overseas requests | 24 |
| Chapter 3: Other provisions about interception | 24 |
| Clause 46: Safeguards relating to retention and disclosure of material | 24 |
| Clause 47: Safeguards relating to disclosure of material overseas | 24 |
| Clause 48: Exclusion of matters from legal proceedings | 24 |
| Schedule 3: Exceptions to section 48 | 24 |
| Clause 49: Duty not to make unauthorised disclosures | 26 |
| Clause 50: Section 49: meaning of “excepted disclosure” | 26 |
| Clause 51: Offence of making unauthorised disclosures | 26 |
| Clause 52: Part 2: interpretation | 26 |
| Part 3: Authorisations for obtaining communications data | 26 |
| Clause 53: Power to grant authorisations | 26 |
| Clause 54: Additional restrictions on grant of authorisations | 27 |
| Clause 55: Procedure for authorisations and authorised notices | 28 |
| Clause 56: Duration and cancellation of authorisations and notices | 28 |
| Clause 57: Duties of telecommunications operators in relation to authorisations | 29 |
| Clause 58: Filtering arrangements for obtaining data | 29 |
| Clause 59: Use of filtering arrangements in pursuance of an authorisation | 30 |
| Clause 60: Duties in connection with operation of filtering arrangements | 30 |
| Clause 61: Relevant public authorities and designated senior officers | 31 |
| Schedule 4: Relevant public authorities | 32 |
| Clause 62: Power to modify section 61 and Schedule 4 | 32 |
| Clause 63: Certain regulations under section 62: supplementary | 32 |
| Clause 64: Local authorities as relevant public authorities | 33 |
| Clause 65: Requirement to be party to collaboration agreement | 33 |
| Clause 66: Judicial approval for local authority authorisations | 33 |
| Clause 67: Use of a single point of contact | 33 |
| Clause 68: Commissioner approval for authorisations to identify or confirm journalistic sources | 34 |
| Clauses 69 and 70: Collaboration agreements | 34 |
| Clause 71: Police collaboration agreements | 34 |
| Clause 72: Lawfulness of conduct authorised by this Part | 34 |
| Clause 73: Offence of making unauthorised disclosure | 35 |
| Clause 74: Certain transfer and agency arrangements with public authorities | 35 |
| Schedule 5: Transfer and agency arrangements with public authorities: further provisions | 35 |
| Clause 75: Applications of Part 3 to postal operators and postal services | 35 |
| Clause 76: Extra-territorial applications of Part 3 | 36 |
| Clause 77: Part 3: interpretation | 36 |
| Part 4: Retention of communications data | 36 |

These Explanatory Notes relate to the Investigatory Powers Bill as introduced in the House of Commons on 19 May 2016 (Bill 2)

| | |
|--|-----------|
| Clause 78: Powers to require retention of certain data | 36 |
| Clause 79: Matters to be taken into account before giving retention notices | 36 |
| Clause 80: Review by the Secretary of State | 36 |
| Clause 81: Data integrity and security | 37 |
| Clause 82: Disclosure of retained data | 37 |
| Clause 83: Variation or revocation of notices | 37 |
| Clause 84: Enforcement of notices and certain other requirements and restrictions | 37 |
| Clause 85: Application of Part 4 to postal operators and postal services | 37 |
| Clause 86: Extra-territorial application of Part 4 | 37 |
| Clause 87: Part 4: interpretation | 38 |
| Part 5: Equipment interference | 38 |
| Clause 88: Warrants under this Part: general | 38 |
| Clause 89: Meaning of "equipment data" | 38 |
| Clause 90: Subject-matter of warrants | 39 |
| Clause 91: Power to issue warrants to intelligence services: the Secretary of State | 40 |
| Clause 92: Power to issue warrants to intelligence services: the Scottish Ministers | 40 |
| Clause 93: Power to issue warrants to the Chief of Defence Intelligence | 40 |
| Clause 94: Members of Parliament etc. | 41 |
| Clause 95: Decision to issue warrants under sections 91 to 93 be taken personally by Ministers | 41 |
| Clause 96: Power to issue warrants to law enforcement officers | 41 |
| Schedule 6: Issue of warrants under section 96 etc: table | 42 |
| Clause 97: Approval of warrants by Judicial Commissioners | 42 |
| Clause 98: Approval of warrants issued in urgent cases | 42 |
| Clause 99: Failure to approve warrant issued in urgent case | 43 |
| Clause 100: Items subject to legal privilege | 43 |
| Clause 101: Requirements which must be met by warrants | 43 |
| Clause 102: Duration of warrants | 44 |
| Clause 103: Renewal of warrants | 44 |
| Clause 104: Modifications of warrants by the Secretary of State or Scottish Ministers | 44 |
| Clause 105: Approval of modifications under section 104 made in urgent cases | 45 |
| Clause 106: Modification of warrants issued by law enforcement chiefs | 45 |
| Clause 107: Approval of modification under section 106 in urgent cases | 45 |
| Clause 108: Cancellation of warrants | 45 |
| Clause 109: Implementation of warrants | 46 |
| Clause 110: Service of warrants outside the United Kingdom | 46 |
| Clause 111: Duty of telecommunications operators to assist with implementation | 46 |
| Clause 112: Safeguards relating to the retention and disclosure of material | 46 |
| Clause 113: Safeguards relating to disclosure of material overseas | 47 |
| Clause 114: Duty not to make unauthorised disclosures | 47 |
| Clause 115: Section 114: meaning of "excepted" disclosure | 47 |
| Clause 116: Offence of making unauthorised disclosure | 47 |
| Clause 117: Restriction on issue of warrants to certain law enforcement officers | 47 |
| Clause 118: Part 5: Interpretation | 48 |
| Chapter 1: Bulk interception warrants | 48 |
| Clause 119: Bulk interception warrants | 48 |
| Clause 120: Obtaining secondary data | 49 |
| Clause 121: Power to issue bulk interception warrants | 49 |
| Clause 122: Additional requirements in respect of warrants affecting overseas operators | 50 |
| Clause 123: Approval of warrants by Judicial Commissioners | 50 |
| Clause 124: Decisions to issue warrants to be taken personally by Secretary of State | 50 |
| Clause 125: Requirements that must be met by warrants | 50 |
| Clause 126: Duration of warrants | 51 |
| Clause 127: Renewal of warrants | 51 |
| Clause 128: Modification of warrants | 51 |

These Explanatory Notes relate to the Investigatory Powers Bill as introduced in the House of Commons on 19 May 2016 (Bill 2)

| | |
|--|-----------|
| Clause 129: Approval of major modifications made in urgent cases | 51 |
| Clause 130: Cancellation of warrants | 51 |
| Clause 131: Implementation of warrants | 52 |
| Clause 132: Safeguards relating to retention and disclosure of material | 52 |
| Clause 133: Safeguards relating to disclosure of material overseas | 52 |
| Clause 134: Safeguards relating to examination of material | 52 |
| Clause 135: Additional safeguards for items subject to legal privilege | 53 |
| Clause 136: Application of other restrictions in relation to warrants | 53 |
| Clause 137: Chapter 1: interpretation | 53 |
| Chapter 2: Bulk acquisition warrants | 53 |
| Clause 138: Power to issue bulk acquisition warrants | 53 |
| Clause 139: Approval of warrants by Judicial Commissioners | 54 |
| Clause 140: Decisions to issue warrants to be taken personally by Secretary of State | 54 |
| Clause 141: Requirements that must be met by warrants | 54 |
| Clause 142: Duration of warrants | 55 |
| Clause 143: Renewal of warrants | 55 |
| Clause 144: Modification of warrants | 55 |
| Clause 145: Approval of major modifications made in urgent cases | 55 |
| Clause 146: Cancellation of warrants | 55 |
| Clause 147: Implementation of warrants | 56 |
| Clause 148: Service of warrants outside the United Kingdom | 56 |
| Clause 149: Duty of operators to assist with implementation | 56 |
| Clause 150: Safeguards relating to the retention and disclosure of data | 56 |
| Clause 151: Safeguards relating to examination of data | 56 |
| Clause 152: Offence of making unauthorised disclosure | 56 |
| Clause 153: Chapter 2: interpretation | 56 |
| Chapter 3: Bulk equipment interference warrants | 56 |
| Clause 154: Bulk equipment interference warrants: general | 56 |
| Clause 155: Meaning of “equipment data” | 57 |
| Clause 156: Power to issue bulk equipment interference warrants | 58 |
| Clause 157: Approval of warrants by Judicial Commissioners | 58 |
| Clause 158: Approval of warrants issued in urgent cases | 58 |
| Clause 159: Failure to approve warrant issued in urgent case | 58 |
| Clause 160: Decisions to issue warrants to be taken personally by Secretary of State | 59 |
| Clause 161: Requirements that must be met by warrants | 59 |
| Clause 162: Duration of warrants | 59 |
| Clause 163: Renewal of warrants | 59 |
| Clause 164: Modification of warrants | 59 |
| Clause 165: Approval of major modifications made in urgent cases | 60 |
| Clause 166: Cancellation of warrants | 60 |
| Clause 167: Implementation of warrants | 60 |
| Clause 168: Safeguards relating to retention and disclosure of material | 61 |
| Clause 169: Safeguards relating to disclosure of material overseas | 61 |
| Clause 170: Safeguards relating to examination of material etc. | 61 |
| Clause 171: Additional safeguards for items subject to legal privilege | 61 |
| Clause 172: Application of other restrictions in relation to warrants | 62 |
| Clause 173: Chapter 3: interpretation | 62 |
| Part 7: Bulk personal datasets | 62 |
| Clause 174: Bulk personal datasets: interpretation | 62 |
| Clause 175: Requirement for authorisation by warrant: general | 62 |
| Clause 176: Exceptions to Section 175(1) and (2) | 62 |
| Clause 177: Class BPD warrants | 63 |
| Clause 178: Specific BPD warrants | 63 |
| Clause 179: Approval of warrants by Judicial Commissioners | 64 |

These Explanatory Notes relate to the Investigatory Powers Bill as introduced in the House of Commons on 19 May 2016 (Bill 2)

| | |
|--|-----------|
| Clause 180: Approval of specific BPD warrants issued in urgent cases | 64 |
| Clause 181: Failure to approve specific BPD warrant issued in urgent case | 64 |
| Clause 182: Decisions to issue warrants to be taken personally by Secretary of State | 65 |
| Clause 183: Requirements that must be met by warrants | 65 |
| Clause 184: Duration of warrants | 65 |
| Clause 185: Renewal of warrants | 65 |
| Clause 186: Modification of warrants | 65 |
| Clause 187: Approval of major modifications made in urgent cases | 66 |
| Clause 188: Cancellation of warrants | 66 |
| Clause 189: Non-Renewal or cancellation of BPD warrants | 66 |
| Clause 190: Initial Examination: time limits | 67 |
| Clause 191: Safeguards relating to the examination of bulk personal datasets | 67 |
| Clause 192: Application of Part to bulk personal datasets obtained under this Act | 67 |
| Clause 193: Part 7: interpretation | 68 |
| Part 8: Oversight arrangements | 68 |
| Chapter 1: Investigatory Powers Commissioner and other Judicial Commissioners | 68 |
| Clause 194: Investigatory Powers Commissioner and other Judicial Commissioners | 68 |
| Clause 195: Terms and conditions of appointment | 68 |
| Clause 196: Main oversight functions | 68 |
| Clause 197: Additional directed oversight functions | 69 |
| Clause 198: Error reporting | 69 |
| Clause 199: Additional functions under this Part | 70 |
| Clause 200: Functions under other Parts and other enactments | 70 |
| Clause 201: Annual and other reports | 70 |
| Clause 202: Investigation and information powers | 70 |
| Clause 203: Information gateway | 70 |
| Clause 204: Funding, staff and facilities | 71 |
| Clause 205: Power to modify functions | 71 |
| Clause 206: Abolition of existing oversight bodies | 71 |
| Chapter 2: Other arrangements | 71 |
| Clause 207: Codes of practice | 71 |
| Schedule 7: Codes of practice | 71 |
| Clause 208: Right of appeal from the Tribunal | 72 |
| Clause 209: Functions of Tribunal in relation to this Act | 73 |
| Clause 210: Oversight by Information Commissioner in relation to Part 4 | 73 |
| Clause 211: Technical Advisory Board | 73 |
| Part 9: Miscellaneous and general provisions | 73 |
| Chapter 1: Miscellaneous | 73 |
| Clause 212: Combination of warrants and authorisations | 73 |
| Schedule 8: Combination of warrants | 73 |
| Clause 213: Payments towards certain compliance costs | 75 |
| Clause 214: Power to develop compliance systems etc. | 75 |
| Clause 215: Amendments of the Intelligence Services Act 1994 | 75 |
| Clause 216: National security notices | 76 |
| Clause 217: Maintenance of technical capability | 76 |
| Clause 218: Further provision about notices under section 216 or 217 | 77 |
| Clause 219: Variation and revocation of notices | 77 |
| Clause 220: Review by the Secretary of State | 77 |
| Clause 221: Amendments of the Wireless Telegraphy Act 2006 | 78 |
| Chapter 2: General | 78 |
| Clause 222: Review of operation of Act | 78 |
| Clause 223: Telecommunications definitions | 78 |
| Clause 224: Postal definitions | 79 |

These Explanatory Notes relate to the Investigatory Powers Bill as introduced in the House of Commons on 19 May 2016 (Bill 2)

| | |
|---|-----------|
| Clause 225: General definitions | 79 |
| Clause 226: Index of defined expressions | 79 |
| Clause 227: Offences by bodies corporate etc. | 79 |
| Clause 228: Regulations | 79 |
| Clause 229: Enhanced affirmative procedure | 79 |
| Clause 230: Financial provisions | 79 |
| Clause 231: Transitional, transitory or saving provision | 79 |
| Schedule 9: Transitional, transitory and saving provision | 80 |
| Clause 232: Minor and consequential provision | 80 |
| Schedule 10: Minor and consequential provision | 80 |
| Clause 233: Commencement, extent and short title | 81 |
| Commencement | 81 |
| Financial implications of the Bill | 81 |
| Compatibility with the European Convention on Human Rights | 82 |
| Related documents | 82 |
| Annex A - Territorial extent and application in the United Kingdom | 84 |

Overview of the Bill

- 1 The Investigatory Powers Bill 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, equipment interference for obtaining communications and other data. It will not be lawful to exercise such powers other than as provided for by the Bill. The Bill also makes provision relating to the security and intelligence agencies' retention and examination of bulk personal datasets.
- 2 Section 7 of the Data Retention and Investigatory Powers Act 2014 required David Anderson QC, in his capacity as the Independent Reviewer of Terrorism Legislation, to conduct a review of existing laws relating to investigatory powers. David Anderson published his review in June 2015. This Bill responds to the recommendations made in that review and those of the reviews undertaken by the Intelligence and Security Committee of Parliament (ISC) and the Panel of the Independent Surveillance Review convened by the Royal United Services Institute (RUSI). All three reviews agreed that investigatory powers remain essential in tackling the current and evolving threats to the United Kingdom.
- 3 The draft Bill was published for pre-legislative scrutiny by a Joint Committee of Parliament on 4 November 2015. The Committee took evidence from a broad section of witness including the Government, Parliamentarians, law enforcement, judicial commissioners, lawyers, journalists, academics, civil society groups, communications service providers and charities' and victims' groups. It also published 148 submissions of written evidence of over 1,500 pages. The Committee's report, including its recommendations, was published on 11 February 2016.
- 4 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.
- 5 Following pre-legislative scrutiny, the Government introduced a revised Bill, accompanied by further explanatory material, on 1 March 2016. The Bill was carried over into the second session and reintroduced in the House of Commons on 19 May 2016.

Policy background

- 6 The Government is introducing legislation to replace the emergency legislation passed in July 2014, the Data Retention and Investigatory Powers Act 2014 (DRIPA), which is 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 Investigatory Powers Bill updates the legal framework governing the state's ability to acquire communications and data about communications.
- 7 The Bill will govern the powers available to the state to obtain communications and communications data in the UK. It will provide consistent statutory safeguards and will clarify

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 Bill will also create a new Investigatory Powers Commissioner to oversee the use of these powers. Finally, the Bill will provide a new power, requiring communications services providers to retain internet connection records when given a notice by the Secretary of State.

- 8 The Bill is in nine parts.
- 9 Part 1 asserts the privacy of communications and provides for related offences. It defines interception and sets out the offences of unlawful interception and unlawful acquisition of communications data and the penalties for committing such offences. It also references the use of powers to acquire stored communications such as an email stored on a web-based server or a voicemail.
- 10 Part 2 provides for targeted interception: acquiring the content of communications. This power is currently provided for under the Regulation of the Investigatory Powers Act 2000 (RIPA). The Bill will repeal and replace the existing interception powers in Part 1, Chapter 1 of RIPA with a new targeted interception power. It will provide for the targeted interception of communications by a limited number of public authorities for a limited number of purposes when a warrant is in place. It will clarify that in all circumstances, when law enforcement or the security and intelligence agencies wish to intercept the communications of a person believed to be in the UK, or examine the communications of a person believed to be in the UK that have been collected in bulk, a targeted interception warrant or targeted examination warrant must be sought. It also lists the other limited circumstances in which interception (including that not undertaken by law enforcement or security and intelligence agencies) can be lawful. It includes the interception powers previously provided for in the Wireless Telegraphy Act 2006.
- 11 Part 3 concerns authorisations for acquiring communications data: the 'who', 'when', 'where' and 'how' of a communication. The Bill will provide powers for public authorities to acquire communications data, replacing and largely replicating the effect of Chapter 2 of Part 1 of RIPA. The classes of communications data will be redefined so that they reflect current technology. The Bill will require requests for communications data to be made on a case by case basis so that access is permitted only when authorised by designated senior officers (who will be, subject to some specific exceptions, independent from investigations), on the advice of an expert Single Point of Contact (SPoC). Minor public authorities will be required to share SPoCs. The individual requests must be in respect of the statutory purposes and must be considered necessary and proportionate by a designated senior officer. The Bill will set out the public authorities that will have access to communications data in future, permitting bodies to retain powers to access to communications data only where a clear case has been made.
- 12 Part 4 covers the retention of communications data. The existing statutory regime by which public telecommunications operators can be required to retain communications data will be broadly replicated, replacing section 1 of DRIPA. It will provide for the Secretary of State to require communications service providers to retain relevant communications data for one or more of the statutory purposes for a period that must not exceed twelve months. It specifies a number of safeguards in respect of data retention, for example the matters that must be considered before the giving of a retention notice, oversight arrangements and means of redress. The Bill also provides a new power for the retention of, and access to, internet connection records (ICRs) (the records captured by a network access provider of the internet services with which a person or device interacts).

- 13 Part 5 concerns equipment interference: interfering with computer equipment to obtain communications, information or equipment data. This is currently provided for the security and intelligence agencies under the Intelligence Services Act 1994 (ISA) and, for law enforcement agencies under the Police Act 1997. The Bill will provide a bespoke statutory framework for the ability of the security and intelligence agencies, Armed Forces and law enforcement agencies to undertake equipment interference to obtain communications and other information. Interference with equipment where the primary purpose is not to acquire communications, equipment data or other information may continue to be authorised under the ISA and the Police Act 1997.
- 14 Part 6 contains powers for the security and intelligence agencies to intercept communications, conduct equipment interference and to obtain communications data in bulk. The Bill will provide for a new 'bulk acquisition' warrant for the security and intelligence agencies to obtain communications data. This replaces the provision at section 94 of the Telecommunications Act 1984, which will be repealed. The Bill will allow the security and intelligence agencies to intercept communications in bulk, where the communications are overseas-related. This will replace the power to intercept "external communications" in Chapter 1, Part 1 of RIPA. Where it is not necessary to obtain the content of such communications, the Bill will provide the Secretary of State with the power to issue, subject to Judicial Commissioner approval, a warrant for the acquisition of secondary data only. The warrant will also pre-authorise the purposes for which communications acquired under a bulk warrant may be examined – looked at or listened to. A bulk equipment interference power will provide the statutory basis for overseas-related equipment interference activity undertaken by the security and intelligence agencies. All bulk powers will be underpinned by safeguards equivalent to the bulk interception regime for the handling, destruction and retention of information.
- 15 Part 7 provides clarity and additional safeguards for the security and intelligence agencies' retention and examination of Bulk Personal Datasets (BPD). The security and intelligence agencies have existing statutory powers under ISA and the Security Service Act 1989 (SSA) which enable them to acquire and access datasets containing personal data about a large number of individuals, many of whom are not of interest to the agencies. The Bill will not create a new power but bring greater transparency to this important capability and provide for enhanced safeguards. Retention and examination of bulk personal datasets by the security and intelligence agencies will be subject to an authorisation process where the Secretary of State will issue either a 'class' or 'specific' warrant which must be approved by a Judicial Commissioner before it can be issued.
- 16 Part 8 sets out new oversight regime arrangements which will replace the three existing Commissioners (the Intelligence Services Commissioner, the Interception of Communications Commissioner and the Chief Surveillance Commissioner, and the Investigatory Powers Commissioner for Northern Ireland who is provided for in law) with a single new Commissioner, the Investigatory Powers Commissioner (IPC). The Investigatory Powers Commissioner, a senior judge, will be supported by a number of Judicial Commissioners undertaking either authorisation or oversight and inspection functions. The Investigatory Powers Commissioner will have significantly greater powers and resources compared to the current oversight regime. The IPC will be a more visible body, providing robust oversight and scrutiny of the use of investigatory powers by a wide range of public authorities. The Investigatory Powers Commissioner will be able to draw on extensive legal and technical expertise. The Investigatory Powers Commissioner will have to report annually and be able to make ad hoc reports on matters that they consider appropriate.
- 17 The Bill will also create a domestic right of appeal from decisions or determinations of the Investigatory Powers Tribunal (IPT) to the Court of Appeal in England and Wales, the Court of

Session or the Court of Appeal in Northern Ireland. It will be possible for appeals to be heard wholly or partly in closed material proceedings (CMP), if it is necessary for the appeal court to review information which was considered by the IPT in closed session.

- 18 The Bill will provide for statutory Codes of Practice providing further guidance on the powers and duties in the Bill, to which public authorities and providers must have regard when carrying out these powers and duties.
- 19 Part 9 contains General and Final Provisions. This includes provision relating to obligations that may be placed on communications service providers to assist in giving effect to warrants and authorisations under the Bill, as well as providing a new framework for obligations previously provided for under s.94 of the Telecommunications Act 1984.

Legal background

- 20 The investigatory powers available to the security and intelligence agencies, law enforcement and other public authorities are currently contained in a number of pieces of legislation. These powers include the interception of communications, the retention and acquisition of communications data, equipment interference, and the acquisition of bulk data.
- 21 RIPA contains much of the current legislative scheme governing the investigatory powers used by the security and intelligence and law enforcement agencies to interfere with communications. Part 1 of the Act concerns communications. Chapter 1 of Part 1 concerns the interception of communications in the course of their transmission. It provides that such interception is an offence if carried out without lawful authority, and sets out the circumstances in which interception may be lawful. It also provides for the circumstances in which the Secretary of State may issue warrants for the interception of communications, and the protections for intercepted material. Chapter 2 of Part 1 concerns powers to acquire communications data (information concerning a communication, but not its content) from communications service providers. It sets out the public authorities who may acquire such data, the purposes for which they may do so, and the procedure for the authorisation of such conduct.
- 22 Part 4 contains oversight measures, providing for the Interception of Communications Commissioner, the Intelligence Services Commissioner and giving additional powers to the Chief Surveillance Commissioner established under the Police Act 1997. Part 4 also establishes the Investigatory Powers Tribunal.
- 23 Sections 1 and 2 of DRIPA and the Data Retention Regulations 2014 (DRR) contain the legislative scheme concerning the power of the Secretary of State to require communications service providers to retain communications data. DRIPA also made clear the extra-territorial extent of Part 1 of RIPA. Part 3 of the Counter-Terrorism and Security Act 2015 (CTSA) amends DRIPA so that an additional category of data - that necessary to resolve Internet Protocol addresses - can be included in a requirement to retain data. DRIPA contains a sunset clause and sections 1 to 7 are repealed on 31 December 2016. Part 11 of the Anti-Terrorism, Crime and Security Act 2001 provides for a voluntary code of conduct concerning the retention of communications data.
- 24 The SSA sets out the functions of the Security Service, and provides that the Service can only obtain or disclose information so far as is necessary for those functions.
- 25 ISA sets out the functions of the Secret Intelligence Service and GCHQ, and contains similar provision concerning the obtaining and disclosure of information. Section 5 provides for the Secretary of State to authorise interference with property or wireless telegraphy where

necessary for assisting the carrying out of any of the three agencies' functions. Section 7 provides for the Secretary of State to authorise activities overseas that would otherwise incur civil or criminal liability, where necessary for the proper discharge of the functions of SIS or GCHQ. These powers are currently used to authorise certain activities of the agencies that will be included in the new legislation.

- 26 Part 3 of the Police Act 1997 provides for the authorisation of interference with property or with wireless telegraphy. It also provides for the appointment of Surveillance Commissioners, who are given additional powers by Part 4 of RIPA.
- 27 The Wireless Telegraphy Act 2006 (section 49) provides for the authorisation of the use of wireless telegraphy equipment to obtain information about a communication, or the disclosure of such information. Such conduct is otherwise an offence under section 48 of the Act.
- 28 Section 94 of the Telecommunications Act 1984 gives the Secretary of State power to issue a direction of a general character to OFCOM or to a communications provider, in the interests of national security or international relations. Such directions must be kept secret.

European law

- 29 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.
- 30 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

- 31 The provisions in this Bill extend to the whole of the United Kingdom.
- 32 See the table in Annex A for a summary of the position regarding territorial extent and application in the United Kingdom. The table also summarises the position regarding legislative consent motions and matters relevant to Standing Orders Nos. 83J to 83X of the Standing Orders of the House of Commons relating to Public Business.

Commentary on provisions of Bill

Part 1: General Privacy Protections

Clause 1: Overview of the Act

33 This clause is self-explanatory.

Clause 2: Offence of unlawful interception

34 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 on a public telecommunications system, private telecommunications system or a public postal service. This is the same offence which previously existed under the RIPA.

35 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 expressed or implied consent of such a person to carry out the interception. This is relevant to computer networks in the home or workplace.

36 Subsections (3), (4) and (5) signpost the sections of the Bill 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;
- c. who has the lawful authority to apply for an interception warrant.

37 A public telecommunications system is the hardware and software used to provide a telecommunications service to the public in the United Kingdom. A private telecommunications system is one that is separate from, but connected to a public telecommunications system. This will include computer networks in the home or workplace.

38 Subsection (6) sets out the penalties for a person who is found guilty of the offence of unlawful interception under section 1. The penalty for unlawful interception is a fine in the magistrates court, or on conviction on indictment a maximum of two years' imprisonment, a fine or both. This replicates the penalty which existed under RIPA.

39 Subsection (7) provides that any proceedings for an offence under subsection (1) must be with the consent of the Director of Public Prosecutions (in England and Wales) or the Director of Public Prosecutions for Northern Ireland (in Northern Ireland).

Clause 3: Definition of "interception" etc.

40 This clause defines interception and sets out when interception is understood to take place in the United Kingdom. The intention is to make clear which actions constitute interception.

41 In relation to a telecommunications system, subsections (1) and (2) set out that a person intercepts a communication if they make some or all of the content of a communication available to a person who is not the sender or intended recipient, by modifying or interfering with the system, monitoring transmissions made by means of the system or monitoring transmissions made by wireless telegraphy to or from apparatus that is part of the system.

42 Subsection (3) gives more detail of the relevant act of modifying a telecommunications system.

43 Subsections (4) and (5) define what is meant by 'relevant time'. The intention of subsection

(4)(b) is to make clear that a communication is still considered in the course of its transmission when it is stored in or by the system used to transmit it. A stored communication includes communications stored on phones, tablets and other individual devices whether before or after its transmission.

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).

44 Subsection (7) sets out when a communication is in the course of its transmission by means of a postal system.

45 Subsection (8) explains when interception is carried out in the UK.

Clause 4: Conduct that is not interception

46 The purpose of clause 4 is to set out conduct which does not constitute interception. Subsection (1) makes clear that interception of a communication broadcast for general reception is not interception within the context of this Bill. Subsection (2) excludes conduct in relation to 'postal data' attached to the communication, e.g. reading the address on the outside of a letter in order to ensure it is delivered to the appropriate location.

Clause 5: Definition of "lawful authority"

47 This clause sets out the circumstances in which a person has lawful authority to carry out interception, so an offence of unlawful interception is not committed. Subsection (1) sets out that lawful authority to carry out interception must be either: in accordance with a warrant; with consent; in certain other circumstances set out in the Bill; or, in relation to stored communications, in exercise of any statutory power for the purpose of obtaining information or taking possession of any document or other property.

Clause 6: Monetary penalties for certain unlawful interceptions

48 This clause provides for the Investigatory Powers Commissioner to impose fines where unlawful interception has taken place but where the person responsible was not intending to intercept a communication.

Example:

A company that develops and uses a piece of software to collect information about Wi-Fi hotspots but does not realise that it is also intercepting content which is being sent from non-secure Wi-Fi devices.

49 Subsections (3) and (4) set out the conditions which must be met for the Investigatory Powers Commissioner to issue a monetary penalty notice. The Investigatory Powers Commissioner may not issue a monetary penalty notice if he or she considers that the person has committed an offence of unlawful interception i.e. the interception was intentional.

50 Subsection (6) introduces Schedule 1 which makes further provision about monetary penalty

notices.

Schedule 1: Monetary Penalty Notices

- 51 Schedule 1 sets out further details about monetary penalty notices. Part 1 sets out what a notice must contain: the 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.

Clause 7: Restrictions on requesting interception by overseas authorities

- 52 This clause provides that where a request is made by 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, it requires a warrant authorised under Chapter 1 of Part 2 to be in place.

Clause 8: Restriction on requesting assistance under mutual assistance agreements etc.

- 53 This clause explains 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 a mutual assistance agreement. Subsection (3) sets out the meaning of "international mutual assistance agreement" and "EU mutual assistance instrument".

Clause 9: Offence of unlawfully obtaining communications data

- 54 This clause creates a new offence of knowingly or recklessly, without lawful authority, obtaining communications data from a telecommunications or postal operator. The offence may be committed by a person within a public authority with powers to acquire communications data under Part 3 of the Bill. 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. The offence is intended to act as a deterrent and provide reassurance that abuse of powers to acquire communications data will be punished.

Clause 10: Abolition or restriction of certain powers to obtain communications data

- 55 This clause and Schedule 2 restrict the use of general information gathering powers and certain specific pieces of legislation to acquire communications data from a telecommunications or postal operator. The intent of these provisions is to ensure that this Bill, with its associated safeguards, is the only route for the acquisition of communications data for the statutory purposes in this Bill.
- 56 Numerous pieces of legislation provide public authorities with powers to require information in certain circumstances. This clause ensures those pieces of legislation will no longer be able to be used to acquire communications data from telecommunications or postal operators.
- 57 This clause does not apply where the power specifically relates to telecommunications or postal operators, or the regulation of telecommunications services. This is to allow OFCOM and the Information Commissioner's Office to carry out legitimate regulatory functions, for example ensuring the radio spectrum is used in an effective way. Regulatory powers should only be used if it is not possible for the regulator to use the powers in the Bill.
- 58 The restrictions in this clause 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 Bill to be used.

- 59 Schedule 2 lists the powers that specifically reference communications data or telecommunications services that are being repealed.

Schedule 2: Abolition of disclosure powers

- 60 Schedule 2 repeals certain powers so far as they enable public authorities to secure the disclosure by a telecommunications operator of communications data without the consent of the operator and ensures the definitions within these Acts have the same meaning as this Act.

Clause 11: Mandatory use of equipment interference warrants

- 61 This clause sets out the conditions in which a warrant must be sought under the powers contained in the Bill before equipment interference can be carried out by an intelligence service.
- 62 Subsections (1) requires that equipment interference must be authorised under the Bill in circumstances where the intelligence service believes that the conduct may constitute one or more offences under sections 1 to 3A of the Computer Misuse Act 1990, and that there is a connection to the British Islands.
- 63 Subsection (2) defines a British Islands connection as either:
- a. Where 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 Bill to authorise their activity, even if the equipment itself leaves or does not enter the British Islands; or
 - b. Where the intelligence service believes the equipment to be interfered with may be located in the British Islands at some point during the interference itself. This will include circumstances where the 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. Where the purpose of the interference is to enable the acquisition of the private information or the communications sent to or from a person believed to be in the British Islands. The interference is aimed at a person in the British Islands.
- 64 Subsection (3) clarifies that where those conditions are not met, an intelligence service may still apply for an equipment interference warrant. The circumstances in which they would do so will be set out in a Code of Practice.

Clause 12: Restriction on use of section 93 of the Police Act 1997

- 65 This clause confirms that applications by law enforcement agencies for property interference under section 93 of the Police Act may not be made where the purpose of the interference is to obtain communications, private information or equipment data, if the applicant believes the conduct constitutes an offence under the Computer Misuse Act and the conduct can be authorised under an equipment interference warrant. This does not remove or otherwise limit the ability for equipment interference to be authorised 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 clause prohibit the use of other legislation 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

Clause 13: Warrants that may be issued under this Chapter

- 66 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.
- 67 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.
- 68 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.
- 69 Subsection (5) confirms that a warrant authorises any conduct necessary to fulfill what is required by the warrant, including interception of communications not specifically described in the warrant, or of secondary data. 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.

Clause 14: Obtaining secondary data

- 70 This clause provides for the obtaining of secondary data under an interception warrant. Secondary data means:
- a. Systems data – which is defined in clause 225 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;
 - b. Identifying data which can be logically separated from the communication and which does not, once separated, reveal the meaning of the content of the communication. Identifying data is defined in clause 225 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 as defined in this clause may be obtained under a targeted interception warrant and, once the data is obtained, will be subject to the 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 (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.

Clause 15: Subject-matter of warrants

75 This clause sets out the permitted subject matter of a warrant. 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).

Clause 16: Persons who may apply for issue of a warrant

76 This clause 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 NCA, the Metropolitan Police, the Police Services of Northern Ireland and Scotland, HM Revenue & Customs and the Chief of Defence Intelligence. A competent authority of another country may also apply for a mutual assistance warrant.

Clause 17: Power of Secretary of State to issue warrants

77 This clause 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 clause 18) 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) requires the Secretary of State to consider whether the information it is thought necessary to obtain under a warrant could be sought by other means. Subsection (5) 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 clause 19).

Clause 18: 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 interest of national security, 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 giving effect to the provisions of a mutual assistance agreement.

Clause 19: Power of Scottish Ministers to issue warrants

80 This clause provides that the Scottish Ministers may issue a Part 2 warrant 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 be approved by a Judicial Commissioner before the warrant comes into force.

Clause 20: "Relevant Scottish applications"

- 81 Clause 20 sets out the cases in which the Scottish Ministers, rather than the Secretary of State, may issue warrants (referred to as a "relevant Scottish application"). These are where the application relates to a person reasonably believed to be in Scotland or premises which are in Scotland; or if the application is made by or on behalf of the chief constable of Police Scotland, the Commissioner of HM Revenue and Customs or the Director General of the National Crime Agency for the purpose of preventing or detecting serious crime in Scotland.

Clause 21: Approval of warrants by Judicial Commissioners

- 82 This clause sets out the test that the Judicial Commissioner must follow when considering whether to approve a decision to issue a warrant. He or she must consider the necessity and proportionality test applied by the Secretary of State under clause 18 in relation to the same grounds that the court would apply for a judicial review.
- 83 Subsection (4) makes clear that where a Commissioner refuses to approve a warrant he or she must set out written reasons for his or her 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.
- 84 Subsection (5) sets out that a Secretary of State or Scottish Ministers may ask the Investigatory Powers Commissioner to reconsider an application that a Judicial Commissioner has refused. Should the Investigatory Powers Commissioner also refuse to approve the warrant there is no right of appeal and the warrant cannot be issued.

Clause 22: Approval of warrants issued in urgent cases

- 85 This clause sets out the process for issuing a warrant in urgent cases. If the person issuing the warrant deems the warrant to be urgent then it can be issued without the approval of a Judicial Commissioner. Subsection (2) requires that the issuing of the warrant must be notified to the Judicial Commissioner. Subsection (3) provides that the Commissioner must decide whether to approve the decision to issue the warrant within three working days.
- 86 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. Subsection (5) refers the reader to the part of the Bill that contains further provision about what happens in these circumstances.

Clause 23: Failure to approve warrant issued in urgent case

- 87 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. A Judicial Commissioner can determine what can happen to any material or intelligence gathered under an urgent warrant that he or she has declined to approve.
- 88 Subsection (4) provides for representations to be made to the Judicial Commissioner from those involved in applying for the warrant or carrying out activity under the authority of the warrant.
- 89 Subsections (6) and (7) provide for the Secretary of State or Scottish Minister who issued an urgent warrant to ask the Investigatory Powers Commissioner to review a decision of a Judicial Commissioner to refuse to approve the decision to issue an urgent warrant. The

Investigatory Powers Commissioner can confirm the Judicial Commissioner's decision or make a fresh determination.

- 90 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.

Clause 24: Members of Parliament etc.

- 91 This clause requires the Secretary of State to consult the Prime Minister before deciding to issue a targeted interception or examination warrant where the purpose 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.

Clause 25: Items subject to legal privilege

- 92 This clause sets out the safeguards which apply when the purpose of a targeted interception or examination warrant is to obtain or look at items which are subject to legal privilege or where it is likely that legally privileged material is to be obtained or examined. 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 Chapter 9 of the Interception of Communications Code of Practice. 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 authorising the warrant 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.
- 93 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.

Clause 26: Decisions to issue warrants to be taken personally by Ministers

- 94 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 Scottish Minister but the Secretary of State or member of the Scottish Government must personally and expressly authorise the issuing of the warrant.

Clause 27: Requirements that must be met by warrants

- 95 This clause deals with the information which needs to be contained in Part 2 warrants. Subsections (2) to (8) specify the information a warrant must contain including the intercepting authority, details of the person or group of persons, organisation or premises to which the warrant relates. In the case where the warrant relates to a group of individuals linked by an activity/investigation/operation, this must be described.

Example:

This involves an operation where an individual has been kidnapped. The agency may have a phone number or numbers but at the time not know who they are being used by. In these circumstances the agency could not describe the individuals (beyond kidnapper 1, kidnapper 2, driver etc.). The warrant could therefore refer to operation 'safe return' and would allow an addition if the investigation then becomes aware of 'kidnapper 3'.

Clause 28: Duration of warrants

- 96 This clause 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 days unless renewed.

Clause 29: Renewal of warrants

- 97 Subsections (1) - (3) state that a warrant may be renewed by an instrument issued by the Secretary of State or member of the Scottish Government. For the warrant to be renewed, it must continue to be necessary and proportionate. As with an application for an interception warrant, the decision to renew the warrant must also be approved by a Judicial Commissioner. The additional protection for Members of Parliament, etc. (see clause 24) and for legally privileged material (see clause 25) apply when renewing warrants as they do when issuing warrants.

Clause 30: Modification of warrants

- 98 This clause provides for a warrant to be modified as specified in subsection (2) by instrument. Subsection (4) explains what "major" and "minor" modifications are and subsections (5) and (6) outline who can undertake a major and minor modification. Subsections (9)-(11) restate the conditions of necessity and proportionality which must be considered before major modifications can be made. The clause also sets out that the additional protections for Members of Parliament, etc. (see clause 24), and items subject to legal privilege (see clause 25) 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.

Clause 31: Approval of major modifications made in urgent cases

- 99 This clause sets out the process for approving a major modification to a warrant which has been made urgently. In this case, the person who made the modification must inform a designated senior official that they have done so. The Secretary of State or member of the Scottish Government must personally be notified of the modification and the reasons for it. The designated senior official has five working days in which to decide whether to approve the modification. If he or she refuses the modification, the warrant (unless it no longer has effect) has effect as if the modification had not been made, and the Secretary of State or member of the Scottish Government must again be personally notified.

Clause 32: Cancellation of warrants

- 100 This clause provides that the Secretary of State, 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.

Clause 33: Special rules for certain mutual assistance warrants

These Explanatory Notes relate to the Investigatory Powers Bill as introduced in the House of Commons on 19 May 2016 (Bill 2)

101 This clause 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.

102 Subsection (2) provides that the decision to provide assistance in such circumstances can be taken by a senior official designated by the Secretary of State. Subsection (4) makes clear that the senior official may also renew the mutual assistance warrant. Subsections (3) and (5) set out what must be included in the warrant. Subsection (7) makes clear that any warrant must be cancelled if the subject of the warrant is in the UK.

Clause 34: Implementation of warrants

103 This clause provides that the person who has obtained the warrant (i.e. the head of the intercepting agency) 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.

Clause 35: Service of warrants outside the United Kingdom

104 This clause sets out the process for serving a targeted interception warrant or a mutual assistance warrant on a person outside the United Kingdom. Subsections (2) and (3) set out the ways a warrant may be served on such a person.

Clause 36: Duty of operators to assist with implementation

105 This clause provides that a telecommunications or postal service provider served with a targeted interception warrant or a mutual assistance warrant is required to take steps to give effect to it. Subsection (3) makes clear that the obligation applies whether or not the operator is in the UK. Subsection (4) ensures that the steps a service provider is required to make must be reasonably practicable and subsection (5) makes clear that in considering what is reasonable, any requirements or restrictions under the laws of the country in which a 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.

106 Subsection (7) sets out the offence for knowingly failing to comply with an interception warrant. Subsection (8) provides that the duty to comply with a warrant is enforceable against a person (whether or not they are inside the UK) by civil proceedings brought by the Secretary of State.

Chapter 2: Other forms of lawful interception

Clause 37: Interception with the consent of the sender or recipient

107 Subsection (1) provides that the interception of a communication is authorised if both the person sending the communication and the intended recipient of the communication have given consent for the interception to take place.

108 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.

Example:

This situation might arise where a kidnapper is telephoning relatives of a hostage, and the police wish to listen to the call in order to identify or trace the kidnapper. The operation will be authorised as surveillance, rather than by means of an interception warrant, because consent can only reasonably be obtained for one end of the communications i.e. the relatives have consented.

Clause 38: Interception by providers of postal or telecommunication services

- 109 This clause authorises interception where it takes place for the purpose of providing or operating a postal service or telecommunications service, or where any enactment relating to the use of such a service is to be enforced. This might occur, for example, where the postal provider needs to open a postal item to determine the address of the sender because the recipient's address is unknown. A further example might be where a telecommunications service provider is delivering a service to its customers and the customer has requested that harmful, illegal or adult content is filtered (e.g. family friendly filtering).
- 110 Subsection (3) makes clear that telecommunication service providers can undertake activity to protect the telecommunication system through which their service is provided and any apparatus attached to that system, to maintain the integrity of their services and to ensure the security of their customers.

Clause 39: Interception by businesses etc. for monitoring and record-keeping purposes

- 111 This clause 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 for training or quality control purposes.

Clause 40: Postal services: interception for enforcement purposes

- 112 This clause provides for the interception of postal items by HM Revenue & Customs in carrying out their duties under clause 159 of the Customs and Excise Act 1979 or by an examining officer under paragraph 9 of Schedule 7 of the Terrorism Act 2000.

Clause 41: Interception by OFCOM in connection with wireless telegraphy

- 113 This clause 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 telegraphy licences and preventing and detecting interference with wireless telegraphy.
- 114 OFCOM use equipment to find the source of radio frequency interference rather than to listen to or read communications.

Clause 42: Interception in prisons

- 115 Subsection (1) makes clear that it is lawful to intercept communications in a prison if it is in

the exercise of any power conferred under prison rules and subsections (2 and 3) sets out what is meant by “prison rules” and “prisons”.

Clause 43: Interception in psychiatric hospitals etc.

116 This clause sets out the circumstances in which interception can be carried out in psychiatric hospitals.

Clause 44: Interception in immigration detention facilities

117 This clause sets out the circumstances in which interception can be carried out in immigration detention facilities.

Clause 45: Interception in accordance with overseas requests

118 This clause deals with the issue of interception when a request is made from overseas.

119 Subsections (2) to (4) sets out the conditions which need to be met in order that a communications provider may intercept the communications of an individual at the request of another country. Further conditions may be contained in regulations made by the Secretary of State.

Chapter 3: Other provisions about interception

Clause 46: Safeguards relating to retention and disclosure of material

120 This clause sets out that the issuing authority must ensure that arrangements are in force for safeguarding material obtained under an interception warrant.

121 Subsection (2) sets out the requirements to keep to a minimum the number of persons who see material and to limit the disclosure and number of copies made of any material to the minimum necessary for the authorised purposes. Subsection (3) sets out the circumstances in which something is necessary for the authorised purposes.

122 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 material subject to legal privilege is retained. Subsections (8) to (10) reference the safeguards relating to disclosure of information overseas at clause 47 and include a definition of “copy”.

Clause 47: Safeguards relating to disclosure of material overseas

123 This clause sets out the safeguards which apply when disclosing intercept material and secondary data to an overseas authority and provides that the Secretary of State must be satisfied that equivalent safeguards are in place, even though they may not appear identical. These safeguards include that material is not disclosed in a way which would constitute unlawful disclosure in the United Kingdom.

Clause 48: Exclusion of matters from legal proceedings

124 This clause prevents intercept material being used or disclosed in legal proceedings or an inquiry held under the Inquiries Act 2005. This includes adducing it in evidence, asking questions about it, disclosing it, or doing anything from which it could be inferred that the material came from interception or which suggests that interception may have occurred. Subsections (2) to (4) provide further detail of the information which may not be disclosed.

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

Schedule 3: Exceptions to section 48

126 Schedule 3 sets out the exceptions to clause 48(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 would not apply.

- 127 Paragraph (2) provides that the contents of a communication, and secondary data, may be disclosed if the communication is obtained under a statutory power exercised to obtain information, documents or property. This specifically applies to stored communications. It also allows for disclosure of any lawful interception carried out in accordance with clause 5(1)(c) and sections 37 to 45.
- 128 Paragraph (3) provides that there is no prohibition on doing anything which discloses conduct for which a person has been convicted of offences under the Acts listed.
- 129 Paragraphs (4) and (5) provide that clause 48(1) does not apply in relation to proceedings before the Investigatory Powers Tribunal or the Special Immigration Appeals Commission, providing the conditions specified in sub-paragraph (5)(2) (a) and (b) are met, which prohibits disclosure to a SIAC applicant or representatives.
- 130 Paragraph (6) provides that clause 48(1) does not apply in relation to proceedings before the Proscribed Organisations Appeal Commission, providing there is no disclosure to the persons or bodies listed in sub-paragraph (6)(2).
- 131 Paragraph (7) provides that clause 48 (1) does not apply to certain civil proceedings where provision for disclosure within closed material procedures is made under section 14(1) of the Justice and Security Act 2013, provided that there is no 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 a relevant person.
- 132 Paragraphs (8) and (9) provide that clause 48(1) does not apply in any proceedings relating to Terrorism Prevention and Investigation Measures or temporary exclusion orders, providing there is no 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.
- 133 Paragraphs (10)-(12) provide that clause 48(1) does not apply into 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.
- 134 Paragraph (13) provides that clause 48(1) does not apply in proceedings relating to the release of prisoners in Northern Ireland providing there is no disclosure to any person who is party to the proceedings or their representatives who are not special advocates.
- 135 Paragraphs (14)-(15) provide that clause 48(1) does not apply in relation to certain employment or industrial tribunal proceedings where the applicant or their representatives are excluded for all or part of the proceedings, providing there is no disclosure to the applicant in the proceedings or their representatives who are not special advocates.
- 136 Paragraph (16) provides that clause 48(1) does not prevent anything done in connection with legal proceedings relating to dismissal for offences under the Acts listed.
- 137 Paragraphs (17)-(18) provide that clause 48(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.
- 138 Paragraph (19) provides that clause 48(1) does not apply in relation to civil enforcement proceedings where a relevant service provider has refused to assist in the implementation of a

warrant.

- 139 Paragraph (20) lists the offences in relation to which clause 48(1) does not apply. These include proceedings for offences under the Act, and related offences.
- 140 Paragraph (21) provides that disclosure can be permitted during criminal proceedings to prosecutors and judges in the interests of a fair prosecution. Sub-paragraph (4) makes provision for judges to direct the prosecution to make relevant admissions if, as a consequence of the disclosure, the judge believes this is essential in the interests of justice as long as it does not contravene clause 48(1).
- 141 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, but as in paragraph (22), that disclosure should be made to the panel of an inquiry or the legal adviser to the inquiry. Paragraph (24) provides that disclosure can be made to a judge or retired judge for the purpose of conducting an inquest into a death. Disclosure is also permitted to the legal adviser to 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 in an inquest for the purpose of appointing a relevant judge who will be able to view the intercept material. Nothing in these sections allows disclosure to be made to any other party in connection with these proceedings.

Clause 49: Duty not to make unauthorised disclosures

- 142 This clause places a duty on those persons listed in subsection (3) not to disclose the existence or details of a warrant or any intercepted material. Subsection (4) sets out the matters which, if disclosed, would constitute unauthorised disclosure.

Clause 50: Section 49: meaning of “excepted disclosure”

- 143 Subsection (1) sets out the categories of excepted disclosure. Subsection (2) provides for disclosure authorised by the warrant. Subsection (3) provides for 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 the relevant company to provide the material). Subsection (4) provides for disclosure made to or authorised by a Judicial Commissioner. Subsection (7) provides for the disclosure of information by a postal operator or telecommunications operator, subject to any requirements imposed by regulations made by the Secretary of State, to publish information about warrants in general. This does not provide for disclosure of any particular warrant issued under Chapter 1.

Clause 51: Offence of making unauthorised disclosures

- 144 This clause provides that it is an offence to fail to comply with the duty in clause 49 and sets out the penalty for unlawful disclosure of intercept material.

Clause 52: Part 2: interpretation

- 145 This clause sets out definitions for a number of terms used throughout this clause.

Part 3: Authorisations for obtaining communications data

Clause 53: Power to grant authorisations

- 146 This clause provides the power for relevant public authorities to acquire communications data.

These Explanatory Notes relate to the Investigatory Powers Bill as introduced in the House of Commons on 19 May 2016 (Bill 2)

An authorisation can be granted where a designated senior officer in a relevant public authority is content that a request is necessary and proportionate for one of the 10 purposes set out in subsection (7). Communications data cannot be acquired in circumstances outside of those purposes and only certain authorities can use certain purposes, as outlined in Schedule 4.

- 147 Subsection (4) provides for some of the conduct which an authorisation may permit for the purpose of acquiring communications data. The types of conduct that can be engaged in are the same as can currently be engaged in under Chapter 2 Part 1 of RIPA. For example the conduct to acquire communications data may involve:
- a. Serving a notice on a telecommunications service provider that requires them to disclose the relevant data;
 - b. Serving a notice on a telecommunications service provider that requires them to obtain and then disclose the relevant data;
 - c. A relevant public authority acquiring the data directly from a communications service provider through a secure auditable system;
 - d. A relevant public authority acquiring the data directly from a telecommunications system.

148 An authorisation which provides for the conduct set out in (d) above can only authorise conduct to acquire communications data which does not require the interception of the content of a communication or require the interference with any equipment on the telecommunications network.

149 Subsection (5) provides examples that may be covered by an authorisation. For example, an authorisation may cover data that is not in existence at the time of the authorisation. This allows a relevant public authority to request communications data on a forward looking basis in respect of a known subject of interest. It also provides that an authorisation can authorise the disclosure of communications data by a communications service provider through a secure auditable system.

Clause 54: Additional restrictions on grant of authorisations

150 This clause provides a restriction on who can authorise the request. The authorising officer can only agree to the acquisition of communications data where they are independent of the operation.

151 Examples of exceptional circumstance where this restriction does not apply include where there is an imminent threat to life, where using an independent authorising officer would immediately impact on national security or where it is simply not possible due to the size of the public authority.

152 This clause also provides restrictions concerning the acquisition of internet connection records that are held by communications service providers. Clause 78(9) of this Bill provides for the retention of communications data including internet connection records. A public authority may only acquire internet connection records that are held by a communications service provider for the following four purposes:

- a. To identify the sender of an online communication; this will often be in the form of IP address resolution and the internet service used must be known in advance of the application.
- b. Identifying which communication services a person has been using, for example determining whether they are communicating through apps on their phone.

- c. Identifying where a person has accessed illegal content, for example an internet service hosting child abuse imagery.
- d. Identifying which internet service is being used and when and how it is being used.

153 In respect of purpose (a), for example, the relevant public authority will be aware of an action on a particular internet service at a specific time or range of time, for example that illegal images have been uploaded. The communications data application would be to determine which individual carried out that action at that time.

154 In respect of purposes (b) and (c) the designated senior officer within a relevant public authority could only approve the application if it was to determine how an individual has been communicating with another individual online, or whether they had been accessing illegal material over a specified timeframe. If approved, a request would then be made to a communications service provider for all internet connection records in that timeframe.

155 In respect of purpose (d), 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. This purpose should be only be used to identify internet services which are not communications services covered by purpose (b) or where the purpose is not to identify whether a person has been accessing illegal content covered by purpose (c).

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

157 Subsection (6) defines an internet connection record for the purposes of the Act.

Clause 55: Procedure for authorisations and authorised notices

158 Subsection (1) sets out that every authorisation must specify certain details. These include the position held by the designated senior officer granting the authorisation, which of the limited purposes it is being granted for (as set out in clause 53(7)), the conduct for which it was authorised, the type of data to be obtained, and who the data will be disclosed to.

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

160 Subsection (3) sets out that the notice must specify the position held by the person giving the notice, the requirements that will be imposed on that communications service provider, and the name of the communications service provider.

161 Subsection (4) sets out that a record must be kept of the notice in order to show that it has been applied for or granted.

Clause 56: Duration and cancellation of authorisations and notices

162 This clause 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.

163 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.

164 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.

165 Subsections (5) and (6) permit the Secretary of State to specify by order the person required to carry out the duty set out in subsection (4) in the event that this would otherwise fall on a person who is no longer available to perform it.

Clause 57: Duties of telecommunications operators in relation to authorisations

166 Communications service providers are required to comply with a request for communications data, except in circumstances where it is not reasonably practicable to comply. If complying with the request is reasonably practicable then the provider should comply in such a way that involves processing the minimum amount of data necessary.

167 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 the specific performance of a statutory duty under clause 45 of the Court of Session Act 1988 or for any other appropriate relief.

Clause 58: Filtering arrangements for obtaining data

168 This clause provides a power to establish filtering arrangements to facilitate the lawful, efficient and effective obtaining of communications data by relevant public authorities and to assist a designated senior officer in each public authority to determine whether he believes the tests for granting an authorisation to obtain data have been met. The filtering arrangements will minimise the interference with the right to privacy, in particular respect for personal correspondence, to which requests for internet based communications data will give rise thereby ensuring that privacy is properly protected. In practice, filtering arrangements would be implemented by the Secretary of State in a Request Filter system which would be used by public authorities granting authorisations for the targeted acquisition of communications data.

Potential use of the Request Filter

Example (1): IP address resolution:

An investigator has details of a number of IP addresses which they believe relate to a specific individual, and have been used to access internet services at known times. However, each IP address cannot be resolved to a single individual because at the known time it has been simultaneously shared between many internet users. In this example the Request Filter would be able to match the specific individual in common between the users of each the IP addresses, then disclose only the communications data about that specific individual to the public authority. Without the Request Filter telecommunications operators would need to disclose details of every individual that had shared the IP addresses at the relevant times, and an analyst working in the public authority would examine all of the 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.

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

170 The power to establish filtering arrangements in subsection (1) operates solely in the context of Part 3 of the Bill which creates a regulatory regime for obtaining data. The power is intended to facilitate the obtaining of data by public authorities only for the purpose of a specific investigation or a specific operation in accordance with an authorisation, whilst protecting privacy. Any communications data obtained by the filtering arrangements must be immediately deleted once the purposes of the authorisation have been met.

Clause 59: Use of filtering arrangements in pursuance of an authorisation

171 This clause will apply in relation to the use of any Request Filter established under the power in clause 58. 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.

172 Subsection (3) sets out the matters which the designated senior officer must record within the authorisation to obtain Part 3 data. These include:

- a. whether the Part 3 data may be obtained and disclosed by use of the filter;
- b. whether the processing of data under the filter is allowed;
- c. if the processing of data is allowed, then a description of data that may be processed must also be included.

173 Subsections (4) and (5) reinforce the conditions that must be met before a designated senior officer can authorise the use of a Request Filter. These conditions are: that it is necessary to obtain the data for a public protection purpose; that it is necessary to obtain the data for a specific investigation or a specific operation; and that the conduct authorised by the authorisation is proportionate to what an investigator is seeking to achieve.

174 Subsections (2) to (5) will accordingly ensure that the use of any Request Filter under Part 3 is specifically authorised by the authorisation, is proportionate and is recorded within the authorisation.

Clause 60: Duties in connection with operation of filtering arrangements

175 This clause imposes duties in connection with the operation of filtering arrangements. In the case of a Request Filter, subsection (1) provides that no communications data must be obtained or processed under the filter except for the purposes of an authorisation granted under clause 53. Data which has been obtained or processed under the filter, and is to be disclosed in accordance with the authorisation or for the purposes of assisting the designated senior officer, shall only be disclosed to authorised individuals. Further, subsection (1)(c) specifically requires any data obtained by the filter to be immediately destroyed in such a way that it can never be retrieved, once the purposes of the authorisation or of the assistance function have been met or if at any time it ceases to be necessary to retain the data for these purposes.

176 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.

177 Subsection (2) limits the disclosure of data other than authorised data which is retained under the filtering arrangements:

- a. to assist a designated senior officer to determine whether he believes the tests for granting an authorisation are met;
- b. for the purposes of support, maintenance, oversight, operation or administration;
- c. to the Investigatory Powers Commissioner for the purposes of any his functions;
- d. as otherwise authorised by law.

178 Subsection (3) requires strict limits to be placed on the persons who are permitted to read, obtain or otherwise process data for the purposes of support, maintenance, oversight, operation or administration in connection with the Request Filter. No other persons must be permitted to access or use the capability except in pursuance of an authorisation or to assist the designated senior officer to determine whether an authorisation is necessary and proportionate.

179 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.

180 Subsection (6)(a) requires procedures to be put in place and maintained to ensure that the Request Filter is functioning properly, including regular testing of the relevant software and hardware. Subsection (6)(b) requires a report to be made, as soon as possible after the end of each calendar year, to the Investigatory Powers Commissioner about the functioning of the Request Filter during that year. Such a report must, in particular, contain information about destruction of data during that year (subsection (6)). Subsections (5) and (6) will ensure that the operation of any Request Filter is subject to rigorous oversight and control.

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

Clause 61: Relevant public authorities and designated senior officers

182 This clause introduces Schedule 4 to the Bill and makes provision in relation to relevant public authorities, designated senior officers and safeguards.

183 Schedule 4 includes a table which lists the public authorities permitted to obtain communications data under Part 3 of the Bill (column 1); the minimum office, rank or position of the designated senior officers permitted to grant authorisations to obtain data (column 2); the types of communications data that may be obtained (column 3); and the statutory purposes for which they may be obtained (column 4).

184 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.

185 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.

186 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.

187 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

188 Column 1 of the table in Part 1 of this Schedule lists all the authorities that are able to acquire communications data. Column 2 provides a minimum rank for designated senior officers. These are the staff within the relevant public authorities that are able to authorise the acquisition of communications data. Columns 3 and 4 provide the types of data that each designated senior officer is able to authorise the acquisition of and the statutory purposes, listed in clause 53(7), for which it can be accessed.

189 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.

190 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.

Clause 62: Power to modify section 61 and Schedule 4

191 This clause provides that the Secretary of State may modify clause 61 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.

192 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.

Clause 63: Certain regulations under section 62: supplementary

193 This clause provides that all changes to clause 61 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.

194 By virtue of clause 228 such orders will be subject to the negative resolution procedure.

195 When making changes to the relevant public authorities in Schedule 4 by the enhanced affirmative procedure, this clause requires the Government to consult the Investigatory Powers Commissioner and the relevant public authority concerned. An example of this would include adding a new public authority to the list of relevant authorities.

Clause 64: Local authorities as relevant public authorities

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

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

198 This clause provides that the rank of a designated senior officer can be amended by the 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.

Clause 65: Requirement to be party to collaboration agreement

199 This clause ensures that local authorities will only be able to obtain communications data if they are party to a collaboration agreement as certified by the Secretary of State. This is a safeguard that ensures local authorities are only able to acquire communications data through an experienced shared Single Point of Contact service.

Clause 66: Judicial approval for local authority authorisations

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

201 This means that a local authority authorisation granted under clause 64 will not take effect until the "relevant judicial authority" has given its approval. The relevant judicial authority is defined in subsection (7). In England and Wales, the judicial authority is a justice of the peace, in Northern Ireland it is a district judge (magistrates' court) and in Scotland, a sheriff.

Clause 67: Use of a single point of contact

202 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. Clause 60 sets out how the SPoC and designated senior officer work together when granting an authorisation for the acquisition of communications data.

203 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.

204 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.

205 Subsections (5) and (6) set out the advisory role that a SPoC plays to both those applying for communications data, and the designated senior officer that authorises the application. SPoCs should advise whether the application and authorisation is lawful, appropriate and cost-effective, and takes into consideration any unintended consequences.

206 Subsection (7) sets out that a SPoC may also provide advice to the designated senior officer about whether the requirements of an authorisation have been met, its use in support of operation or investigations and any other effects the authorisation may have.

Clause 68: Commissioner approval for authorisations to identify or confirm journalistic sources

207 This clause 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.

208 Subsections (1), (2) and (3) set out that an authorised communications data application made by public authorities for the purpose of identifying the source of journalistic information must not take effect until approved by a Judicial Commissioner. Prior Judicial Commissioner approval is not required in an imminent threat to life situation.

209 Subsection (4) sets out that in making an application for data to identify a journalistic source, the applicant is not required to notify either the person to whom the applications relates i.e. the journalistic source, nor that person's legal representative.

210 Subsection (5) sets out that a Judicial Commissioner should only approve an authorisation to acquire communications data to identify a journalistic source if satisfied that the conditions of the authorisation by the designated senior officer have been met.

211 Subsection (6) sets out that the Judicial Commissioner may quash any authorisation given by the designated senior officer, if the Judicial Commissioner refuses to approve it.

212 Subsection (7) sets out what is meant by the "source of journalistic information". It is defined as an individual (i.e. the source) who provides material intending the recipient (i.e. the journalist) to use it for the purpose of journalism or knowing that it is likely to be used for journalism.

Clauses 69 and 70: Collaboration agreements

213 Clauses 69 and 70 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.

Clause 71: Police collaboration agreements

214 The Police are already permitted to be in collaboration agreements and this outlines their arrangements. Subsection (6) sets out that references to a police force in this clause include the National Crime Agency.

Clause 72: Lawfulness of conduct authorised by this Part

215 Subsection (1) has the effect of making conduct lawful for all purposes if it is conduct in which that person is authorised to engage by virtue of an authorisation, and the conduct is in accordance with, or in pursuance of, the authorisation.

216 Subsection (2) exempts a person from civil liability in respect of conduct which is incidental to, or reasonably undertaken in conjunction with, that authorised in subsection (1). The conduct must not itself be conduct for which an authorisation or warrant:

- a. is capable of being granted under the enactments referred to in subsection (3), and;
- b. might reasonably have been expected to have been sought in the case in question.

Clause 73: Offence of making unauthorised disclosure

217 This clause 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.

218 The intent of these provisions is to prevent the so called 'tipping-off' of criminal suspects or subjects of interest that their data has been sought, thus informing them that they are under suspicion.

Clause 74: Certain transfer and agency arrangements with public authorities

219 This clause allows for the Secretary of State by making regulations to transfer ownership of the filtering arrangements to a public authority.

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

220 This Schedule outlines the provisions that apply should the Home Secretary transfer ownership of the Request Filter to a public authority. Paragraph 1, subparagraph (2) requires the Secretary of State to approve the measures to be adopted by a designated public authority for complying with the requirements in clause 60. A designated public authority must send the reports required under subparagraph (3), 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.

221 Paragraph 3 sets out that the Secretary of State, in connection with regulations made under clause 74(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.

222 Sub-paragraph (3) lists consequential, supplementary, incidental and transitional provision that may be made by a transfer scheme. These include making provision the same as or similar to the TUPE regulations (the Transfer of Undertakings (Protections of Employment) Regulations 2006 (S.I. 2006/246). By virtue of sub-paragraph (5), a scheme may make provision for the payment of compensation, for example to a designated public authority in circumstances where functions conferred on that body are brought back within the Home Office. Sub-paragraph (6) provides that a transfer scheme may be included in regulations made under clause 74(1) but if not, must be laid before Parliament after being made.

223 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.

Clause 75: Applications of Part 3 to postal operators and postal services

224 This clause provides that all clauses in Part 3 relating to telecommunications operators and telecommunications services also apply to postal operators and postal services.

Clause 76: Extra-territorial applications of Part 3

225 This clause sets out that communications service providers overseas are also subject to the provisions of Part 3 of the Bill. 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 to take steps to comply with a duty under clause 57. These include the law of the country in question.

Clause 77: Part 3: interpretation

226 This clause clarifies terms that are regularly referred to throughout Part 3 of the Bill.

Part 4: Retention of communications data

Clause 78: Powers to require retention of certain data

227 This clause provides a power to require telecommunications operators to retain communications data, where necessary and proportionate for one or more of the statutory purposes (at clause 53(7)) for which it can be acquired for a maximum period of 12 months.

228 The power is exercised by giving a retention notice to a telecommunications operator. 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 served a telecommunications operator is not required to retain any communications data under this Bill.

229 Subsection (9) 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.

230 Subsection (9) also makes clear that communications data that can be retained includes internet connection records. Internet connection records, which are defined in clause 54(6), are a record of the internet services that a specific device connects to – such as a website or instant messaging application – captured by the company providing access to the internet. They could be used, for example, to demonstrate a certain device had accessed an online communications service but they would not be able to be used to identify what the individual did on that service. Clause 54 provides certain restrictions on the acquisition of internet connection records.

Clause 79: Matters to be taken into account before giving retention notices

231 This clause sets out a number of factors that the Secretary of State must take into account before giving a retention notice to a communications service provider. 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.

Clause 80: Review by the Secretary of State

232 This clause 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.

233 Subsection (4) states that the person is not required to comply with the specific obligations under referral until the notice has been reviewed by the Secretary of State. The actions that the Secretary of State must take in reviewing the notice and the role of the Technical Advisory Board and the Investigatory Powers Commissioner are outlined at subsections (5 to 8).

234 Subsection (9) requires 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.

235 Subsection (12) imposes an obligation on the Secretary of State to keep a notice under review, regardless of whether or not it has been referred.

Clause 81: Data integrity and security

236 This clause 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, deleted in a way that ensures access is impossible.

Clause 82: Disclosure of retained data

237 Communications service providers must put in place adequate security procedures governing the access of communications data in order to protect it against unlawful disclosure.

Clause 83: Variation or revocation of notices

238 Subsections (1) to (8) provide for the Secretary of State to vary a notice. Where a notice is varied the same considerations will apply as in the giving of a notice.

239 Subsections (9) to (12) provide for the revocation of data retention notices in full or in part.

Clause 84: Enforcement of notices and certain other requirements and restrictions

240 Telecommunications operators are required to comply with a data retention notice and the requirements in the Bill relating to the security, integrity, deletion and disclosure of data.

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

242 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 for the specific performance of a statutory duty or for any other appropriate relief.

Clause 85: Application of Part 4 to postal operators and postal services

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

Clause 86: Extra-territorial application of Part 4

244 This clause provides that communications service providers 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 communications service 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 clause 84(5) does not apply.

Clause 87: Part 4: interpretation

245 This clause provides for interpretation of this Part, including references for relevant definitions.

Part 5: Equipment interference

Clause 88: Warrants under this Part: general

246 This clause provides for the issuing of targeted equipment interference and targeted examination warrants and explains the activities and conduct these may authorise when meeting the test of necessity and proportionality. 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.

247 Subsection (3) sets out the additional activity that a targeted equipment interference warrant authorises. An equipment interference warrant must authorise the recipient to obtain communications, equipment data or other information (subsection (3)(a)), and may also authorise the recipient of the material under the warrant to subsequently disclose (subsection (3)(b)). 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, without the need for the activity to be authorized separately under Part 2 of RIPA, however, this does not permit the acquisition of communications (other than stored communications) in circumstances where an interception warrant is required (6). If an investigation requires both equipment interference and interception techniques then a combined warrant may be issued.

248 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 relates to any material obtained under a bulk equipment interference warrant other than equipment data or non-private information.

Clause 89: Meaning of “equipment data”

249 This clause defines the material which is equipment data in relation to a targeted equipment interference warrant. Equipment data means:

- a. Systems data – which is defined in clause 225 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;
- b. Identifying data which can be logically separated from the communication or item of information and which does not, once separated, reveal the meaning of the content of the communication or the meaning (if any) of an item of information (disregarding any inferred meaning). Identifying data is defined in clause 225 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.

250 Equipment data as defined in this clause 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.

251 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.

252 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

Clause 90: Subject-matter of warrants

253 This clause sets out the equipment that an equipment interference warrant may relate to. For interference to be considered targeted it must relate to:

- a. a particular person or persons (e.g, the computer equipment of Person X);
- b. 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); or
- d. equipment that is being used for testing and development.

254 The targeted equipment interference warrant may also relate to equipment where there is a common link between multiple people, locations or organisations where the interference is for the purpose of the same investigation or operation (so, for example, computers believed to being used by Terrorist Plot Group X), or equipment that is being used for a particular activity. These latter warrants have sometimes been described as 'thematic'.

255 In some instances it may not be possible to be specific about the nature of the equipment to be interfered with in advance, or there may be a technique that in itself carries out a specific small amount of interference, but enables access to the data that may already have been granted under an existing authorisation. In these cases the warrant should be specific about the technique and the circumstances in which the warrant is to be used. In such cases, the circumstances must be described in a way that enables the requirements of section 100 of the Act to be met.

256 Subsection (2) regards targeted examination warrants. In contrast to targeted equipment interference warrants, examination warrants do not need to describe the subject equipment, but rather the individual/s to which the warrant relates. This reflects the fact that the data has already been gathered under a bulk equipment interference warrant, so an examination warrant regards the identification of specific data in an existing pool of data, rather than data acquisition. A targeted examination warrant therefore 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.

Clause 91: Power to issue warrants to intelligence services: the Secretary of State

257 This clause establishes the process and requirements for equipment interference warrants that are applied for by and issued to a director of one of the intelligence services. The intelligence services comprise the Security Service, the Secret Intelligence Service and Government Communication Headquarters.

258 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 interest of national security, for the purposes of preventing or detecting serious crime, or in the interests of the economic wellbeing of the United Kingdom (so far as those interests are also relevant to the interests of national security).

259 Subsection (1) also sets out that it is permitted for a warrant to be applied for on behalf of the head of one of the services, meaning it is not necessary for every warrant application to be made personally by the head of service. Subsection (8) states that when a warrant is applied for on behalf of a head of the service, the application must be made by a person holding office under the Crown.

260 Subsection (2) prevents the Secretary of State issuing a targeted equipment interference warrant that relates to serious crime in Scotland. This is because Scotland have devolved responsibility for matters relating to crime. Clause 92 addresses the process for such warrants. Similarly, subsection 4 prohibits the Secretary of State from issuing a targeted examination warrant if it relates to serious crime and the subject of the warrant is in, or reasonably believed to be in, Scotland when the application for the examination warrant is made.

261 Subsections (1) (b) (c) and (d) together ensure that the 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. In addition, subsection (7) requires that the Secretary of State, in considering the necessity and proportionality of the proposed activity, also considers if what is sought through equipment interference could reasonably be achieved by other means.

Clause 92: Power to issue warrants to intelligence services: the Scottish Ministers

262 This clause explains that when a targeted equipment interference warrant or targeted examination warrant – for the purpose of preventing and detecting serious crime - relates to interference with equipment believed to be in Scotland, or the examination of protected material of an individual in, or reasonably believed to be in, Scotland it is the responsibility of Scottish Ministers, rather than the Secretary of State, to issue the warrant. This only applies to the security and intelligence agencies, as law enforcement agencies will apply to their relevant law enforcement chief in all circumstances. The same consideration of necessity and proportionality still applies as set out in (1) (b) and (c) and (2) (b) and (c) and the Scottish Minister will still require approval from a Judicial Commissioner before they can issue a warrant, except if the case is considered urgent.

Clause 93: Power to issue warrants to the Chief of Defence Intelligence

263 This clause makes provision for the Chief of Defence Intelligence to apply for targeted equipment interference warrants. Such warrants work in the same way as warrants issued to the intelligence services, with approval also dependent upon the Secretary of State's consideration. The exception in this instance is that warrants issued to the Chief of Defence

Intelligence can only be issued for national security purposes.

Clause 94: Members of Parliament etc.

264 This clause requires the Secretary of State to consult the Prime Minister before a targeted equipment interference or examination warrant may be issued, where the purpose of the warrant is to obtain the communications or private information of a person who is a member of Parliament, the Devolved Administrations of Northern Ireland, Scotland or Wales or the European Parliament ('relevant legislatures').

Clause 95: Decision to issue warrants under sections 91 to 93 be taken personally by Ministers

265 This clause states that the Secretary of State or, where relevant, Scottish Minister must personally take the decision to issue a warrant under this power to the security and intelligence services and Chief of Defence Intelligence. This ensures that they are accountable for the use of this power and have the opportunity in all cases to ensure that its use is necessary and proportionate.

266 There are some instances in which the Secretary of State or Scottish Minister will not be able to physically sign a warrant. In these circumstances a designated senior official may sign the warrant, as set out in subsections (3) (b) and (4) (b). The Secretary of State or Scottish Minister is still the decision maker in these instances and will confirm verbally with the designated official that he or she is in agreement that the warrant is to be signed.

Clause 96: Power to issue warrants to law enforcement officers

267 This clause establishes the process and requirements for targeted equipment interference warrants that are applied for by law enforcement officers and issued by law enforcement chiefs.

268 Subsection (1) sets out the conditions that must be met for a law enforcement chief to issue a targeted equipment interference warrant for the purpose of preventing or detecting serious crime. A law enforcement chief may only issue a targeted information warrant if he believes that the warrant is necessary to prevent and detect serious crime and that the conduct authorised is proportionate ((1) (a) and (1) (b)). Subsection (1) (d) provides that all decisions to issue a warrant require the prior approval of a Judicial Commissioner, except where the law enforcement chief believes there is an urgent case to issue the warrant. The process for urgent warrants is covered in clause 98. Subsection (1)(c) provides that in order to issue a warrant a law enforcement chief must be satisfied that satisfactory arrangements are in place to safeguard the material obtained (as detailed in clause 101). This mirrors the provision for warrants issued by the Secretary of State.

269 Subsection (2) enables warrants to be issued for purposes other than serious crime by specified law enforcement agencies. 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. In practice, this would permit certain law enforcement agencies to use equipment interference to locate and ensure the safety of vulnerable people, such as missing children. The law enforcement agencies that may apply for a warrant on these grounds is limited to the appropriate agencies named in Part 1 of Schedule 6.

270 Subsection (3) 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 when it is not reasonably practical for a law enforcement chief to consider the application and issue the warrant. The appropriate delegates in each law

enforcement agency that can apply for an equipment interference warrant is detailed in Schedule 6.

271 Subsections (5) to (10) refer to specific law enforcement agencies and variations or restrictions of the permitted purpose of targeted equipment interference warrants for each organisation. These variations and restrictions ensure that equipment interference can only be used in appropriate circumstances in relation to the purpose of each agency, for instance immigration officers may only be issued with an equipment interference warrant if the respective law enforcement chief considers that the warrant is necessary and the serious crime relates to an immigration or nationality offence (and all the other requirements of subsection (1)).

Schedule 6: Issue of warrants under section 96 etc: table

272 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 should apply to them in each case.

273 Paragraph 7 defines collaborative force and collaborative agreement in relation to a police force for the purpose of understanding the first three entries in the table.

274 Part 3 of the Schedule defines collaborative police force in relation to the National Crime Agency 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.

Clause 97: Approval of warrants by Judicial Commissioners

275 This clause explains the role of a Judicial Commissioner in approving targeted equipment interference and targeted examination warrants. Subsection (1) reiterates the same test of necessity and proportionality that the Secretary of State, Scottish Minister or law enforcement chief will have applied when issuing the warrant. The Judicial Commissioner, as per subsection 97 (2), will apply the same principles as they would apply in a judicial review and determine whether the person issuing the warrant has properly considered the necessity and proportionality of the operation or investigation.

276 Following their considerations a Judicial Commissioner can approve the decision to issue a warrant, refuse to approve the decision or refer the warrant to the Investigatory Powers Commissioner for further consideration.

277 Subsections (4) and (5) set out that should a warrant be refused by a Judicial Commissioner they must give written reasons for the refusal to the applicant. Should the person requesting the warrant so wish they may then refer the application to the Investigatory Powers Commissioner for their opinion.

Clause 98: Approval of warrants issued in urgent cases

278 This clause establishes the process for the approval of equipment interference warrants in urgent cases. These are warrants that will be issued in cases that demand very quick actions from the applicant that cannot wait until a Judicial Commissioner has approved the warrant. For example, in a serious crime context an urgent warrant may be required if a law enforcement agency understands that a person's life is in immediate danger and equipment interference would obtain communications and information, that may be used to prevent imminent harm. These warrants will still be issued by the Secretary of State, Scottish Minister or law enforcement chief (or appropriate delegate) and may be signed by the issuing authority personally or by a senior official if required.

279 Subsections (2) to (4) set out the role of the Judicial Commissioner once a warrant has been

issued through the urgent process. It is the duty of the person who issues an urgent warrant to inform the Judicial Commissioner that they have done so. This will prompt the Judicial Commissioner to either approve the warrant, allowing it to continue to have effect; or refuse to approve the warrant, in which case the activity described within the warrant should cease. This process must not exceed three working days.

280 If the Judicial Commissioner neither approves nor refuses to approve an urgent warrant it will cease to have effect five working days from the date that it was issued.

Clause 99: Failure to approve warrant issued in urgent case

281 This clause details the process that follows when a warrant is refused by a Judicial Commissioner, having previously been issued under urgent provisions.

282 The Judicial Commissioner has responsibility for determining what should be done with the material obtained up to this point. In all instances this will be the same Judicial Commissioner (or the Investigatory Powers Commissioner) that refused the warrant.

283 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.

284 Subsection (8) clarifies that if a warrant is refused, or not approved, the actions carried out whilst the warrant was active are not made invalid or unlawful by the ceasing of the warrant. This ensures that the recipient and their delegated officials can act appropriately and with confidence as soon as the urgent warrant is issued.

Clause 100: Items subject to legal privilege

285 This clause sets out the safeguards which apply when the purpose of a targeted equipment interference or examination warrant is to obtain items which are subject to legal privilege. Items subject to legal privilege are defined in subsection (7), and further information is provided in the Equipment Interference Code of Practice. In this case, the warrant application must make clear that the intention is to obtain items subject to legal privilege. The person authorising the warrant must be satisfied firstly that there are exceptional and compelling circumstances which make the acquisition or selection for examination of these items necessary, and secondly that there are specific arrangements in place for how these items will 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.

286 Where an agency applies for a targeted equipment interference warrant and believes that they may 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. Again, if the agency wishes to retain an item subject to legal privilege, the Investigatory Powers Commissioner must be informed as soon as possible.

Clause 101: Requirements which must be met by warrants

287 This clause details the criteria that must be included in targeted equipment interference warrants and targeted examination warrants.

288 The table at subsection (3) sets out the matters to which a warrant can relate and the details that must be included in a 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.

289 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.

Clause 102: Duration of warrants

290 Subsection (2) sets the standard duration of a warrant at 6 months. It also states when that 6 months begins, both for the initial warrant and any subsequent renewals. An exception applies for urgent warrants, which are described in subsection (3) and last for five working days.

Clause 103: Renewal of warrants

291 Subsections (1), (2) and (3) state that at any time before the warrant expires a renewal can be issued by the Secretary of State, Scottish Minister or law enforcement chief where relevant. In either case a Judicial Commissioner will also need to approve the renewal of the warrant. The person renewing the warrant will at this stage need to confirm that the activity described in the warrant remains necessary and proportionate.

292 Subsections (5) (6) and (7) ensures that any renewals are done personally by the Secretary of State, law enforcement chief (or appropriate delegate) or Scottish Minister where relevant. This provides the opportunity to review the necessity and proportionality of the action. The warrant will not be renewed if the action is no longer necessary or proportionate.

293 In the context of urgent warrants, renewals serve the purpose of allowing the Secretary of State, law enforcement chief (or appropriate delegate) or Scottish Minister and a Judicial Commissioner to review the warrant and, should they consider it necessary and proportionate, extend the duration to 6 months.

Clause 104: Modifications of warrants by the Secretary of State or Scottish Ministers

294 This clause addresses the possibility that warrants may need to be modified. For instance, a target of an investigation subject to an equipment interference warrant might acquire a new smart phone or a new subject of interest may become relevant to an investigation.

295 Subsection (2) sets out the different elements of a warrant that are subject to modification. These elements have the potential to change as an operation or investigation develops. Subsection (2) (c) ensures that any additions to the warranted activity are in relation to a matter to which the warrant relates. This means that modifications cannot alter the existing scope of the warrant.

296 Modifications can also include the removal of subjects from a warrant. This may occur, if during the course of an operation, it is determined that one or more of the subjects under the warrant are no longer of intelligence interest, but other subjects under the warrant remain of interest. In this instance the warrant can be modified to remove the unnecessary subjects from the warrant, minimising any incursions in to their privacy.

297 Modifications of this nature may be made by the Secretary of State or Scottish Minister (where relevant) or a senior official acting on their behalf, except in urgent circumstances. Where a modification is made by a senior official the Secretary of State or Scottish Minister must be notified of the modification and the reasons for making it. In urgent circumstances the person to whom the warrant is addressed or a person who holds a senior position in the same public authority may make a modification.

298 Any modifications must be considered both necessary on any relevant ground and proportionate to what is sought to be achieved by making the modification.

Clause 105: Approval of modifications under section 104 made in urgent cases

299 This clause sets out that once an urgent modification has been made a senior official designated by the Secretary of State or Scottish Minister must be informed and the Secretary of State or Scottish minister must also be notified.

300 Within five working days the designated senior official must decide whether to approve the modification and notify the person who made the modification of their decision. If the urgent modification is refused the modification will cease to have effect, the Secretary of State or Scottish Minister will be informed of the refusal 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 may then, if required, authorize 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.

Clause 106: Modification of warrants issued by law enforcement chiefs

301 This clause permits modifications to warrants issued by law enforcement chiefs.

302 Subsection (2) sets out the different elements of a warrant that are subject to modification. These elements have the potential to change as an operation or investigation develops. Subsection (2) (c) ensures that any additions to the warranted activity are in relation to a matter to which the warrant relates. This means that modifications cannot alter the existing scope of the warrant.

303 Modifications can also include the removal of subjects from a warrant. This may occur, if during the course of an operation, it is determined that one or more of the subjects under the warrant are no longer of intelligence interest, but other subjects under the warrant remain of interest. In this instance the warrant can be modified to remove the unnecessary subjects from the warrant, minimising any incursions in to their privacy.

304 Modifications of this nature may be made by the law enforcement chief or appropriate delegate that issued the warrant and, except in urgent circumstances, any modification must be approved by a Judicial Commissioner.

Clause 107: Approval of modification under section 106 in urgent cases

305 This clause sets out that once an urgent modification has been made a law enforcement chief or an appropriate delegate a Judicial Commissioner must be informed.

306 Within five working days the Judicial Commissioner must decide whether to approve the modification and notify the person who made the modification of their decision. 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, authorize 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.

Clause 108: Cancellation of warrants

307 This clause sets out that a Secretary of State, Scottish Minister, law enforcement chief (or appropriate delegate) or a designated senior official in a warrant granting department has the power to cancel a warrant at any time, if the warrant was originally issued by their

organisation.

308 Subsection (2) makes it a requirement that once a warrant is no longer necessary, or if through a change of circumstance the conduct is no longer proportionate, the appropriate person must cancel that warrant. This provision will ensure that equipment interference is not able to continue for any longer than is strictly necessary, minimising any potential incursions of privacy.

Clause 109: Implementation of warrants

309 Subsection (1) of this clause gives the recipient of the warrant the power to work with others to carry out the actions outlined in the warrant, this may include disclosure of material acquired under the warrant to the implementing authority. Subsection (2) specifies that the warrant recipient can serve a copy of the warrant to a person if they think that the person is able to help them carry out the warranted actions. Subsection (3) permits the person on whom the warrant is served to seek assistance from a person outside of the United Kingdom.

Clause 110: Service of warrants outside the United Kingdom

310 This clause sets out how a targeted equipment interference warrant may be served upon a person outside the United Kingdom when the warrant recipient requires their assistance. Subsection (2) sets out the three possible options for serving a warrant in this situation. Subsection (3) states that the third option set out in subsection (2) – to make the warrant available for inspection in the United Kingdom – should not be used unless the options under subsection (2) (a) and (b) are not reasonably practicable.

Clause 111: Duty of telecommunications operators to assist with implementation

311 This clause places a duty upon telecommunications providers to assist with the implementation of targeted equipment interference if they are served with a copy of a warrant by the warrant recipient.

312 Subsections (1) (2) and (3) set out that this duty is limited to a selection of organisations that mirrors the agencies permitted to use interception techniques. In all cases the Secretary of State or Scottish Minister will approve the proposed interference, even if the normal warrant process would not require their involvement (for instance, for warrants issued to law enforcement officers).

313 This clause 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.

314 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.

Clause 112: Safeguards relating to the retention and disclosure of material

315 This clause places a duty on the issuing authority to ensure safeguards are in place for any material acquired by the activity permitted through a targeted equipment interference warrant. This is intended to protect the privacy of anyone affected by a warrant and maintain the integrity of the operations to which the warrants relate.

316 This clause ensures that any disclosure of material derived from equipment interference is disclosed to the minimum level required and that copies of any material are kept to the minimum quantity required - and that disclosure and copying of material is only ever done if it is necessary for one of the relevant grounds as set out in subsection (7); is necessary for the

Secretary of State, Scottish Minister or warrant recipient to carry out their functions under this Bill; is necessary for the Investigatory Powers Commissioner or Investigatory Powers Tribunal to carry out their functions in relation to this Bill; is necessary for the purpose of legal proceedings; or is necessary for the performance of any person by or under any enactment. Subsection (5) ensures that material is destroyed as soon as there are no longer any grounds for retaining it.

Clause 113: Safeguards relating to disclosure of material overseas

317 This clause requires the issuing authority to consider that appropriate safeguards in relation to the disclosure, copying and destruction of material are in place before any material is shared with an overseas authority.

Clause 114: Duty not to make unauthorised disclosures

318 This clause explains what matters (subsection 4) may not be disclosed, and by whom. Any disclosure of such matters by the persons listed at subsection (3) will be considered unauthorised and subject to the offence detailed in clause 116. This does not apply if the disclosure is an 'excepted' disclosure, which are detailed in clause 115.

Clause 115: Section 114: meaning of "excepted" disclosure

319 This clause sets out the four categories of excepted disclosure. If a disclosure is made in line with any of these categories it is not unauthorised and the offence of making unauthorised disclosure does not apply. These categories have been designed to ensure that material derived from equipment interference can be used appropriately and responsibly, whilst protection sensitive information.

320 Disclosure is considered and excepted disclosure if it falls within one of the heads of disclosure.

Clause 116: Offence of making unauthorised disclosure

321 This clause states that a person commits an offence if a person discloses any material that should not have been disclosed, according to clause 114.

322 This clause makes clear that the offence should only apply where the person making the disclosure is aware that the disclosure of the material will breach the duty. This ensures that the offence only captures individuals who knowingly disclose material in breach of disclosure requirements and does not capture those who may disclose EI material unknowingly (as not clear the material was obtained under EI warrant/subject to disclosure restrictions).

Clause 117: Restriction on issue of warrants to certain law enforcement officers

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

324 Subsection (2) lists the forces that may only apply for an equipment interference warrant where there is a connection to the British Islands. Subsection (3) also extends this provision to collaborative forces led by the National Crime Agency.

325 Subsection (4) described a connection to the British Islands as:

- a. the proposed activity would take place in the British Islands (regardless of where the equipment to be interfered with is located); or
- b. the UK police force believes the equipment to be interfered with may be located in the British Islands at some point during the interference itself. The computer equipment

could be located in the British Islands or carried by someone transiting through the British Islands, for example, 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.

326 Subsection (5) provides that all other law enforcement officers are able to apply for an equipment interference warrant under clause 96 in circumstances where there is a connection to the British Islands and also where there is no connection to the British Islands.

Clause 118: Part 5: Interpretation

327 This clause provides definitions for ‘communication’, ‘equipment’, ‘equipment data’, ‘private information’, ‘senior official’ and ‘targeted examination warrant’ that ensure that all intended applications of equipment interference are captured under the powers set out in this Bill. Part 6: Bulk warrants

Chapter 1: Bulk interception warrants

Clause 119: Bulk interception warrants

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

329 The main purpose for which a warrant may be sought 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 people in the British Islands.

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

331 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.

332 Subsection (5) sets out the 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 any activity for obtaining secondary data.

333

Example:

A bulk warrant is sought for the interception of communications. The primary objective of the warrant is to obtain the communications of persons believed to be outside the UK, which are likely to be of national security interest and may be selected for examination subsequently. Due to the nature of internet-based communications, it is inevitable that some communications between persons in the UK will also be intercepted. In order to 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 judge.

Clause 120: Obtaining secondary data

334 This clause provides for the obtaining of secondary data under a bulk interception warrant.

Secondary data means:

- a. Systems data – which is defined in clause 225 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;
- b. Identifying data which can be logically separated from the communication and which does not, once separated, reveal the meaning of the content of the communication. Identifying data is defined in clause 225 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.

335 Secondary data as defined in this clause may be obtained under a bulk interception warrant and, once the data is obtained, will be subject to the safeguards set out in Chapter 1 of Part 6.

336 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 (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 contact 'mailto' addresses within a webpage.

Clause 121: Power to issue bulk interception warrants

337 This clause sets out the power to issue bulk interception warrants. Subsections (1) to (7) set out the power for the Secretary of State to issue a bulk interception warrant, only where it is necessary and proportionate, for one or more specified statutory purposes. The interests of national security must always be one of those purposes. A bulk interception warrant may only be issued to one of the three intelligence agencies. The decision to issue a warrant must also be approved by a Judicial Commissioner,

338 Subsection (1) also requires the Secretary of State to believe it is necessary to examine material obtained under the warrant for specified operational purposes. Operational purposes limit the purposes for which data collected under a warrant can be selected for examination and no official is permitted to gain access to the data other than as permitted by these purposes. 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 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 purposes. Operational purposes will provide the Secretary of State and Judicial Commissioner with a granular picture of the purposes for which the intercepted content and secondary data collected under a warrant can be selected for examination.

339 Subsection (5) requires the Secretary of State, when considering whether the warrant is necessary and proportionate, to take into account whether the information it is thought necessary to obtain under the warrant could reasonably be obtained by other means.

Clause 122: Additional requirements in respect of warrants affecting overseas operators

340 This clause outlines the requirements relating to warrants that the Secretary of State believes are likely to require the assistance of a telecommunications operator who is based outside the United Kingdom to give effect to.

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

342 Subsection (3) sets out factors that must be taken into account before issuing the warrant in those cases. These include costs and technical feasibility, as well as the likely benefits of the warrant.

Clause 123: Approval of warrants by Judicial Commissioners

343 Subsection (1) sets out the matters that must be reviewed by a Judicial Commissioner when deciding whether to approve the decision to issue a bulk interception warrant, including a consideration of necessity and proportionality and the necessity of the operational purposes.

344 Subsection (2) requires that, in determining the matters in subsection (1), a Judicial Commissioner must apply judicial review principles.

Clause 124: Decisions to issue warrants to be taken personally by Secretary of State

345 This clause requires the Secretary of State personally to take the decision to issue a bulk interception warrant. The warrant must be signed by the Secretary of State before it can be issued.

Clause 125: Requirements that must be met by warrants

346 This clause sets out the information which must be contained in a bulk interception warrant. Subsection (3) requires that a warrant must set out the operational purposes for which any intercepted content or secondary data obtained under the warrant can be selected for examination. Subsection (4) makes clear that it is not sufficient for operational purposes to use the wording of one of the statutory purposes. Operational purposes must include more detail to ensure that intercepted content or secondary data can only be selected for examination for specific reasons.

347 Subsection (5) makes clear that a bulk interception warrant may specify however many operational purposes are considered will be, or may be, necessary for the examination of content and secondary data obtained under the warrant. Given the global nature of internet communications and reflecting the fact that bulk interception is primarily an intelligence gathering tool, bulk interception warrants are highly likely to specify a large number of operational purposes. Each operational purpose included on the warrant must have been agreed by the Secretary of State and approved by a Judicial Commissioner before the warrant can be issued, in line with clause 121.

Clause 126: Duration of warrants

348 This clause sets out the details surrounding the duration of a bulk interception warrant. Bulk interception warrants will last for six months, beginning on the day the warrant was issued.

Clause 127: Renewal of warrants

349 This clause sets out the conditions for renewing a bulk interception warrant. The decision to renew a bulk interception warrant must be taken personally by the Secretary of State.

350 Subsection (2) sets out the conditions that must be met for a warrant to be renewed. The Secretary of State believes that the warrant continues to be necessary and proportionate in relation to relevant statutory purpose(s) and the decision to renew the warrant has also been approved by a Judicial Commissioner.

Clause 128: Modification of warrants

351 This clause sets out the conditions for modifying a bulk interception warrant.

352 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.

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

354 Subsection (7) provides for a senior official, acting on behalf of the Secretary of State, to make a modification to remove an operational purpose or to cancel the interception of communications. Subsection (12) provides that where a warrant is modified to cancel the interception of communications it remains a bulk interception warrant. Subsection (8) requires that, where this is the case, the Secretary of State must be personally notified of the modification, as well as the reasons for making it.

355 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.

356 Subsection (11) provides that where there is a need to make a 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 the 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.

357 Subsection (13) provides that a warrant may be modified in a way which does not affect the conduct authorised or required by it.

Clause 129: Approval of major modifications made in urgent cases

358 This clause sets out the process for approving a major modification to a bulk interception warrant which has been made urgently, as per subsection (11) of Clause 128. In this case, the Secretary of State must inform a Judicial Commissioner that the modification has been made. The Judicial Commissioner has five working days from the date of the modification in which to approve the decision to modify the warrant. If he or she refuses it, the modification no longer has effect, and anything done as a result of that modification must stop as soon as possible.

Clause 130: Cancellation of warrants

359 This clause sets out the circumstances under which a bulk interception warrant may be cancelled.

360 Subsection (2) requires that where a Secretary of State or senior official decides the warrant is no longer necessary, or the conduct authorised by it is no longer proportionate, he or she must cancel the warrant. A warrant may also be cancelled by the Secretary of State or a senior official at any time.

Clause 131: Implementation of warrants

361 This clause 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.

Clause 132: Safeguards relating to retention and disclosure of material

362 This clause 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.

Clause 133: Safeguards relating to disclosure of material overseas

363 This clause sets out the safeguards relating to the disclosure of intercept material overseas in relation to a bulk interception warrant. These replicate the safeguards for overseas disclosure in relation to targeted interception warrants.

Clause 134: Safeguards relating to examination of material

364 This clause 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.

365 Subsection (4) places a prohibition on selecting intercepted material for examination if any criteria used for the selection of that material refer to an individual known to be currently in the British Islands and are aimed at identifying the content of communications sent by or intended for that individual. Where such examination is required, a targeted examination warrant must be obtained, issued by the Secretary of State and the decision to issue the warrant must be approved by the Judicial Commissioner.

Example:

A member of an intelligence service is investigating an international terrorist group and one of that group regularly travels to the UK. In order to enable the selection of that person's communications for examination, including during the periods when he is in the UK, a targeted examination warrant must be sought. This will need to be issued by the Secretary of State and approved by a judge.

366 Subsections (5) to (7) deal with cases in which there is a change of circumstances such that a person whose communications were being selected for examination is discovered to be in the British Islands or has entered the British Islands. In those cases, a senior official may authorise the continued selection for examination for a period of five 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 his communications. This authorisation only lasts for five working days, after which the selection for examination of his communications must cease or a targeted examination warrant must be sought. This will need to be issued by the Secretary of State and the decision to issue the warrant approved by a judge before any further selection is permitted.

Clause 135: Additional safeguards for items subject to legal privilege

367 This clause 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), and (whether the acquisition of such items is intended or merely a possibility) specific arrangements are in place for how these items will be handled, retained, used and destroyed.

Clause 136: Application of other restrictions in relation to warrants

368 This clause sets out that the exclusion of matters from legal proceedings apply to bulk interception warrants. The duty not to make unauthorised disclosure also applies to bulk interception warrants.

Clause 137: Chapter 1: interpretation

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

Chapter 2: Bulk acquisition warrants

Clause 138: Power to issue bulk acquisition warrants

370 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 on behalf of the three intelligence agencies.

371 Subsection (1) also requires the Secretary of State to believe it is necessary to examine material obtained under the warrant for specified operational purposes. This will provide a detailed list of purposes for which examination of bulk communications data may be necessary. Before selecting any material for examination, a member of a security and intelligence agency will need to be sure that the examination is necessary for one of those purposes.

372 Subsection (4) requires the Secretary of State, when considering whether the warrant is necessary and proportionate, to take into account whether the information it is thought necessary to obtain under the warrant could reasonably be obtained by other means.

- 373 Subsection (5) describes a bulk acquisition warrant. Subsection (6) sets out that the warrant authorises requiring a telecommunications operator to disclose specified communications data in its possession or obtain and disclose communications data which is not in its possession; the selection for examination of the data obtained under the warrant and the onward disclosure of such data.
- 374 Subsection (7) provides for a bulk acquisition warrant to authorise conduct necessary to do what is required by the warrant.
- 375 Subsection 89) provides that a bulk acquisition warrant may be issued on a forward looking basis.
- 376 Subsection (9) requires an application for the issue of a bulk acquisition warrant to be made by or on behalf of the head of an intelligence agency.

Clause 139: Approval of warrants by Judicial Commissioners

- 377 Subsection (1) sets out the matters that must be reviewed by a Judicial Commissioner when deciding whether to approve a bulk acquisition warrant, including a consideration of necessity and proportionality and the necessity of the operational purposes.
- 378 Subsection (2) requires that, in determining the matters in subsection (1), a Judicial Commissioner must apply judicial review principles.
- 379 Where a Judicial Commissioner refuses to approve a warrant they must set out written reasons for their refusal. This will allow the agency requesting the warrant to alter their application and what action they are seeking to take in order to meet any concerns expressed by the Judicial Commissioner.
- 380 Should a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuse to approve a decision to issue a warrant the Secretary of State may escalate the case to the Investigatory Powers Commissioner and ask them to approve the decision to issue the warrant. Should the Investigatory Powers Commissioner refuse to approve the warrant then there is no further right of appeal from that decision.

Clause 140: Decisions to issue warrants to be taken personally by Secretary of State

- 381 This clause requires that the decision to issue a bulk acquisition warrant must be taken by the Secretary of State. The Secretary of State must sign the warrant before it is issued.

Clause 141: Requirements that must be met by warrants

- 382 This clause sets out the information which must be contained in a bulk acquisition warrant. Subsection (3) requires that a warrant must set out the operational purposes for which any communications data obtained under the warrant can be selected for examination. Subsection (4) makes clear that it is not sufficient for operational purposes to use the wording of one of the statutory purposes. They must include more detail to ensure that communications data can only be selected for examination for specific reasons.
- 383 Subsection (5) makes clear that a bulk interception warrant may specify however many operational purposes are considered will be, or may be, necessary for the examination of content and secondary data obtained under the warrant. As a bulk acquisition warrant may lead to the collection of communications data that is relevant to a range of operational purposes. Accordingly bulk acquisition warrants are highly likely to specify a large number of operational purposes. Each operational purpose included on the warrant must have been agreed by the Secretary of State and approved by a Judicial Commissioner before the warrant can be issued.

Clause 142: Duration of warrants

384 This clause sets out that a bulk acquisition warrant has a duration of six months from the date of issue or, in the case of a renewed warrant, from the day after it would otherwise have expired.

Clause 143: Renewal of warrants

385 This clause sets out the conditions for renewing a bulk interception warrant. The decision to renew a bulk acquisition warrant must be taken personally by the Secretary of State.

386 Subsection (2) sets out the conditions that must be met for a warrant to be renewed. These include that the Secretary of State believes that the warrant continues to be necessary and proportionate in relation to relevant statutory purpose(s) and that the decision to renew the warrant has also been approved by a Judicial Commissioner.

Clause 144: Modification of warrants

387 This clause sets out the conditions for modifying a bulk acquisition warrant.

388 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.

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

390 Subsection (7) provides for a senior official, acting on behalf of the Secretary of State, to make a modification where an operational purpose is being removed or where the collection of data is being ceased. Subsection (8) requires that, where this is the case, the Secretary of State must be personally notified of the modification, as well as the reasons for making it.

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

392 Subsection (11) provides that where there 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.

393 Subsection (13) provides that a warrant may be modified in a way which does not affect the conduct authorised or required by it.

Clause 145: Approval of major modifications made in urgent cases

394 This clause sets out the process for approving a major modification to a bulk acquisition warrant which has been made urgently, as per subsection (5) of clause 144. In this case, the Secretary of State must inform a Judicial Commissioner that the modification has been made. The Judicial Commissioner has three working days from the date of the modification in which to approve it. If they refuse it, the modification no longer has effect, and anything done as a result of that modification must stop as soon as possible.

Clause 146: Cancellation of warrants

395 This clause sets out the circumstances under which a bulk acquisition warrant may be cancelled.

396 Subsection (2) requires that where a Secretary of State or senior official decides the warrant is no longer necessary, or the conduct authorised by it is no longer proportionate, they must cancel the warrant. The Secretary of State or a senior official may also cancel a warrant at any time.

Clause 147: Implementation of warrants

397 This clause sets out how a bulk acquisition warrant is implemented, including assistance with giving effect to the warrant and how the warrant may be served.

Clause 148: Service of warrants outside the United Kingdom

398 This clause sets out the process for serving a bulk acquisition warrant on a person outside the United Kingdom.

Clause 149: Duty of operators to assist with implementation

399 This clause requires a telecommunications operator to take whatever steps are necessary to give effect to a bulk acquisition warrant. The operator is not required to take steps which are not reasonably practicable. Subsection (2) clarifies that this clause applies whether or not the provider is in the UK.

400 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.

Clause 150: Safeguards relating to the retention and disclosure of data

401 This clause sets out the safeguards which apply to bulk acquisition warrants. Subsection (2) requires the Secretary of State concerned to ensure arrangements are in place to limit the disclosure of data to the minimum necessary for an authorised purpose. Data must be held securely and destroyed when there are no longer grounds for retaining it. Subsection (9) provides protection for data disclosed to authorities of a country or territory outside the UK.

Clause 151: Safeguards relating to examination of data

402 This clause provides that data obtained under a warrant may only be examined in accordance with the operational purposes specified in the warrant and only when necessary and proportionate.

Clause 152: Offence of making unauthorised disclosure

403 This clause makes it an offence for persons specified in subsection (1) to make an unauthorised disclosure to another person in relation to a bulk acquisition warrant. Subsection (2) lists the circumstances where disclosure is authorised. Subsection (3) sets out the maximum penalties for the offence.

Clause 153: Chapter 2: interpretation

404 This clause defines the terms used in this Chapter.

Chapter 3: Bulk equipment interference warrants

Clause 154: Bulk equipment interference warrants: general

405 This clause sets out the characteristics of bulk equipment interference, and sets out the conditions that a warrant issued under this chapter must meet, differing from the targeted equipment interference regime.

406 The main purpose for which a warrant may be sought is limited to interference 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 people in the British Islands or information relating to people in the British Islands.

407 Subsection (2) defines “overseas-related communications” and “overseas-related information”.

408 Subsection (5) sets out that a bulk equipment interference warrant also authorises conduct necessary to do what is required by the warrant.

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.

Clause 155: Meaning of “equipment data”

409 This clause defines the material which is equipment data in relation to a bulk equipment interference warrant. Equipment data means:

- a. Systems data – which is defined in clause 225 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;
- b. Identifying data which can be logically separated from the communication or item of information and which does not, once separated, reveal the meaning of the content of the communication or the meaning (if any) of an item of information (disregarding any inferred meaning). Identifying data is defined in clause 225 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.

410 Equipment data as defined in this clause may be obtained under a bulk equipment interference warrant and, once the data is obtained, will be subject to the safeguards set out in Chapter 3 of Part 6.

411 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.

412 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 contact 'mailto' addresses within a webpage

Clause 156: Power to issue bulk equipment interference warrants

406 This clause provides the power for the Secretary of State to issue a bulk equipment interference warrant, only where it is necessary and proportionate on behalf of an intelligence agency for one or more specified statutory purposes. The interests of national security must always be one of those purposes. It also requires the Secretary of State to believe it is necessary to examine material obtained under the warrant for specified operational purposes. A bulk equipment interference warrant may only be issued to one of the three intelligence agencies. Except in urgent cases the decision to issue a bulk equipment interference warrant must be authorised by a Judicial Commissioner before the warrant can be issued.

Clause 157: Approval of warrants by Judicial Commissioners

407 Subsection (1) sets out the matters that must be determined by a Judicial Commissioner when deciding whether to approve the decision by a Secretary of State to issue a bulk equipment interference warrant.

408 Subsection (2) requires that, in determining the matters in subsection (1), a Judicial Commissioner must apply judicial review principles.

409 Subsections (3) and (4) set out that a Judicial Commissioner can either approve the decision to issue a warrant, refuse to approve the decision to issue a warrant or refer the application to the Investigatory Powers Commissioner for further consideration.

Clause 158: Approval of warrants issued in urgent cases

410 This clause sets out that a bulk equipment interference warrant may be issued in an urgent case, without the approval of a Judicial Commissioner, in the same way as targeted equipment interference warrants. This enables a warrant to be issued where there is insufficient time to seek the Judicial Commissioner's approval, for example, to counter unanticipated emerging threats.

411 Subsection (3) requires a Judicial Commissioner to consider the warrant within three working days of issuing and inform the Secretary of State of their decision. If the decision to issue the urgent warrant is refused it will cease to have effect.

Clause 159: Failure to approve warrant issued in urgent case

412 This clause details the process that follows when the decision to issue an urgent bulk equipment interference warrant is refused by a Judicial Commissioner.

413 The Judicial Commissioner has responsibility for determining what should be done with the material obtained up to the point of refusing to approve the issue of the warrant.

414 Subsection (3) 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.

415 Subsection (8) clarifies that if the decision to issue an urgent warrant is refused, or not approved, the actions carried out whilst the warrant was active are not made invalid or

unlawful by the ceasing of the warrant. This ensures that the recipient and their delegated officials can act appropriately and with confidence as soon as the urgent warrant is issued.

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

416 This clause ensures that the decision to issue a bulk equipment interference warrant may only be taken by a Secretary of State. Subsection (2) sets out that the warrant may be signed by either the Secretary of State or, if not reasonably practicable, a designated senior official.

Clause 161: Requirements that must be met by warrants

417 This clause sets out the information which must be contained in a bulk equipment interference warrant.

418 Subsection (3) requires the warrant to describe conduct authorised by the warrant, with the warrant setting out the type of interference which will take place.

419 Subsection (4) requires that a warrant must set out the operational purposes for which any material obtained under the warrant can be selected for examination. Subsection (5) makes clear that it is not sufficient for operational purposes to use the wording of one of the statutory purposes. Operational purposes must include more detail to ensure that material under the warrant can only be selected for examination for specific reasons. For example, the person requesting the warrant might for example state that the proposed interference will be used to gather intelligence relating to terrorism in a particular country.

420 Subsection (6) makes clear that a bulk equipment interference warrant may specify however many operational purposes are considered will be, or may be, necessary for the examination material obtained under the warrant. This reflects the fact that bulk equipment interference warrants are highly likely to specify a large number of operational purposes. Each operational purpose included on the warrant must have been agreed by the Secretary of State and approved by a Judicial Commissioner before the warrant can be issued.

Clause 162: Duration of warrants

421 This clause sets out the details surrounding the duration of a bulk equipment interference warrants. Upon approval, bulk equipment interference warrants will last for a maximum of six months. Urgent warrants will last for five working days, unless renewed. The original decision to issue the urgent warrant will also have to been approved by a Judicial Commissioner within three working days from when it was first issued.

Clause 163: Renewal of warrants

422 This clause sets out the conditions for renewing a bulk equipment interference warrant. The decision to renew a bulk equipment interference warrant must be taken personally by the Secretary of State. The Secretary of State must consider that it continues to be necessary and proportionate. The requirements relating to statutory and operational purposes which had to be met when the warrant was first issued have to continue to be satisfied. The Secretary of State's decision to renew a warrant does not come into effect unless a Judicial Commissioner, upon reviewing the decision, approves it.

423 In the context of urgent warrants, renewals serve the purpose of allowing the Secretary of State and a Judicial Commissioner to review the warrant and, should they consider it necessary and proportionate, extend the duration to six months.

Clause 164: Modification of warrants

424 This clause sets out the conditions for modifying a bulk equipment interference warrant.

Modifications to bulk equipment interference warrants follow the same authorisation process as a new warrant application. Accordingly, any element of the warrant may be modified, but

the decision to modify the warrant must be approved by a Judicial Commissioner before it can take effect.

425 The only category where a non-urgent modification is not subject to approval from a judicial commissioner is where the modification is to remove an operational purpose specified in the warrant or removing any description of conduct authorised by the warrant. These are described as ‘minor modifications’. In such circumstances, the Secretary of State may delegate the authority to a senior official. If a senior official makes a minor modification they must inform the Secretary of State of this change.

426 Subsection (11) provides that where there 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.

427 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.

Clause 165: Approval of major modifications made in urgent cases

428 This clause provides for a Secretary of State to make a ‘major’ modification (i.e. to add or vary any operational purposes or description of conduct in the warrant), without the prior approval of a Judicial Commissioner. The decision to make an urgent modification must be reviewed by a Judicial Commissioner within five working days. If they refuse to approve, the activity authorised must cease as far as reasonably practicable.

429 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.

430 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. This ensures that the recipient and their delegated officials can act appropriately and with confidence as soon as the urgent warrant is issued.

Clause 166: Cancellation of warrants

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

432 Subsection (2) ensures that if an appropriate person is satisfied that the warrant is no longer required, they must cancel it. A warrant may be cancelled by the Secretary of State or a senior official at any time.

Clause 167: Implementation of warrants

433 This clause sets out the requirements for giving effect to a bulk equipment interference warrant. This replicates the provisions relating to the implementation of a targeted equipment interference warrant and ensures that a person to whom the warrant is addressed may work with others to effect the activity described within it.

434 Subsection (5) states that the same provision for targeted equipment interference, that allows a

warrant holder to compel a telecommunications provider to assist in the implementation of warranted activity, applies in the same way for bulk equipment interference.

Clause 168: Safeguards relating to retention and disclosure of material

435 This clause sets out the general safeguards which apply to bulk equipment interference warrants. This replicates the general safeguards which apply to the handling of targeted equipment interference warrants.

436 The clause ensures that any disclosure of the information obtained through bulk equipment interference is kept to a minimal amount. Any copies of the information are also kept to a minimum. However subsection (3) is clear that the disclosure of material obtained under a bulk equipment interference warrant is permitted in where necessary for the purposes of legal proceedings, ensuring that this material can be used as evidence when required.

Clause 169: Safeguards relating to disclosure of material overseas

437 This clause requires the issuing authority to consider that appropriate safeguards in relation to the disclosure, copying and destruction of material are in place before any material is handed over to an overseas authority. These replicate the safeguards for overseas disclosure in relation to targeted equipment interference warrants.

Clause 170: Safeguards relating to examination of material etc.

438 This clause sets out the safeguards relating to the examination of material which has been acquired under a bulk equipment interference warrant.

439 Subsection (3) introduces the safeguards that apply to ‘protected material’ (as defined in subsection (9)). This is any material of persons within the British Islands, mirroring the safeguards provided in the bulk interception regime. Where protected material of a person in the UK is being targeted for examination, a targeted EI warrant will be required.

440 This distinction ensures that any examination of protected material related to persons in the UK, obtained through bulk equipment interference, is specifically authorised by the Secretary of State and a Judicial Commissioner on the grounds of necessity and proportionality.

Example:

A member of an intelligence service is targeting a hostile foreign intelligence officer through a bulk equipment interference operation. The foreign intelligence officer is overseas, so the analyst can examine the content that they acquire through the provisions made in the bulk equipment interference warrant. That foreign intelligence officer decides to visit the UK. At this point, a targeted equipment interference examination warrant must be sought in order to examine any content acquired through bulk equipment interference relating to the target.

Clause 171: Additional safeguards for items subject to legal privilege

441 This clause includes additional safeguards to activity that may result in the acquisition or examination of items subject to legal privilege, equivalent to those provided in the targeted equipment interference regime.

442 If the criteria used to select material for examination will, or would be likely to, identify items subject to legal privilege the Secretary of State or designated senior official must then only issue the warrant if they consider that there are exceptional circumstances to merit such

activity and if they are satisfied that specific safeguards are in place for the handling, retention, use and destruction of such items.

443 Subsection (4) requires a person retaining any items subject to legal privilege to inform the Investigatory Powers Commissioner of the retention as soon as reasonably practicable.

Clause 172: Application of other restrictions in relation to warrants

444 This clause applies the targeted equipment interference clauses relating to unauthorised disclosure of material acquire under a warrant, to the bulk equipment interference regime.

Clause 173: Chapter 3: interpretation

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

Part 7: Bulk personal datasets

Clause 174: Bulk personal datasets: interpretation

446 Subsection (1) sets out the circumstances in which, for the purposes of this Bill, an intelligence service retains a bulk personal dataset (BPD). An intelligence service is defined in the general definitions clause of the Bill to mean the Security Service (MI5), Secret Intelligence Service (MI6) or GCHQ. As a result, the safeguards set out in later clauses must be followed if these circumstances are met.

447 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 is because the bulk personal datasets that an intelligence service may retain or examine might include data relating to deceased persons.

Example:

The electoral roll, which would be a bulk personal dataset if it was retained by an intelligence service and held in one of its analytical systems, will inevitably include persons who are deceased given it is not updated constantly.

Clause 175: Requirement for authorisation by warrant: general

448 This clause specifies that an intelligence service may not exercise a power to retain or examine a BPD without a warrant. Subsection (3) describes the two types of warrant provided for under this Part of the Bill – a ‘class BPD warrant’ and a ‘specific BPD warrant’.

Clause 176: Exceptions to Section 175(1) and (2)

449 This clause explains when the general requirements listed in the previous clause do not apply. Subsection (1) states that a BPD warrant is not required if the BPD has been obtained under another regime outlined in this Bill - for example if a BPD is obtained by interception, carried out under an interception warrant.

450 Subsection (2) clarifies that BPD 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 agency to delete the applicable dataset immediately from their systems. This provision allows the agencies to hold the BPD while they are ensuring that the relevant data is entirely removed from their systems and ensure that they

are legally compliant.

451 Subsection (3) explains that other exceptions to clause 175(1) and (2) are contained in clauses 181(8), 189(7) and 190(5).

Clause 177: Class BPD warrants

452 This clause explains how the class BPD warrant authorisation process works. A class 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.

453 Subsection (2) specifies what an application for a class warrant must include – a description of the class of BPD and, if applicable, the operational purposes for which the intelligence agency wishes to examine datasets of that class.

454 Subsection (3) explains that a Secretary of State can issue a class warrant (thus enabling the retention and examination of BPDs 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 (for example, protective security measures) 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. (A subsequent clause includes further provision relating to approval of warrants by the Judicial Commissioner, including that in deciding this matter the Judicial Commissioner applies judicial review principles.)

455 Subsection (4) explains that an application can only be made on behalf of the head of an intelligence service by a person holding office under the Crown.

Clause 178: Specific BPD warrants

456 This clause explains how the specific BPD warrant authorisation process works. The Bill 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.

457 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.

458 Subsection (3) describes the second case where a specific BPD warrant may be applied for. This is when a dataset falls within a class warrant, but, for any reason, the intelligence service believes that it would be appropriate to seek a specific warrant. An example of this could be when an intelligence agency receives a dataset that, while already covered by a class warrant, could raise international relations concerns such that the intelligence agency believes that the Secretary of State should decide whether to authorise retention and use of that specific dataset. Another example could be where the nature or the provenance of the dataset raises particularly novel or contentious issues; if it contains a significant component of intrusive data; or if it contains a significant component of confidential information relating to members of sensitive professions.

459 The information that must be included in the application is set out in subsection (4) – a

description of the specific dataset and, if applicable, the operational purposes for which the dataset is to be examined.

460 Subsection (5) describes the conditions which must be met before a specific BPD warrant can be issued by the Secretary of State. They are the same ones as for a class BPD warrant: the Secretary of State can issue a specific warrant if s/he believes that it is necessary for specified purposes and proportionate, and that adequate handling arrangements (for example through appropriate protective security measures) are in place. 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 clause 180), a Judicial Commissioner must have approved the Secretary of State's decision to issue a warrant before the warrant can be issued. (A subsequent clause includes further provision relating to approval of warrants by the Judicial Commissioner, including that in deciding this matter the Judicial Commissioner applies judicial review principles.)

461 Subsection (6) 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 (6) allows the agencies to retain and examine this updated data under the existing authorisation and without the need for a new specific BPD warrant.

462 Subsection (7) explains that an application can only be made on behalf of the head of an intelligence service by a person holding office under the Crown.

Clause 179: Approval of warrants by Judicial Commissioners

463 This clause 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 Bill (e.g. in authorising interception warrants).

Clause 180: Approval of specific BPD warrants issued in urgent cases

464 This clause applies to specific BPD warrants only. If the Secretary of State believes 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, the 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 their decision. This is the same approach as for urgent targeted interception warrants.. Subsection (4) explains that if the Commissioner refuses to approve the decision to issue the warrant, it ceases to have effect.

Clause 181: Failure to approve specific BPD warrant issued in urgent case

465 This clause explains the process if a Judicial Commissioner refuses to approve a specific 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 to do 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 retention or examination of any of the material. 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. Subsection (8) makes clear that an intelligence service is not in breach of the requirement for a warrant under subsections (1) and (2) of clause 175 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) of clause 181. Subsection (9) ensures that actions taken in reliance on a warrant before it ceases to have effect or at the point it ceases to have effect (and which cannot reasonably be stopped) remain lawful.

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

466 This section specifies that the decision to issue a class or specific BPD warrant must be taken personally by the Secretary of State. A warrant must also be signed by the Secretary of State. 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.

Clause 183: Requirements that must be met by warrants

467 This clause explains that a BPD warrant 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 BPD or BPDs can be selected for examination. Subsection (5) makes clear that it is not sufficient for operational purposes to use the wording of one of the statutory purposes set out in subsection (3)(a) of clause 177 or subsection (5)(a) of clause 178. Whilst the operational purposes may still be general, they must include more detail than the statutory purposes, in order to provide better understanding of the reasons for which the agency can select for examination data from a BPD or BPDs.

Clause 184: Duration of warrants

468 This clause explains that, for non-urgent warrants, the warrant has effect on the day on which it is issued or, in the case of a renewed warrant, the day following the day on which it would otherwise have ceased to have effect. In either case, it lasts for six months. An urgent warrant 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 Bill.

Clause 185: Renewal of warrants

469 Subsections (1) to (3) set out that the Secretary of State may renew a 'class' or 'specific' BPD warrant if he or she continues to believe it is necessary and proportionate; if he or she considers 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) of clause 177 or subsection (5)(a) of clause 178; and provided that his/her renewal decision is approved by a Judicial Commissioner. This is consistent with other forms of warrant in the Bill.

Clause 186: Modification of warrants

470 This clause explains the process by which BPD warrants can be modified, what constitutes a major or minor modification to a BPD warrant and who is authorised to make or approve those modifications. The only modification that can be made to any BPD warrant is to add, vary or remove an operational purpose. The clause also provides for major modifications (the addition or varying of an operational purpose) in urgent circumstances. These provisions are consistent with equivalent clauses in Part 6 of the Bill.

471 Subsection (11) provides that where there 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.

Clause 187: Approval of major modifications made in urgent cases

472 This clause 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 BPD warrant, this may be made without the approval of the Judicial Commissioner. If this happens, the 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 his/her decision. This is the same approach as for urgent modifications of targeted interception warrants, and is consistent with equivalent clauses in Part 6 of the Bill. Subsection (4) explains that if the Commissioner refuses to approve the modification decision to the warrant, it ceases to have effect.

Clause 188: Cancellation of warrants

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

Clause 189: Non-Renewal or cancellation of BPD warrants

474 This clause 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 obtained under that warrant. The material may be destroyed; clause 176(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 security and intelligence agency may consider it necessary and proportionate to retain some or all of the material that had been retained under the authority of that warrant. Clause 189 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.

475 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 BPD should be retained, but that it is necessary and proportionate to retain a subset or subsets of that material. If the Judicial Commissioner does not approve a decision to authorise the continued retention or examination of any of the material, he or she must give the Secretary of State written reasons for this (subsection (4)). Subsection (5) provides that if a Judicial Commissioner other than the Investigatory Powers Commissioner does not approve such a decision, the Secretary of State can ask the Investigatory Powers Commissioner to decide whether to approve the decision.

476 Subsection (6) 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. Subsection (7) makes provision for time limits in relation to this clause, and

provides that if those time limits are adhered to then the retention and examination of the data throughout the process remains lawful.

Clause 190: Initial Examination: time limits

- 477 This clause explains the process of, and sets time limits for, the initial examination of a BPD. Subsection (1) states that this section applies when a security and intelligence agency obtains 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 agency in the exercise of its functions (and so the information may be BPD or may include BPD).
- 478 Subsection (2) outlines the steps that the intelligence service must take, and requires these steps to be taken within a set period. These steps are: an initial examination to determine whether it is BPD; 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).
- 479 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 BPD 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 BPD during that period for the purpose of applying for the warrant.

Clause 191: Safeguards relating to the examination of bulk personal datasets

- 480 This clause outlines safeguards relating to the examination of BPDs under a class or specific BPD warrant. Data can only be selected for examination from the BPD for an operational purpose specified in the warrant, and the selection of that data must be necessary and proportionate.

Clause 192: Application of Part 7 to bulk personal datasets obtained under this Act

- 481 This clause relates to BPD obtained by a security and intelligence agency using a capability for which a warrant or other authorisation was issued or given under the Act. The general rule is that Part 7 of the Bill does not apply to BPD acquired pursuant to such a warrant or authorisation, as a result of the exception set out in clause 176(1). Instead, any provisions from the regime governing the acquisition capability that are relevant to the BPD will apply. However, under clause 192 the security and intelligence agency can apply to the Secretary of State for a direction which has the effect of applying the Part 7 regime to the BPD, thereby displacing the exception in 176(1).
- 482 The direction will confirm that the power of the security and intelligence agency to retain and examine the BPD arises under the direction; that any other power to do so ceases to apply; and that any associated regulatory provision (as defined in subsection (13)) arising in the acquisition capability 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 BPD obtained by interception which identifies itself as the product of interception, such a direction may not disapply the provisions in clause 48 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 clauses 49 to 51 of the Act. These clauses 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.

483 Such a direction can only be given with the approval of a Judicial Commissioner. The effect of such a direction will be that a Part 7 warrant is required to retain and examine the BPD, and subsection (12) allows the security and intelligence agency 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.

484 Where a Judicial Commissioner refuses to approve a decision by the Secretary of State to give such a direction, he or she must give written reasons for this (subsection (8)); 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 (9)).

Clause 193: Part 7: interpretation

485 This clause defines specific terms used in this Part.

Part 8: Oversight arrangements

Chapter 1: Investigatory Powers Commissioner and other Judicial Commissioners

Clause 194: Investigatory Powers Commissioner and other Judicial Commissioners

486 This clause establishes the office of the Investigatory Powers Commissioner, who will be supported in fulfilling their functions by other Judicial Commissioners. No-one will be appointed as the Investigatory Powers Commissioner or as a Judicial Commissioner unless they have held a judicial position at least as senior as a high court judge. Appointments to these positions will be made by the Prime Minister after consultation with the Lord Chief Justice of England and Wales, the Lord President of Scotland, the Lord Chief Justice of Northern Ireland, the Scottish Ministers, and the First Minister and deputy First Minister in Northern Ireland. A memorandum of understanding will also be established to detail how Scottish Ministers will be consulted on the appointment.

487 To allow them to work effectively, the Investigatory Powers Commissioner will be able to delegate functions to the other Judicial Commissioners. The Investigatory Powers Commissioner is a Judicial Commissioner, so where the Bill or these Explanatory Notes refers to a Judicial Commissioner this includes the Investigatory Powers Commissioner.

Clause 195: Terms and conditions of appointment

488 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.

Clause 196: Main oversight functions

489 This clause gives the Investigatory Powers Commissioner a broad remit to keep under review the use of investigatory powers. This clause does not contain an exhaustive list of all the functions that we expect the Commissioner to undertake. 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. The clause then lists additional matters not caught by that starting point, such as the acquisition, retention and use of bulk personal data sets. The Investigatory Powers Commissioner will undertake, with the assistance of their office, the functions currently undertaken by the Intelligence Services Commissioner, the Interception of Communications Commissioner and the Surveillance Commissioners. The Investigatory Powers Commissioner and other Judicial Commissioners will have discretion as to how they must fulfill their functions, but this must include audits, inspections and investigations.

490 Subsection (4) explains that, to prevent inefficiency and duplication of oversight, the Investigatory Powers Commissioner will not oversee particular areas that are already subject to oversight by other individuals or bodies. The Investigatory Powers Commissioner will not oversee decisions by other judicial authorities or where information is obtained through a search warrant or production order issued by a judicial authority. The Investigatory Powers Commissioner will not oversee matters which are overseen by the Information Commissioner.

491 Subsection (5) and (6) seek to ensure that the oversight activities do not have a negative effect upon the ability of law enforcement agencies and security and intelligence agencies to perform their statutory functions. The Judicial Commissioners will have to decide for themselves if their proposed activity will prejudice national security or impede the effectiveness of operations. These subsections do not apply to the authorisation functions of the Commissioners – such as deciding whether to approve the issuing, renewing or modification of a warrant.

Clause 197: Additional directed oversight functions

492 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 Investigatory Powers Commissioner to oversee new areas. This is to ensure that independent oversight keeps pace with developments within the security and intelligence agencies.

493 Subsection (5) sets out that the Prime Minister must publish any direction that he makes to the Investigatory Powers Commissioner to ensure that there is full transparency about their role. However, this will need to be balanced against a situation where saying too much about what is being overseen will give away details of the policy or capability to the extent that it damages national security.

Clause 198: Error reporting

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

495 When the Investigatory Powers Commissioner becomes aware of an error, the Commissioner must decide whether the error is serious. An error can only be considered serious if it has caused significant prejudice to the person concerned. The Investigatory Powers Commissioner must then decide whether it is in the public interest for the person concerned to be informed. In reaching this decision 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.

496 If the Investigatory Powers Commissioner decides that the person should be informed, that person must also be informed of their right to bring a claim in the IPT. The person must also

be provided with the details necessary to bring such a claim, to the extent that disclosing information is in the public interest.

497 The Investigatory Powers Commissioner's annual report (see clause 201) 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.

Clause 199: Additional functions under this Part

498 This clause sets out that a Judicial Commissioners must give the IPT any documents, information and assistance the IPT may ask for, including Commissioner's opinion on anything the IPT has to decide. This allows the IPT to take advantage of the Investigatory Powers Commissioner's expertise and the expertise of his office when reaching a decision.

499 Subsection (2) allows the Investigatory Powers Commissioner to provide advice and information to both public authorities and the general public. If the Commissioner thinks that providing such information or advice might be contrary to the public interest or be damaging to one of the things listed, including national security, the Commissioner must consult with the Secretary of State first. The Commissioner does not have to consult the Secretary of State before providing information to the IPT.

Clause 200: Functions under other Parts and other enactments

500 This clause means that functions of the existing commissioners, and in particular the role of the Surveillance Commissioners, in authorising certain conduct will instead be carried out by the Investigatory Powers Commissioner.

Clause 201: Annual and other reports

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

502 Subsections (3) and (4) state that upon receipt of an annual report from the Investigatory Powers Commissioner the Prime Minister must publish that report and lay it before Parliament. However, the Prime Minister may redact information from the report if that information would damage national security or damage operational effectiveness. The Prime Minister must consult with the Investigatory Powers Commissioner before deciding to redact anything from the report. 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 and the First Minister and deputy First Minister to be laid before the Scottish Parliament and the Northern Irish Assembly.

Clause 202: Investigation and information powers

503 This clause ensures that the Investigatory Powers Commissioner has access to the information necessary to carry out the Commissioner's oversight role effectively. The clause does this by requiring people to provide the Judicial Commissioners with all the information, documents and access to technical systems that the Commissioner may need. They must also provide the Commissioner, or anyone assisting the Commissioner with the performance of their statutory functions, with any assistance they may need. The persons to whom these obligations apply includes public authorities and also telecommunications and postal operators who are subject to obligations under this Act.

Clause 203: Information gateway

These Explanatory Notes relate to the Investigatory Powers Bill as introduced in the House of Commons on 19 May 2016 (Bill 2)

504 This clause allows people to provide information to the Investigatory Powers Commissioner, regardless of any other legal restrictions that might exist. 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 Investigatory Powers Commissioner.

Clause 204: Funding, staff and facilities

505 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.

506 Subsection (2) requires the Secretary of State to provide the Investigatory Powers Commissioner with the staff, accommodation, equipment and facilities that the Secretary of State thinks necessary. It is intended that the resources afforded to the Investigatory Powers Commissioner will ensure that the office is fully staffed with judicial, official, legal and technical support to ensure that the Commissioners are fully able to perform their oversight and authorisation functions and to hold those that use investigatory powers to account. In determining the resources that should be provided the Secretary of State will consult with the Investigatory Powers Commissioner. Treasury approval will be required as to the number of staff. Should the Investigatory Powers Commissioner believe that the resources afforded to them are insufficient then they may publicly report the fact in their Annual Report or raise the matter with the Intelligence and Security Committee of Parliament.

Clause 205: Power to modify functions

507 This clause allows the functions of the Investigatory Powers Commissioner to be changed. This would require the approval of both Houses of Parliament. The ability to change the function allows a level of flexibility about the role of the Commissioner to ensure that it can be modified and adapted to fit with the work that needs to be overseen. However, this power cannot be used to change or remove the Judicial Commissioners' authorisation functions.

Clause 206: Abolition of existing oversight bodies

508 The Investigatory Powers Commissioner will replace the existing commissioners who provide oversight of investigatory powers: the Interception of Communications Commissioner, the Surveillance Commissioners (including Assistant Surveillance Commissioners), the Intelligence Services Commissioner and the Investigatory Powers Commissioner for Northern Ireland. The abolition of the Chief Surveillance Commissioner and Assistant Surveillance Commissioners includes those appointed by Scottish Ministers for the purposes of the Regulation of Investigatory Powers (Scotland) Act 2000. Accordingly, this clause abolishes those offices.

Chapter 2: Other arrangements

Clause 207: Codes of practice

509 This clause provides for the Secretary of State to issue codes of practice covering the use of powers covered by the Bill, as outlined in Schedule 7.

Schedule 7: Codes of practice

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

511 Paragraph 2 specifies that each code of practice must include provisions designed to protect

the confidentiality of journalistic sources. It should also outline particular considerations which should be applied to data relating to a member of a profession which would regularly hold legally privileged or relevant confidential information, such as medical professionals, those in the legal profession or MPs. Both legally privileged information and confidential information are defined in sub-paragraph 2.

512 Paragraph 3 requires a code of practice to cover communications data held by public authorities acquired under the powers provided by Part 3. Subsection 2 specifies that the code of practice must explain the criteria listed in (a) to (f) covering why the data is held, access to the data, disclosure of the data, interrogation of the data and destruction of the data.

513 Paragraph 4 specifies that the Secretary of State must consult on any draft code of practice but may modify a code on the basis of representations made after its publication. The Secretary of State must specifically consult the Investigatory Powers Commissioner on the draft code and additionally the Information Commissioner on a Part 4 code of practice. A code will come into force in accordance with regulations made by the Secretary of State, which must be made by statutory instrument and laid in draft before Parliament and approved by each House. The draft code should be laid alongside the draft instrument. No statutory instrument can be laid until the consultation has taken place.

514 Paragraph 5 allows the Secretary of State to make revisions to a code of practice. The Secretary of State is required to publish and consult on the revised code. In particular the Investigatory Powers Commissioner must be consulted, as must the Information Commissioner for a code of practice regarding the retention of communications data. A revised code comes into force in accordance with regulations made by the Secretary of State, which must be made by statutory instrument and laid before Parliament. The revised code should be laid alongside the draft instrument. No statutory instrument can be laid until the consultation on the revised code has taken place.

515 Paragraph 6 requires a person exercising any function to which a code relates to have due regard for the code. Sub-paragraph (2) clarifies that failure to comply with the code does not make a person liable to criminal or civil proceedings. Subparagraphs (3) and (4) specify however, that the code can be admissible in evidence in any such legal proceedings and a court or tribunal may take a person's failure to comply with the code into account in determining a question in such proceedings.

Clause 208: Right of appeal from the Tribunal

516 Currently there is no domestic route of appeal from a decision or determination of the Investigatory Powers Tribunal, with Claimant's having to pursue appeals to the European Court of Human Rights if they wish to challenge a decision. This clause 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, the Court of Session or the Court of Appeal in Northern Ireland. Regulations will detail the criteria to be considered by the Investigatory Powers Tribunal when determining the relevant appellate court.

517 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.

518 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.

519 The clause also amends RIPA to clarify 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, except where they are prevented from doing so by the procedure rules governing the IPT, for example where the decision relates to closed proceedings.

Clause 209: Functions of Tribunal in relation to this Act

520 This clause extends the functions of the Investigatory Powers Tribunal in relation to retention notices under Part 4.

Clause 210: Oversight by Information Commissioner in relation to Part 4

521 The Information Commissioner must audit requirements related to the retention of communications data, for example, to ensure the data is retained securely. This is distinct from the Investigatory Powers Commissioner's requirements in respect of the acquisition of communications data.

Clause 211: Technical Advisory Board

522 This clause provides for the continued existence by order of a Technical Advisory Board. Its make-up will be prescribed by 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 clause may also set out how many members must be present for the Board to carry out its functions.

Part 9: Miscellaneous and general provisions

Chapter 1: Miscellaneous

Clause 212: Combination of warrants and authorisations

523 This clause explains that Schedule 8 allows for the combination of targeted interception and equipment interference warrants with other warrants or authorisations. This builds on the existing ability to combine certain warrants and authorisations (RIPA allows authorisations that combine property interference (under the Intelligence Services Act 1994) and Intrusive Surveillance).

Schedule 8: Combination of warrants

524 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.

525 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.

526 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 Bill with a targeted examination warrant issued under Part 5 of the Bill.

527 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 equipment interference warrant and an authorisation for intrusive surveillance. The National Crime Agency would apply to the Secretary of State (or Scottish Ministers) who may issue the combined warrant, even though the Secretary of State 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 an authorisation.

528 Paragraphs 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.

529 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.

530 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 the Intelligence Services Act 1994. Judicial Commissioner approval is not required for the part containing the section 5 warrant.

531 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.

532 Paragraphs 25 and 26 are similar to paragraph 24, except they provide that certain rules in RIPA and RIPSAs do not apply to authorisations for intrusive or directed surveillance when

they are part of a combined warrant.

- 533 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.
- 534 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.
- 535 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 would apply to warrants under Part 2 or Part 5 of the Bill 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.
- 536 Clause 48 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 clause 48 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 means that one of the exceptions to the rules against disclosure -the ability to obtain legal advice – applies to advice about this Schedule.

Clause 213: Payments towards certain compliance costs

- 537 This clause requires the Secretary of State to ensure that there are arrangements to secure that communications service providers receive a fair contribution towards their costs of complying with the provisions in the Act. Subsection (6) makes clear that the appropriate contribution must never be nil. Subsection (7) requires that a retention notice under Part 4 or national security notice under clause 216 must specify the level of contribution to be made.

Clause 214: Power to develop compliance systems etc.

- 538 This clause enables the Secretary of State to develop, provide, maintain or improve equipment that can be used by the Secretary of State, another public authority or any other person to facilitate compliance with the provisions in the Act. The clauses also enable the Secretary of State to enter into financial arrangements with any other person to develop, provide, maintain or improve any such system.

Clause 215: Amendments of the Intelligence Services Act 1994

- 539 Clause 215 amends the Intelligence Services Act 1994 (ISA).
- 540 Subsection (2)(a) amends subsection (1)(a) of section 3 of ISA to provide that GCHQ can “make use of” as well as “monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material”. This clarifies that GCHQ may, in the performance of its functions, make use of communications services in the manner in which it was intended they would be used. This could be used for public

communications as well as for investigative purposes.

541 Subsection (2)(b) amends subsection (1)(b)(ii) of section 3 of ISA to allow GCHQ to provide advice and assistance on the protection of information to other 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 which affect not just the Government but also business and the public in general e.g. cyber security.

542 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 to support 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.

Clause 216: National security notices

543 This clause 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.

544 Subsections (1) and (2) specify that a national security notice may only be given by the Secretary of State where the conduct required by the notice is necessary and proportionate.

545 Subsection (3) outlines the types of support that the telecommunications operator may be required to provide to satisfy the requirement, for example to provide services or facilities which would assist the intelligence agencies in safeguarding the security of their personnel and operations.

546 Subsection (4) stipulates that the notice cannot be used where the primary purpose is to authorise interference with privacy where a warrant or authorisation is required under this Act. In any circumstance where a notice would involve the acquisition of communications or data, a warrant or authorisation under the relevant part of this Act would always be required in parallel. Subsection (5) states that the time required to comply with the notice must be reasonable.

Clause 217: Maintenance of technical capability

547 This clause allows the Secretary of State to impose obligations upon telecommunications operators.

548 Subsection (1) provides that the Secretary of State may impose obligations upon a postal operator, a telecommunications operator or a person proposing to become a postal operator or a telecommunications operator by giving a technical capability notice.

549 Subsection (3) 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 where the Secretary of State believes the obligations are reasonable, and with the aim of ensuring that providers are capable of providing technical assistance in relation to any warrant under Part 2, 5 or 6, or any authorisation given under Part 3.

550 Subsection (4) sets out the types of obligations that may be imposed, for example (a) providing communications facilities and capacity to support the implementation of warrants or (d) ensuring the security of facilities or staff who may be required to handle classified material.

551 Subsection (5) requires the Secretary of State to consult a number of people prior to making the regulations provided for at subsection (3). These include the Technical Advisory Board, the persons likely to have obligations imposed on them and their representatives, and persons with statutory functions affecting providers of communication services.

552 Subsection (6) makes clear that the only steps that may be set out in the notice are those which the Secretary of State considers are necessary to ensure that the operator to whom the notice is to be given can provide assistance in relation to any warrant under Part 2, 5 or 6, or any authorisation given under Part 3.

553 Consideration of the time required to comply with the notice is covered in subsection (7). 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.

Clause 218: Further provision about notices under section 216 or 217

554 This clause provides further details about notices given under the previous two sections. Subsection (2) ensures that the Secretary of State must consult the operator before giving either a national security notice or technical capability notice. Subsection (3) sets out the considerations the Secretary of State must take into account before giving 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 in a technical capability notice that relate to the removal of electronic protections.

555 Subsection (6) set out the mechanisms by which a notice may be given to a person outside the United Kingdom. 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.

556 Subsection (9) requires persons served with a notice under clauses 216 or 217 to comply with it.

557 Subsection (10) outlines that the Secretary of State may bring civil proceedings to enforce both a national security and technical capability notice on persons within the UK. For persons outside of the UK, the Secretary of State may only bring civil proceedings to enforce a technical capability notice which relates to interception warrants or an authorisation or notice given under Part 3.

Clause 219: Variation and revocation of notices

558 This clause requires the Secretary of State to keep notices under review and allows the Secretary of State to vary or revoke a technical capability notice or national security notice. Subsection (4) requires the Secretary of State to consider that any variation of a national security notice is proportionate to what is sought to be achieved by the conduct. Subsections (6) and (7) makes clear that subsections (2) to (7) of clause 218 apply in relation to varying or revoking a notice. Subsection (6) ensures that in the application of clause 218(3) and (4) in relation to varying a notice, references to the notice are to be read as references to the notice as varied.

Clause 220: Review by the Secretary of State

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

560 Subsection (3) states that the person is not required to comply with the specific obligations under referral until the notice has been reviewed by the Secretary of State. The actions that the Secretary of State must take in reviewing the notice, and the role of the Technical Advisory Board and the Investigatory Powers Commissioner in the review process, are outlined at subsections (5 to 8).

561 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. After consideration of the conclusions of the Commissioner and Board, the Secretary of State may decide to confirm the effect of the notice, vary the notice or withdraw it.

Clause 221: Amendments of the Wireless Telegraphy Act 2006

562 This clause 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 Bill provides for such interception.

Chapter 2: General

Clause 222: Review of operation of Act

563 This clause 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 Joint Committee of both Houses of Parliament.

Clause 223: Telecommunications definitions

564 This clause provides relevant definitions in relation to telecommunication systems, services and operators. These new categories are intended to be technology neutral and replace the three categories of communications data in RIPA: traffic data, service use data and subscriber data, which no longer adequately reflect the data available from telecommunication operators or systems.

565 Subsection (2) defines a telecommunication. It includes communications between persons, between a person and a machine and between machines.

566 Subsection (3) defines entity data as data about entities or links between them but does not include information about individual events. Entities could be individuals, groups and objects.

567 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.

568 Subsection (5) defines the subset of entity data and events data which constitute communications data. The authorisation levels provided for in Schedule 4 reflect the fact that the set of events data as a whole contains the more intrusive communications data.

Example 1: Entity Data:

Phone numbers or other identifiers linked to communications devices; address provided to a communications service provider; IP address allocated to an individual by an internet access provider.

Example 2: Events Data:

The fact that someone has sent or received an email, phone call, text or social media message; the location of a person when they made a mobile phone call or the Wi-Fi hotspot that their phone connected to; the destination IP address that an individual has connected to online.

569 Subsection (6) provides a definition of content based around the meaning of the communication excluding any meaning that can be inferred from the fact of the

communication. While it is possible to draw an inference from the fact a person has contacted another person this is distinct from the content of the call.

570 Subsection (6)(b) makes clear that anything which meets the definitions of systems data within clause 225 is not content.

571 Subsections (8 to 14) define communication service providers and systems for the purpose of the bill.

Clause 224: Postal definitions

572 This provision defines the scope of communications data in the postal context. Subsection (3)(a), (b) and (c) are traffic data, service use data and subscriber data respectively. Subsection (4) makes clear that anything on the outside of a postal item which relates to its transmission or identifies the sender or recipient is communications data.

573 Subsection (5) defines a postal item. This does not include containers or any other form of freight. The provisions of the Bill do not apply to freight.

574 Subsections (6 to 8) define communication service providers and systems for the purpose of the Bill.

Clause 225: General definitions

575 This provision is self-explanatory.

Clause 226: Index of defined expressions

576 This provision is self-explanatory

Clause 227: Offences by bodies corporate etc.

577 This provision applies if a body corporate or Scottish partnership, or a senior officer within a body corporate or Scottish partnership commits an offence under this Act.

Clause 228: Regulations

578 This clause outlines the procedure under which the Secretary of State may make regulations. It sets out that parliamentary procedures applicable to the regulations under the Bill and provides that regulations subject to certain procedures may be combined.

Clause 229: Enhanced affirmative procedure

579 This clause outlines the 'enhanced affirmative procedure'. This is a procedure for making secondary legislation that allows for further scrutiny than the affirmative procedure, outlined in the preceding clause. It applies to clause 62, which deals with modifying Schedule 4. In particular this means that there will be an enhanced scrutiny process should the Government wish to provide for additional authorities to be able to acquire communications data. The enhanced scrutiny process includes a statutory duty to consult and for a relevant parliamentary committee to comment on the draft legislation. The Secretary of State must have regard to these representations.

Clause 230: Financial provisions

580 This provision is self-explanatory.

Clause 231: Transitional, transitory or saving provision

581 This clause states that Schedule 9 applies and gives power for the Secretary of State to make any transitional, transitory or saving provisions as he or she considers appropriate in connection with the coming into force of the provisions in the Bill. This standard power enables the changes made the Bill to be implemented in an orderly manner.

These Explanatory Notes relate to the Investigatory Powers Bill as introduced in the House of Commons on 19 May 2016 (Bill 2)

Schedule 9: Transitional, transitory and saving provision

582 Schedule 9 explains transitional, transitory and saving provisions for the Bill. Paragraph 1 provides for agreements in force under section 1(4) of RIPA to be considered as international mutual assistance agreements on the day the Act comes in to force, by the virtue of the regulations under section 8 of this Bill.

583 Paragraph 3 sets out transitional arrangements for communications data being retained under DRIPA 2014. Retention notices under that legislation remain in force until six months after commencement of Part 4 of the Bill.

Clause 232: Minor and consequential provision

584 This clause introduces Schedule 10 and provides that the Secretary of State may make any provision by regulations as is considered necessary as a consequence of the provisions of the Bill.

Schedule 10: Minor and consequential provision

585 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.

586 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 Bill. The Schedule also updates certain definitions, including some in RIPA, to refer to the definitions in the Bill. 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 Bill.

587 The Schedule also provides that provisions in other legislation that refer to matters in RIPA will now apply to equivalent matters in the Bill. For example, section 6(4) of the Justice and Security Act 2013 provides for courts seised with 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 48 of the Schedule replaces the reference to section 17 of RIPA with the equivalent provision of the Bill (clause 48). This means that the provision of the Justice and Security Act 2013 will continue to have the same effect, despite this Bill replacing parts of RIPA.

588 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 Bill. Such amendments are made by Paragraphs 7 and 8, 11 to 13, 15 to 27, 29 to 33 and 46 of this Schedule.

589 Paragraphs 2 and 38 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 38 maintain the current position, so that anything currently excepted or reserved will continue to be excepted or reserved. A similar amendment is made to the Scotland Act 1998 by paragraph 37.

590 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 63 of this Schedule means that consent will be required before an NCA officer interferes with equipment that is known to be in Northern Ireland.

591 Part 5 of the Schedule makes a number of amendments in consequence of the existing Commissioners being replaced by the Investigatory Powers Commissioner and the Judicial Commissioners. This is in addition to the amendments made by clause 200 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 29. This is amended so that it will be necessary to consult the Investigatory Powers Commissioner instead. In some places, rules regarding the existing Commissioners have been omitted because they replicate matters dealt with in the Bill. 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 Judicial Commissioners (clause 202 of this Bill) will apply.

Clause 233: Commencement, extent and short title

592 This clause is self-explanatory.

Commencement

593 Clauses 222 to 230, 231(2), 232(2) and (3) and 233 of the Bill will commence on Royal Assent. The main provisions of the Bill will be brought into force by means of regulations made by the Secretary of State.

Financial implications of the Bill

594 The provisions enabled by the Bill is estimated to lead to an increase in public expenditure of £247 million over 10 years from 2015/16. These costs are based on:

- a. costs to Government Departments associated with the establishment of the Investigatory Powers Commission and authorisation of warrantry;
- b. costs associated with the ongoing running costs, compliance and reimbursement to business of costs associated with new communications data provisions;
- c. costs associated with increased compliance, reporting and safeguards to the agencies, law enforcement and other public authorities;
- d. costs to the justice system for offences and changes to the Investigatory Powers Tribunal.

Compatibility with the European Convention on Human Rights

595 The Home Secretary, the Rt Hon Theresa May MP, has made the following statement under section 19(1)(a) of the Human Rights Act 1998:

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

596 The Government has published a separate ECHR memorandum which explains its assessment of the compatibility of the Bill's provisions with the Convention rights; the memorandum is available on the Home Office website.

Related documents

597 The following documents are relevant to the Bill and can be read at the stated locations:

- European Court Judgement: 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>
- Draft Investigatory Powers Bill Cm 9152:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf
- Joint Committee report on the draft Investigatory Powers Bill:
<http://www.publications.parliament.uk/pa/jt201516/jtselect/jtinvpowers/93/93.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>
- 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#](http://isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt(web).pdf#)
- Intelligence and Security Committee Report on the draft Investigatory Powers Bill
[http://isc.independent.gov.uk/files/20160209_ISC_Rpt_IPBill\(web\).pdf](http://isc.independent.gov.uk/files/20160209_ISC_Rpt_IPBill(web).pdf)
- House of Commons Science and Technology Committee – Investigatory Powers Bill: technology issues

These Explanatory Notes relate to the Investigatory Powers Bill as introduced in the House of Commons on 19 May 2016 (Bill 2)

<http://www.publications.parliament.uk/pa/cm201516/cmselect/cmsctech/573/573.pdf>

- 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

Annex A - Territorial extent and application in the United Kingdom

The Bill extends to the whole of the United Kingdom. This is subject to the exception that amendments, repeals and revocations have the same extent as the enactment to which they relate. There are no clauses or Schedules in the Bill that apply only to England or only to England and Wales, as set out in the table below. It is therefore not necessary to consider, for the purposes of Standing Order No. 83J of the Standing Orders of the House of Commons relating to Public Business, whether any provisions have minor or consequential effects outside England and Wales, or whether any provisions would be within the competence of any of the devolved legislatures.¹

| Provision | Extends to E & W and applies to England? | Extends to E & W and applies to Wales? | Extends and applies to Scotland? | Extends and applies to Northern Ireland? | Would corresponding provision be within the competence of the National Assembly for Wales? | Would corresponding provision be within the competence of the Scottish Parliament? | Would corresponding provision be within the competence of the Northern Ireland Assembly? | Legislative Consent Motion needed? |
|---|--|--|----------------------------------|--|--|--|--|------------------------------------|
| Part 1: General privacy Protections | | | | | | | | |
| Clauses 1 to 11 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | No |
| Schedule 1 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | No |
| Schedule 2 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | No |
| Clause 12 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | S |
| Part 2: Lawful interception of communications | | | | | | | | |
| Clauses 13 to 18 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | No |
| Schedule 3 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | No |
| Clauses 19 to 20 | No | No | Yes | No | N/A | N/A | N/A | S |
| Clauses 21 to 41 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | No |
| Clauses 42 and 43 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | S |

¹ References in this Annex to a provision being within the legislative competence of the Scottish Parliament, the National Assembly for Wales or the Northern Ireland Assembly are to the provision being within the legislative competence of the relevant devolved legislature for the purposes of Standing Order No. 83J of the Standing Orders of the House of Commons relating to Public Business.

| Provision | Extends to E & W and applies to England? | Extends to E & W and applies to Wales? | Extends and applies to Scotland? | Extends and applies to Northern Ireland? | Would corresponding provision be within the competence of the National Assembly for Wales? | Would corresponding provision be within the competence of the Scottish Parliament? | Would corresponding provision be within the competence of the Northern Ireland Assembly? | Legislative Consent Motion needed? |
|--|--|--|----------------------------------|--|--|--|--|------------------------------------|
| Clauses 44 and 52 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | No |
| Part 3: Authorisations for obtaining communications data | | | | | | | | |
| Clause 53 to 77 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | No |
| Schedule 4 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | No |
| Schedule 5 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | No |
| Part 4: Retention of communications data | | | | | | | | |
| Clauses 78 to 87 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | No |
| Part 5: Equipment Interference | | | | | | | | |
| Clauses 88 to 118 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | S (in part) |
| Schedule 6 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | S (in part) |
| Part 6: Bulk Warrants | | | | | | | | |
| Clauses 119 to 172 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | No |
| Part 7: Bulk personal data warrants | | | | | | | | |
| Clauses 173 to 189 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | No |
| Part 8: Oversight arrangements | | | | | | | | |
| Clauses 190 to 207 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | S (in part) NI (in part) |
| Schedule 7 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | No |
| Part 9: Miscellaneous and general provisions | | | | | | | | |
| Clauses 208 to 228 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | S (in part) NI (in part) |
| Schedule 8 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | S (in part) |
| Schedule 9 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | No |
| Schedule 10 | Yes | Yes | Yes | Yes | N/A | N/A | N/A | No |

These Explanatory Notes relate to the Investigatory Powers Bill as introduced in the House of Commons on 19 May 2016 (Bill 2)

INVESTIGATORY POWERS BILL

EXPLANATORY NOTES

These Explanatory Notes relate to the Investigatory Powers Bill as introduced in the House of Commons on 19 May 2016 (Bill 2).

Ordered by the House of Commons to be printed, 19 May 2016.

© Parliamentary copyright 2016

This publication may be reproduced under the terms of the Open Parliament Licence which is published at www.parliament.uk/site-information/copyright

PUBLISHED BY AUTHORITY OF THE HOUSE OF COMMONS

LONDON - THE STATIONERY OFFICE LIMITED

Printed In the United Kingdom by The Stationery Office Limited

£ FOR TSO USE