Investigatory Powers Bill

European Convention on Human Rights Memorandum

1. This memorandum addresses issues arising under the European Convention on Human Rights ("ECHR") in relation to the Investigatory Powers Bill. The Department is satisfied that, in the event that the Bill is introduced into Parliament, the responsible Minister could make a statement under section 19(1)(a) of the Human Rights Act 1998 that, in the Minister's view, the provisions of the Bill are compatible with the Convention rights.

Summary of the Bill

2. The Bill will provide a clear framework for the use of investigatory powers by law enforcement and security and intelligence agencies, and other public authorities. This includes the interception of communications, the retention and acquisition of communications data, the use of equipment interference, and the acquisition of bulk data for target discovery purposes.

3. Section 7 of the Data Retention and Investigatory Powers Act 2014 (DRIPA) required David Anderson QC, the Independent Reviewer of Terrorism Legislation, to conduct a review of existing laws relating to investigatory powers. The Bill responds to and accepts the majority of the recommendations made in his report ('the Anderson Report').[1] Further reports were published by the Intelligence and Security Committee and the Royal United Services Institute.[2]

Targeted interception of communications

4. The Bill will repeal and replace Part 1, Chapter 1 of the Regulation of Investigatory Powers Act 2000 (RIPA). It will provide for the targeted interception of communications by the existing intercepting agencies. Interception under the Wireless Telegraphy Act 2006 will be brought within the new law.

Communications data

5. The existing statutory regime by which public telecommunications operators can be required to retain communications data will be broadly replicated. This will

[1] A Question of Trust: Report of the Investigatory Powers Review, David Anderson QC, June 2015.
[2] 'Privacy and Security: A modern and transparent legal framework', the Intelligence and Security Committee of Parliament, 12 March 2015; A Democratic License to Operate: Report of the Independent Surveillance Review, The Royal Services Institute, July 2015.

replace DRIPA, which is subject to a 31 December 2016 sunset clause, and Part 11 of the Anti-Terrorism Crime and Security Act 2001.

6. The Bill will provide for powers by public authorities to acquire communications data, replacing and largely replicating the effect of Chapter 2 of Part 1 of RIPA. This will include the power to require the retention of Internet connection records (ICRs), which are a form of communications data.

Equipment interference

7. The existing statutory regime allows the law enforcement and security and intelligence agencies to interfere with property, to put the use of equipment interference on a clearer legal footing and to make its use more transparent and foreseeable (so that the public will understand what powers are available and the circumstances in which they can be used). The Bill will provide for the authorisation of the use of equipment interference to obtain communications, and private information and equipment data.

Bulk interception, equipment interference and communications data

8. Part 6 of the Bill contains powers for the security and intelligence agencies to intercept communications, conduct equipment interference and to obtain communications data in bulk.

9. A key characteristic of these bulk activities is that they will involve some interferences with the privacy rights of individuals who are not of intelligence interest, in order to obtain the communications of those who are. They will be subject to an authorisation process involving Secretary of State issue of a warrant, approved by a Judicial Commissioner.

Bulk personal data

10. The security and intelligence agencies have existing statutory powers which enable them to acquire and exploit large datasets containing personal data. The Bill will not create a new power but make clearer that these powers can be used to obtain data in bulk and create an additional safeguard: the acquisition and exploitation of bulk personal data by the security and intelligence agencies will be subject to an authorisation process involving Secretary of State issue of a warrant, approved by a Judicial Commissioner.

Safeguards and oversight

11. The Bill will provide for an authorisation process. Warrants will be issued by the Secretary of State but will not come into force until approved by a Judicial Commissioner. This process will apply to warrants authorising:

    a. targeted interception;

b. targeted equipment interference;

c. bulk interception, equipment interference and the bulk acquisition of communications data;

d. acquisition and access/exploitation of bulk personal data by the security and intelligence agencies.

12. The Interception of Communications Commissioner's Office, the Office of Surveillance Commissioners and the Intelligence Services Commissioner will be replaced by a single oversight body led by a powerful new Investigatory Powers Commissioner. The new oversight body will have oversight of the use of the powers in the Bill, plus public authorities' access to intercept and communications data through existing statutory powers.

13. A domestic route of appeal will be created from the Investigatory Powers Tribunal (IPT), with appeal possible on a point of law only.

Introduction

14. The provisions in the Bill engage Articles 8 and 10, and Article 1 of the First Protocol ('A1P1') of the ECHR. They are all qualified rights, which means that interference with the rights may be permissible. Any interference must be set down and regulated by a clear and ascertainable legal regime ("in accordance with the law", "prescribed by law", or "subject to the conditions provided for by law"). Furthermore, Articles 8 and 10 require that any interference is necessary in a democratic society and is a proportionate means of achieving a legitimate aim, while A1P1 requires that any deprivation of possessions must be "in the public interest".

15. It is axiomatic that for an interference with an ECHR right to be in accordance with the law there must be a lawful domestic basis for it, this law must be adequately accessible to the public, and its operation must be sufficiently foreseeable, so that people who are subject to it can regulate their conduct.

16. Given the inevitable tension between the requirements of foreseeability and the covert use of investigatory powers it is worth considering at this juncture what the requirement that the law is foreseeable means in this context. In *S and Marper v United Kingdom*, the ECtHR found that the level of precision required depends heavily on the context and cannot in any case cover every eventuality. The law does not need to set out each and every way that the powers in the Bill may be used.[3]

[3] *S and Marper* v. *United Kingdom,* 4 December 2008, (2009) 48 EHRR 50

17. The requirement that the law be foreseeable does not mean that a target of covert techniques should be able to foresee when powers are likely to be deployed against them, so that they may adapt their conduct accordingly.[4]

18. In *S and Marper*, the ECtHR set out that:

> "*... it is essential ... [in the context of] secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning,* inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction*…".

In order to address the foreseeability and compatibility with the rule of law requirements of Article 8, as many as possible of those minimum safeguards should be set out expressly in legislation, codes of practice or published guidance.

19. The requirement of legality goes further than the law being adequately prescribed, accessible and foreseeable. The law must contain sufficient safeguards to avoid the risk that power will be arbitrarily exercised and thus that unjustified interference with a fundamental right will occur.

General Safeguards

20. The Bill establishes (or enhances) a number of safeguards against the arbitrary or unlawful use of investigatory powers by the executive. To avoid repetition, as these safeguards are relevant to a number of the potential interferences with convention rights, we will describe some of these safeguards at this point.

Judicial approval of warrants

21. The primary safeguard established by the Bill is an authorisation process which includes prior approval of warrants by independent judges called Judicial Commissioners.

22. It will only be possible for warrants to be issued where the decision maker is satisfied that the warrant is necessary and proportionate and where that decision to issue the warrant has been approved by a Judicial Commissioner. The Judicial Commissioner will decide whether to approve the decision to issue a warrant, applying the same principles that would apply in a judicial review. Judicial Commissioners must also approve the renewal of warrants.

[4] *Weber and Saravia v. Germany,* Admissibility Decision, 29 June 2006

23. The Department's view is that this model more than meets the requirements of ECHR case law. It should also be noted that David Anderson QC saw as acceptable a model that retains the executive as the primary authoriser with the judicial or independent authoriser controlling executive decisions by applying judicial review principles.

24. The Bill anticipates situations where the need to issue a warrant is so urgent that it is not possible to seek the approval of a Judicial Commissioner. Such a situation may include where there is an imminent threat to a person's life. In such a situation, an urgent warrant may be issued without a Judicial Commissioner's approval. An urgent warrant must be reviewed within five working days by a Judicial Commissioner and will cease to have effect if it is not approved by the Commissioner. This means that a Judicial Commissioner can effectively cancel an urgent warrant that the judge does not consider to be both necessary and proportionate.

Oversight

25. The Bill will create an Investigatory Powers Commissioner, replacing the existing offices of the Interception of Communications Commissioner, Chief Surveillance Commissioner, and Intelligence Services Commissioner. The Investigatory Powers Commissioner will be supported by other Judicial Commissioners. The Commissioners will be judges who hold or have held high judicial office (i.e. they will be High Court Judges or more senior judges). These Commissioners will be independent of the Executive: they will be appointed by the Prime Minister for a fixed term and a resolution of both Houses of Parliament will be required to remove them from office.

26. The Investigatory Powers Commissioner, supported by the Judicial Commissioners and a technical staff, will scrutinise the use of all of the investigatory powers in the Bill, including through audit and inspection.

27. All members of public authorities, plus anyone on whom an obligation is placed pursuant to the Bill, will be under a duty to provide or disclose to the Investigatory Powers Commissioner all documents and information the Commissioner may require to carry out the Commissioner's functions. Similarly, all members of public authorities will be required to provide the Investigatory Powers Commissioner with such assistance as the Commissioner may reasonably require. This will allow the Commissioner wide ranging access, including to on-going investigations.

28. The Investigatory Powers Commissioner will, in addition to an annual report, be able to report at any time, on anything of which the Commissioner has oversight. Reports will be made to the Prime Minister and, subject to the Prime Minister's power to exclude matters from the report on narrowly defined grounds, published

and laid before Parliament. This means that the Commissioner will be able to highlight any arbitrary or potentially unlawful use of the powers in the Bill.

29. Where the Investigatory Powers Commissioner becomes aware of an error, either through inspections or through self reporting by public authorities, the Commissioner must inform the member of the public concerned if a statutory test is met. That test is that the Commissioner regards the error as serious and the IPT agrees that the error is serious and considers that it is in the public interest for the person to be informed. The IPT will consider, in particular, the seriousness of the error and its impact on the person concerned, but also the extent to which disclosing the error would be contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic wellbeing of the UK or the continued discharge of the functions of any of the intelligence services. If the statutory test is met, the Investigatory Powers Commissioner must inform the member of the public of the error and of any right to bring a claim for compensation.

Investigatory Powers Tribunal

30. The Bill will create a domestic right of appeal from decisions of the IPT to the Court of Appeal (regulations will make provision for claims relating to a devolved matter in Northern Ireland and Scotland), in cases where the IPT has made a determination and found there is a point of law at issue. This will allow IPT decisions to be subject to challenge domestically. Currently the only option available to a complainant wishing to challenge a decision of the IPT is to bring a case before the ECtHR.

31. The existing IPT rules and procedures have been found to be lawful by the European Court of Human Rights.[5] The provision of a domestic right of appeal therefore bolsters a system that is already ECHR compliant.

Targeted Interception of Communications

32. The targeted interception of communications, involving as it does the making available the content of private communications, inevitably engages Article 8. In addition, it is arguable that the possibility of interception has the ability to discourage freedom of expression and public discourse and therefore interfere with Article 10 rights.

[5] Kennedy v United Kingdom [2011] 52 EHRR 4

In accordance with the law

33. The Bill will establish a clear and accessible domestic basis for interception. The regime will be sufficiently foreseeable in that it builds on the safeguards in the existing interception regime which has been scrutinised by the ECtHR and found to be foreseeable.

34. In the context of interception of communications, the ECtHR has ruled that foreseeability cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly (*Leander v Sweden*),[6] but the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to intercept communications. The law must indicate the scope of the competent authorities' discretion and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.

35. The ECtHR has developed a list of 'minimum safeguards' that need to exist within the legal framework governing the interception of communications. In order to ensure that the requirements of foreseeability are met, as many as possible of these minimum should be in place. The minimum safeguards, as set out in *Weber and Saravia*, are:

> "the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed."[7]

36. In *Kennedy v UK*, the ECtHR assessed the law governing the interception of communications between persons in the United Kingdom against the criteria set out in *Weber v Saravia.* The Court found that the regime was foreseeable and that Article 8 was therefore not violated. The Court explained that:

> "the domestic law on interception of internal communications together with the clarifications brought by the publication of the Code indicate with sufficient clarity the procedures for the authorisation and processing of interception warrants as well as the processing, communicating and destruction of intercept material collected."

[6] Leander v Sweden (1987) 9 E.H.R.R. 433
[7] Weber and Saravia v Germany (2008) 46 E.H.R.R. SE5

Necessary

37. A warrant authorising the interception of communications may only be granted by the Secretary of State where he or she considers it necessary in the interests of national security, for the prevention or detection of serious crime, or for the purpose of safeguarding the economic well-being of the United Kingdom (which will be expressly limited to circumstances where there is a link to national security).

38. The ability of law enforcement and the security and intelligence agencies to intercept communications is vital in protecting national security and preventing and detecting serious crime.

Proportionate means of achieving a legitimate aim

39. As set out below, the Bill contains a range of safeguards around the interception of communications, and the processing and communication of intercepted material. This includes the same safeguards for targeted interception as are included in Chapter 1 of Part 1 of RIPA, and substantially builds on those safeguards.

40. A warrant may only be issued by the Secretary of State and only certain departments may apply for an interception warrant. The Secretary of State must consider that the warrant is necessary for one of these purposes and proportionate to what is sought to be achieved. The warrant cannot be issued (subject to the procedure for urgent warrants) unless the decision that the warrant is necessary and proportionate is approved by a Judicial Commissioner.

41. A warrant lasts for 6 months. If at any time the warrant is no longer necessary and proportionate it must be cancelled. The material obtained under an interception warrant must be handled in accordance with arrangements which must, among other things, ensure that the copying and distribution of the material is kept to the minimum necessary and that the material is destroyed when there is no longer any need to keep it. There will be a duty to keep secret the contents of intercepted material and it will be an offence to make an unauthorised disclosure of intercepted material.

42. A Code of Practice will set out additional details regarding the procedures that must be followed before public authorities may intercept communications. It is intended that this Code will set out that particular consideration must be given where the subject of the interception may reasonably assume a high degree of privacy or where confidential information is involved. This will include where confidential journalistic material may be involved. Where the intention is to acquire such material, the application should set out the reasons why, and why it is considered necessary and proportionate to do so. If acquiring such material

is likely but not intended, the Code will require that applications should set out what steps will be taken to mitigate the risk.

43. The draft Bill provides that, in addition to approval by a Judicial Commissioner, the Prime Minister must be consulted before the Secretary of State can decide to issue a warrant to acquire an MP's communications. This will cover all warrants for targeted interception (with the exception of those issued by Scottish Ministers). It will also include a requirement for the Prime Minister to be consulted in the event that a Parliamentarian's communications collected under a bulk interception or equipment interference warrant were to be selected for examination. It will apply to MPs, members of the House of Lords, UK MEPs and members of the Scottish, Welsh and Northern Ireland Parliaments and Assemblies.

44. The Code of Practice will set out additional safeguards regarding privileged material. These will include that:

    a. where an application is likely to lead to privileged material being intercepted, the application will need to set out an assessment of the likelihood and the steps that will be taken to mitigate the risk;

    b. where it is intended that privileged material be intercepted, the warrant will only be granted where the Secretary of State is satisfied that there are exceptional and compelling circumstances that make it necessary;

    c. additional safeguards regarding the handling, retention and disclosure of the privileged material will apply.

45. The use of the power to intercept communications, along with the performance of duties imposed by the Bill, will be subject to scrutiny by the new Investigatory Powers Commissioner.

Communications Data

46. Part 4 of the Bill will enable the Secretary of State to impose requirements and restrictions on telecommunications operators to retain communications data. Part 3 of the Bill will provide for the acquisition of communications data by public authorities. This may include communications data retained under Part 4, other communications data held by providers for their own purposes, or communications data obtained otherwise than from a provider.

47. There is limited ECtHR case law on the application of Article 8 to communications data, but the case of *Malone v UK*[8] provides some guidance, to the effect that while it is to be distinguished from the interception of the content of

[8] *Malone v UK* (1984) 7 EHRR 14 (paragraphs 83 to 88)

communications, Article 8 issues still arise. The exercise of the power to require the retention of communications data, and the acquisition of communications data by public authorities, will engage Article 8.

48. The acquisition of communications data may, exceptionally, lead to the identification of a source of journalistic information. Such acquisition may constitute an interference with Article 10.

In accordance with the law

49. The interferences with Convention Rights will be in accordance with the law because the Bill will create a clear provision in domestic legislation governing the requirement on operators to retain communications data and the circumstances in which the retained communications data may be obtained by relevant public authorities. These provisions are formulated with sufficient precision to enable a person to know in what circumstances and to what extent the powers can be exercised. The test of foreseeability in the context of the retention of communications data is whether the law indicates the scope of any discretion and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference. The provisions of the Bill meet that test.

Necessary

50. The ability of law enforcement and the security and intelligence agencies to obtain communications data is vital in protecting national security, preventing and detecting crime and protecting the public.[9] Communications data is used not only as evidence in court but also to eliminate people from law enforcement investigations. It can be used to prove a person's innocence as well as his or her guilt. It is essential that communications data of this sort continues to be available to be obtained by the law enforcement and intelligence agencies and other relevant public authorities. The CJEU judgment in *Digital Rights Ireland* recognises that data relating to the use of electronic communications 'are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, in particular organised crime' and concluded that their retention genuinely satisfies an objective of general interest.

[9] See e.g., K.U. v Finland [2008] ECHR 2872/02, at para. 49 ("....Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others. …It is nonetheless the task of the legislator to provide the framework for reconciling the various claims which compete for protection in this context."

Proportionate means of achieving a legitimate aim

51. The Department's view is that the provisions regarding the retention of communications data are proportionate. A notice imposing a requirement on a provider to retain data may only be given if the Secretary of State believes that it is necessary and proportionate to do so for one or more of the purposes set out in clause 46(7). The Bill will contain an extensive range of safeguards and restrictions regarding the retention of communications data to ensure that the use of these powers is proportionate.

52. The Bill limits the circumstances in which providers may be required to retain data, and the data they may be required to retain. The notice-giving power in clause 71 enables the Secretary of State to limit the requirement to retain to a description of data held by a provider, so a notice need not require the retention of all data by a particular operator (but may extend to all relevant data if that requirement is necessary and proportionate).

53. The requirement to retain data may be for no more than 12 months. A notice may impose different requirements in respect of different types of data, so, for example, a shorter retention period could be specified in respect of a certain category of data. The requirements of a notice will be tailored according the assessment of the necessity and proportionality of retention. A notice must be kept under review.

54. The Bill also provides for an extensive range of safeguards against the abuse of retained data to ensure that operators are subject to all the obligations necessary to secure respect for the private life of individual telecommunications users. These include: a requirement to secure the integrity of retained data and subject it to the same security and protections as the data on the operator's systems; a requirement to secure, by organisational and technical means, that data can only be accessed by specially authorised personnel; and a requirement to protect the retained data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful retention, processing, access or disclosure. The retained data must be destroyed by the operator if the retention of the data ceases to be authorised (if, for example, a notice is revoked, or at the end of the retention period specified in the notice). Data must be deleted in such a way as to make access to the data impossible.

55. The Information Commissioner must audit compliance by providers with the requirements in respect of the security, integrity and deletion of data retained under a notice.

56. The Department further considers that the provisions regarding the acquisition of communications data are proportionate. Under clause 54 and Schedule 4 access is only permitted by certain public authorities for certain specified purposes.

Different public authorities are able to access different categories of data for different purposes. A notice or authorisation to access communications data must be necessary and proportionate for one of the authorised purposes, taking into account any collateral intrusion.

57. An authorisation may be granted by a designated person of a specified seniority within the public authority, who must be independent of the investigation in the context of which the communications data is sought.

58. The designated senior officer must consult a 'single point of contact' within the organisation, who has expertise in the acquisition of communications data and who can advise on the practicality of obtaining the data sought, and the lawfulness of the proposed authorisation.

59. The Investigatory Powers Commissioner must keep under review the exercise and performance of powers and duties under Part 4. The Commissioner's inspection team will actively examine applications to ensure the decision making (around necessity and proportionality) is appropriately rigorous.

60. The Commissioner will publish a report annually which outlines where mistakes have been made in the application process, as well as including full statistics for all public authorities who have used their powers. If a serious error is made, there will be a process through which the Commissioner must inform the member of the public concerned, as set out above in paragraph 29.

61. If any person believes their data has been acquired inappropriately they can complain to the Investigatory Powers Tribunal, which can investigate the details of the case, and award compensation.

62. The Bill will contain additional safeguards regarding the use of communications data in order to identify a source of journalistic information. Certain public authorities will able to authorise access for that purpose only with the approval of a Judicial Commissioner. Therefore, such a warrant authorising the use of communications data to identify a journalistic source can only have effect if a judge is satisfied that there are reasonable grounds for believing that the warrant is necessary and proportionate.

63. Additional safeguards for communications data relating to members of professions that handle confidential information (including lawyers, doctors, journalists and Members of Parliament) will be set out in a Code of Practice. It will require authorisations regarding such communications data to draw attention to any circumstances that may lead to an unusual degree of intrusion or infringement with rights and must give special consideration to the necessity and proportionality of the request.

64. Additional safeguards are also being put place for local authorities. All requests must be routed through the National-Anti Fraud Network. This will help to ensure that all applications are consistent and of sufficient quality. In addition all requests for communications data made by local authorities must be approved by a magistrate. Local authorities are not permitted to access certain, more intrusive, categories of communications data.

Equipment Interference

65. The Bill will make provision for equipment interference warrants to be issued to law enforcement agencies, security and intelligence agencies and the Ministry of Defence. They will authorise interference with equipment in order to obtain communications, private information and equipment data.

66. The power to interfere with equipment is not new. The security and intelligence agencies can currently be issued with warrants under section 5 of the Intelligence Services Act 1994 authorising property interference. Law enforcement authorise interference with property largely, but not exclusively, under section 93 of the Police Act 1997. While the existing statutory framework for interference with property is adequate, the Bill will provide for a regime that is more transparent and contains more safeguards for the public.

67. Equipment interference necessarily engages Article 8 as it relates to the obtaining of communications and private information. For the same reason as the interception regime, it is arguable that the potential for communications to be obtained via equipment interference could discourage freedom of expression and therefore engage Article 10. The fact that the warrants can authorise interference with private property means that Article 1 of the First Protocol (A1P1) is also engaged.

In accordance with the law

68. The equipment interference powers will meet the test of being "in accordance with the law" because the scheme will be clearly described in primary legislation, ensuring it is accessible and foreseeable. The powers will also be supported by a statutory Code of Practice, further enhancing transparency and foreseeability.

Necessary

69. It will only be possible for an equipment interference warrant to be issued where it is necessary in the interests of national security, for the purpose of detecting and preventing serious crime, or in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to national

security. A Judicial Commissioner will be required to approve the decision that the warrant is necessary.

70. The ability of law enforcement and security and intelligence agencies to conduct operations using equipment interference is a vital part of helping to ensure that they are able to continue to access information and evidence in order to detection and prevent of serious crimes and respond to threats to our national security.

71. The internet and other forms of technology are now used extensively by terrorists and criminals to organise and carry out their crimes, so there is a clear need to have the ability to access suspect's computers and devices for the purposes of intelligence and evidence gathering. If equipment interference warrants are not available, the detection and prevention of serious crime and threats to national security could be undermined, leaving law enforcement and security and intelligence agencies unable to access critical information.

Proportionate means of achieving a legitimate aim

72. It will only be possible to issue an equipment interference warrant where the conduct authorised is proportionate to what is sought to be achieved. A Judicial Commissioner will be required to approve the decision that the warrant is proportionate.

73. An equipment interference warrant will last for six months and any renewal will require further approval from a Judicial Commissioner. If the warrant ceases to be necessary and proportionate it must be cancelled.

74. A number of safeguards have been included in the Bill to ensure that any interference with Convention Rights in kept to the minimum necessary. Public authorities conducting activity under an equipment warrants will be required to ensure that adequate safeguards are in place for information that is acquired. This will include arrangements to ensure the extent to which any material is disclosed or copied is limited to the minimum necessary, that material is stored in a safe manner, and to ensure that material is destroyed as soon as it is not necessary to retain it.

75. The Code of Practice issued under the Bill will contain similar safeguards regarding access to confidential information (such as legal privileged or journalistic material) as the draft equipment Interference Code of Practice. The draft Code makes it clear that special consideration should be given where such information is likely to be acquired. A warrant to obtain legally privileged material should only be issued in "exceptional and compelling circumstances" and requires enhanced handling arrangements to be in place to ensure this sensitive material is handled appropriately. Similar requirements are imposed for the acquisition and retention of other confidential material.

76. The same protection for communications by a Member of Parliament will apply to equipment interference warrants issued by the Secretary of State as for interception. The Secretary of State will only be able to issue an equipment interference warrant relating to the communications of a Member of Parliament with the approval of a Judicial Commissioner and after first consulting the Prime Minister. As above, this will apply to members of the devolved legislatures and UK Members of the European Parliament.

77. All equipment interference activity will be subject to oversight from the Investigatory Powers Commissioner, who will be able to report on errors and problems. Where a serious error is made the Commissioner must, subject to the procedure set out in paragraph 29 above, inform a member of the public effected. That member of the public will be able to seek damages by complaining to the IPT.

Bulk interception, equipment interference and communications data

78. Powers regarding bulk interception, bulk equipment interference and the bulk acquisition of communications data engage Article 8 and Article 10 for the same reasons as the targeted powers. Bulk equipment interference also engages and interferes with A1P1 for the same reason as targeted equipment interference.

In accordance with the law

79. As for the targeted powers, the bulk powers in the Bill will be in accordance with the law because the regime will be clearly set out in primary legislation. This will be supported by statutory Codes of Practice. In combination these will make it clear in what situations the bulk powers may be used and for what purpose.

Necessary

80. The use of bulk powers is necessary for the security and intelligence services to effectively counter threats to national security.

81. It will only be possible for bulk interception warrants, bulk equipment interference warrants and bulk acquisition notices to be issued where the warrant is necessary in the interests of national security. The Secretary of State's decision that the warrant is necessary will be subject to approval by a Judicial Commissioner.

Proportionate means of achieving a legitimate aim

82. It will only be possible for bulk warrants to be issued in the interests of national security. They will only be available to the three intelligence and security services. They will all require warrants to be issued by the Secretary of State. The primary safeguard is that the Secretary of State can only decide to issue a bulk warrant where it is necessary in the interests of national security and the conduct authorised is proportionate, and that decision will require the approval of a Judicial Commissioner.

83. Bulk interception operations typically result in the acquisition of large volumes of untargeted or unselected data. Accordingly, there is a degree of interference with the privacy of a large number of persons, most of whom will not be of intelligence interest. The greater interference comes when information from that volume is selected for examination. Part 6 of the Bill will contain safeguards that apply at the stage that communications are selected for examination, to ensure that material is only selected where it is necessary for specific purposes.

84. For each bulk power, the security and intelligence services will be required to ensure that arrangements are in place to secure that the disclosure and copying of the material is limited to what is necessary, that it is stored securely, and that it is destroyed as soon as it is no longer necessary to retain it.

85. The regime for bulk interception under the Bill will contain the same safeguards as set out in relation to targeted interception. There will be additional safeguards to reflect the special characteristics of bulk interception:

    a. A bulk interception warrant may only be issued where the main purpose relates to communications sent or received by persons overseas.

    b. Each bulk warrant will set out the operational purposes for which the information may be selected for examination. The warrant, which must be approved by a Judicial Commissioner as being necessary and proportionate, will therefore authorise the examination of information obtained for only certain specified purposes.

    c. Material intercepted under the warrant must only be examined for one of the specified purposes and the selection of intercepted material for examination must be necessary and proportionate in all the circumstances.

    d. If the communications of an individual known to be in the British Islands are selected for examination, a targeted examination warrant must additionally be obtained. Accordingly, the communications of a target who is known to be in the United Kingdom may not be examined unless the Secretary of State is satisfied that the examination is necessary for

one of the statutory purposes is and proportionate, and a Judicial Commissioner has approved that decision.

86. The bulk interception regime in the Bill is more transparent and contains stronger safeguards than the provisions in RIPA which provide for bulk interception of communications and the selection for examination of those communications. Those provisions in RIPA have recently been upheld as compatible with Articles 8 and 10 by the IPT in its judgment of 12 December 2014 (in a case brought by Liberty and Privacy International).[10]

87. The power to acquire communications data in bulk will be subject to safeguards and restrictions that are additional to those that apply to the targeted communications data regime. Each bulk acquisition warrant will set out the operational purposes for which information that is obtained may be selected for examination. The warrant, which must be made by the Secretary of State and only when approved by a Judicial Commissioner, will therefore authorise the purposes for which communications data can be selected for examination.

88. The bulk equipment interference regime will contain the safeguards in place for the targeted regime, plus the following additional safeguards.

    a. A bulk equipment interference warrant may only be issued where the main purpose is to facilitate the obtaining of communications sent or received by someone overseas or of private information relating to someone overseas.

    b. A bulk equipment interference warrant must specify the operational purpose for which information obtained may be selected for examination. The security and intelligence agency must ensure that there are arrangements in place to secure that material is only examined as far as it is necessary for one of the operational purposes.

    c. A further additional safeguard will be in place where material is selected for examination by criteria which relates to an individual known to be in the UK or which is to identify communications set or received by a person in the UK, or private information relating to a person in the UK. In such a case, the examination of material will additionally require a targeted examination warrant. This means that the examination of material that relates to a person in the UK will involve an equivalent process to the interception of a person's communications.

89. The safeguards will closely mirror those in place for bulk interception. It is worth noting, therefore, that the existing bulk interception regime (provided for in RIPA)

[10] Liberty & Others vs. the Security Service, SIS, GCHQ. IPT/13/77/H

was recently found by the IPT to be fully in accordance with the requirements of Article 8 of the ECHR.[11]

Bulk Personal Data

90. The security and intelligence agencies have the power to acquire collections of data which contains personal information about a large number of individuals. Bulk personal data can be acquired from a range of sources including Government Departments and Agencies, other intelligence agencies and private sector bodies. Some of this data is publicly available, some of it is purchased and some of it is acquired covertly.

91. In the light of ECtHR case-law, it is clear that the acquisition, access, disclosure and retention of personal information engage Article 8.

In accordance with the law

92. The acquisition and use of bulk personal data is in accordance with the law. The current basis in domestic law is clear and will be made clearer and more transparent by the provisions in the Bill. Section 2(2)(a) of the Security Service Act 1989 and sections 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994 enable the security and intelligence agencies to obtain and use information where this is necessary for the proper discharge of their statutory functions. This includes the acquisition of bulk personal data. In addition, section 19 of the Counter-Terrorism Act 2008 provides that a person may disclose information to the Agencies for the exercise of their functions and that any information disclosed to an Agency for one of its functions may be used for any of its other functions.

Necessary

93. The security and intelligence agencies use bulk personal data, in conjunction with other data, in order to perform their functions, for example, to identify subjects of interest, validate intelligence or to ensure the security of operations or staff.

94. Under the Bill the security and intelligence agencies' acquisition and retention of bulk personal data can be authorised only where it is necessary in the interests of national security, for the purposes of preventing or detecting serious crime, or in the interests of the economic well-being of the United Kingdom so far as those interests are relevant to the interests of national security. The Secretary of State's decision that the warrant is necessary must be approved by a Judicial Commissioner.

[11] Liberty & Others vs. the Security Service, SIS, GCHQ. IPT/13/77/H

Proportionate means of achieving a legitimate aim

95. Under the Bill the security and intelligence agencies' acquisition and use of bulk personal can be authorised only if the Secretary of State decides that the warrant is proportionate and a Judicial Commissioner approves that decision.

96. The use of bulk personal data is proportionate in that it can limit the use of intrusive powers in two ways. Firstly, it can provide the security and intelligence agencies with information that would otherwise be sought through more intrusive means. It may also be used to facilitate the elimination of individuals from an investigation or in pursuit of other intelligence requirements. This ensures that the activities of the agencies are focused on those individuals or organisations that are relevant to the performance of their statutory functions.

The Charter of Fundamental Rights

97. On 8 April 2014, the Court of Justice of the European Union (CJEU) gave judgment in *'Digital Rights Ireland'*, two joined preliminary references on the validity of the Data Retention Directive, which harmonised the retention of communications data.[12] The Court ruled that the Directive was invalid on the grounds that it breached Articles 7 and 8 of the Charter of Fundamental Rights (the right to respect for family and private life, and the right to protection of personal data).

98. The UK's implementation of the Data Retention Directive was replaced by DRIPA. The provisions of DRIPA, in combination with the Regulations made under it, are in substance the same as the provisions of Part 4 of the Bill. The 2014 Act is currently subject to judicial review proceedings, on the grounds that it is incompatible with EU law as set out in the Digital Rights judgment.

99. The Divisional Court found in July this year that section 1 of the Act is incompatible with Articles 7 and 8 of the Charter of Fundamental Rights, to the extent that it does not restrict the purposes for which communications data may be accessed to serious crime, and does not provide for prior independent administrative or judicial authorisation of access to the retained communications data. The Home Secretary has appealed to the Court of Appeal and that appeal was heard in October 2015. The Court of Appeal indicated that it would be making a reference to the CJEU.[13]

100. The Department's view is that the CJEU was only concerned with the legality of the EU legislation, and its findings should not be applied to domestic legislation. The CJEU did not have before it any evidence on the nature of Member States'

[12] C-293/12 Digital Rights Ireland & C-594/12 Seitlinger.
[13] R. (on the application of Davis) v Secretary of State for the Home Department, [2015] EWHC 2092 (Admin)

access regimes. Domestic access regimes are not implementing EU law and so subject to EU law and the Charter does not apply. The requirements of the Charter do not in any event go beyond the requirements of Art 8 ECHR, and the provisions of DRIPA are compatible with ECHR.

Home Office

4 November 2015