Investigatory Powers Bill

European Convention on Human Rights Memorandum

1. This memorandum addresses issues arising under the European Convention on Human Rights ("the Convention") in relation to the Investigatory Powers Bill ("the Bill"). The memorandum has been prepared by the Home Office.

2. The Secretary of State has made a statement under section 19(1)(a) of the Human Rights Act 1998 that, in the Secretary of State's view, the provisions of the Bill are compatible with the Convention rights.

Summary of the Bill

3. The Bill will provide a clear framework for the use of investigatory powers by law enforcement, the 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 retention and use of bulk data by the security and intelligence agencies.

4. 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 of Parliament[2] and a panel convened by the Royal United Services Institute.[3]

5. The Bill was published in draft on 4 November 2016 and subject to pre-legislative scrutiny by the Intelligence and Security Committee of Parliament, the House of Commons Science and Technology Committee and the Joint Committee on the Draft Investigatory Powers Bill (the "Joint Committee"). The Bill has been redrafted in response, with the Home Office accepting, in full or in part, the majority of the recommendations made by the three committees. It was introduced into Parliament on 1 March 2016.

Targeted interception of communications

[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, March 2015.
[3] A Democratic License to Operate: Report of the Independent Surveillance Review - The Royal Services Institute, July 2015.

6. 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 authorities. Interception under the Wireless Telegraphy Act 2006 will be brought within the new law.

Communications data

7. The existing statutory regime by which telecommunications operators can be required to retain communications data will be broadly replicated. This will replace sections 1 and 2 of DRIPA, which is subject to a 31 December 2016 sunset clause, and Part 11 of the Anti-Terrorism Crime and Security Act 2001.

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

Equipment interference

9. The existing statutory regime allows the security and intelligence agencies to authorise interference with property (under sections 5 and 7 of the Intelligence Services Act 1994). Law enforcement agencies conduct this activity using a number of statutory powers, including the authorisation of covert property interference (under section 93 of the Police Act 1997). To put the use of equipment interference on a more open and transparent legal footing (so that the public will better understand what powers are available and the circumstances in which they can be used), the Bill will provide for warrants authorising the use of equipment interference to obtain communications, information and equipment data.

Bulk interception, equipment interference and communications data

10. 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. This will bring together existing powers, which are provided for across a number of statutes including RIPA, the Intelligence Services Act 1994 and the Telecommunications Act 1984, and provide for greater safeguards.

11. A key characteristic of these bulk activities is that they will involve some interference 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 warrants which are then approved by a Judicial Commissioner.

Bulk personal data

12. The security and intelligence agencies have existing statutory powers which enable them to acquire and use large datasets containing personal data. The Bill will not create a new power but will create safeguards regarding the retention and use of datasets. In particular, the retention and exploitation of bulk personal data by the security and intelligence agencies will be subject to an authorisation process involving Secretary of State issued warrants and judicial approval.

Safeguards and oversight

13. The Bill will provide for an authorisation process under which 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. interception;
    b. targeted equipment interference by the security and intelligence agencies and the Ministry of Defence;
    c. bulk equipment interference;
    d. the acquisition of communications data *in bulk*;
    e. the obtaining, retaining and examination of bulk personal data by the security and intelligence agencies.

14. Warrants authorising targeted equipment interference by law enforcement will be issued by law enforcement chiefs, subject to approval of those warrants by Judicial Commissioners.

15. The Bill will contain an authorisation process for obtaining communications data which will broadly replicate the existing authorisation process, but with enhanced safeguards.

16. The Interception of Communications Commissioner, the Surveillance Commissioner, the Intelligence Services Commissioner and the Investigatory Powers Commissioner for Northern Ireland will be replaced by a single oversight body led by a powerful new Investigatory Powers Commissioner. The Investigatory Powers Commissioner will have oversight of the use of the powers in the Bill, as well as carrying out the functions of the existing Commissioners.

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

Introduction

18. The provisions in the Bill engage Articles 8 and 10, and Article 1 of the First Protocol of the Convention. These 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 Article 1 of the First Protocol requires that any deprivation of possessions must be "in the public interest".

19. It is axiomatic that for an interference with a Convention 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 accordingly.

20. 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 European Court of Human Rights ("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.[4]

21. 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.[5]

22. 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.

[4] *S and Marper* v. *United Kingdom,* 4 December 2008, (2009) 48 EHRR 50
[5] *Weber and Saravia v. Germany,* Admissibility Decision, 29 June 2006

23. 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

24. 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, at this point this memorandum describes some of these safeguards.

Judicial approval of warrants

25. A fundamental safeguard established by the Bill is an authorisation process (a 'double-lock') which provides that decisions to issue warrants will be subject to approval by independent judges called Judicial Commissioners.

26. The decision to issue a warrant must be taken personally by the Secretary of State. The Secretary of State will have to decide, amongst other things, that the warrant is necessary and proportionate. It will not be possible for the Secretary of State to issue a warrant until that decision has been reviewed and approved by a Judicial Commissioner. The Judicial Commissioner will review the Secretary of State's decision that the warrant is necessary and proportionate according to the principles that would apply on a judicial review. A key guarantee that warrants are necessary, proportionate and lawful is therefore the role played by a judge in assessing them as such. Judicial Commissioners will provide the same safeguard when warrants are to be renewed.

27. The Department's view is that this model more than meets the requirements of the Convention. 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. The double-lock authorisation process was similarly endorsed by the Committees that conducted pre-legislative scrutiny of the Bill.

28. 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, for example, 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 then be reviewed by a Judicial Commissioner within three working days and will cease to have effect if it is not approved. This means that a Judicial Commissioner can effectively

cancel an urgent warrant that he does not consider to be both necessary and proportionate. Where an urgent warrant is cancelled, the Judicial Commissioner will have the power to determine that any information that has already been obtained should be destroyed.

Oversight

29. The Bill will create an Investigatory Powers Commissioner, replacing the existing offices of the Interception of Communications Commissioner, Chief Surveillance Commissioner, Intelligence Services Commissioner and Investigatory Powers Commissioner for Northern Ireland. 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 at least as senior as a judge of the High Court). 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.

30. The Commissioners will be supported by a staff and will have access to technical and legal expertise. They will scrutinise the use of all of the investigatory powers in the Bill, including through audit and inspection and investigations.

31. The Judicial Commissioners will have access to all the information they need to provide effective oversight. 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 a Judicial Commissioner all documents and information the Commissioner may require to carry out their functions. Similarly, all members of public authorities will be required to provide a Judicial Commissioner with such assistance as the Commissioner may reasonably require. In particular, people will be required to provide the Judicial Commissioners with access to apparatus, systems and other facilities. This will allow the Commissioner wide ranging access, including to on-going investigations.

32. The Bill provides that people will be able to provide information to the Judicial Commissioners, regardless of any other legal restriction that might exist. This ensures, for example, that anyone with concerns about the use of investigatory powers will be able to inform a Judicial Commissioner. The only exception to this is that the protections for personal data in the Data Protection Act 1998 will continue to apply.

33. 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.

34. Where the Investigatory Powers Commissioner becomes aware of an error, either through inspections or through self reporting by public authorities, the Commissioner will have to inform the member of the public concerned if the Commissioner regards the error as serious and that it is in the public interest for the person to be informed. The Commissioner 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

35. The Bill will create a domestic right of appeal from decisions of the IPT, to the Court of Appeal, the Court of Session, or the Court of Appeal for Northern Ireland. Appeals will be possible in circumstances where the IPT has made a decision or determination and found there is a point of law at issue, which raises an important point of principle or practice (or there is some other compelling reason for an appeal to proceed). Currently the only option available to a complainant wishing to challenge a decision of the IPT is to bring a case before the ECtHR, while public authorities have no route of appeal.

36. The existing IPT rules and procedures have been found to be lawful by the ECtHR.[6] The provision of a domestic right of appeal therefore bolsters a system that is already compliant with the Convention.

Targeted Interception of Communications

37. 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.

In accordance with the law

38. The Bill will be a clear and accessible domestic basis for interception. The regime will be sufficiently foreseeable in that it builds on the safeguards in the

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

existing interception regime which has been scrutinised by the ECtHR and found to be foreseeable.

39. 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*),[7] 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.

40. 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 safeguards 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."[8]

41. 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."

Necessary

42. 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

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

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 is expressly limited to circumstances where there is a link to national security).

43. 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

44. 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.

45. The Secretary of State, or Scottish Ministers, may only issue a warrant if it is necessary in the interests of national security or the economic well-being of the UK where that is linked to national security, or for the purpose of the prevention or detection of serious crime. The warrant may only be issued if the conduct authorised is 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.

46. A warrant lasts for six 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.

47. The Bill includes specific and additional protections for items subject to legal privilege. Where one of the purposes of a warrant is to intercept items subject to legal privilege, the application for the warrant must include a statement that this is the case. Such a warrant can only be issued if the Secretary of State, or Scottish Ministers,consider that there are *exceptional* and *compelling* circumstances which make it necessary. Where the authority applying for the warrant considers that it is likely that items subject to legal privilege will be intercepted, the warrant application must state this and include a statement as to how likely intercepting such material is. A warrant for the purpose of intercepting items subject to legal privilege, , may only be issued if there are

specific safeguards in place for the handling, retention, use and destruction of privileged items. If such items are retained, the Investigatory Powers Commissioner must be informed as soon as reasonably practicable.

48. A Code of Practice will set out additional details regarding the procedures that must be followed before public authorities may intercept communications.[9] 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.

49. 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 targeted interception warrant to acquire a MP's communications. It will also include a requirement for the Prime Minister to be consulted in the event that an MP's communications collected under a bulk interception or equipment interference warrant were to be selected for examination. These protections will apply to MPs, members of the House of Lords, UK MEPs and members of the Scottish, Welsh and Northern Irish legislatures.

50. 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

51. 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.

52. There is limited ECtHR case law on the application of Article 8 to communications data, but the case of *Malone v UK*[10] provides some guidance, to the effect that while the situation is to be distinguished from the interception

[9] The Interception of Communications draft code of practice has been published for consultation alongside the Investigatory Powers Bill: www.gov.uk/government/uploads/system/uploads/attachment_data/file/504234/Interception_draft_code_of_practice.PDF

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

of the content of 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.

53. 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

54. 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

55. 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.[11] 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.

Proportionate means of achieving a legitimate aim

[11] 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."

56. 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 53(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.

57. 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).

58. 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.

59. 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.

60. 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.

61. The Department further considers that the provisions regarding the acquisition of communications data are proportionate. Access is only permitted by certain public authorities (see Schedule 4 to the Bill) 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.

62. 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. The designated senior officer must consult an accredited '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.

63. The Investigatory Powers Commissioner will be required to keep under review the exercise and performance of powers and duties under Part 3. The Commissioner's inspection team will actively examine applications to ensure the decision making (around necessity and proportionality) is appropriately rigorous.

64. 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 34.

65. 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.

66. The Bill provides for a sanction for misuse of the power to obtain communications data. A person within a public authority who knowingly or recklessly obtains communications data from a telecommunications operator without lawful authority will commit an offence. The offence is punishable by imprisonment for up to two years.

67. The Bill will contain additional safeguards regarding the use of communications data in order to identify a source of journalistic information. Public authorities will not be able to access communications data for that purpose without first obtaining the approval of a Judicial Commissioner. Therefore, 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.

68. 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.[12] 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.

69. Additional safeguards are also being put place for local authorities. The Bill includes a power to ensure that 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

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

71. The power to interfere with equipment is not new. The security and intelligence agencies may currently be issued with warrants under section 5 of the Intelligence Services Act 1994 authorising property interference. Law enforcement agencies 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.

72. Equipment interference necessarily engages Article 8 as it relates to the obtaining of communications and information which may be private. 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 is also engaged.

73. The Department's view is that the existing statutory basis for targeted equipment interference is adequate, providing a legal framework which ensures

[12] The Communications Data draft code of practice has been published for consultation alongside the Investigatory Powers Bill: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504239/Draft_CD_code_of_practice.PDF

that equipment interference is conducted in a proportionate and lawful way. This view is supported by the recent decision of the Investigatory Powers Tribunal, where the court concluded that the existing powers for property interference were lawful, with a proper balance being struck ensuring powers are used in a way which is proportionate.[13]

In accordance with the law

74. 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.[14] The targeted equipment interference regime will clarify, and build additional safeguards into, the existing legal framework which has been found to be lawful by the IPT.

Necessary

75. It will only be possible for an equipment interference warrant to be issued to the security and intelligence agencies 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. The Ministry of Defence can only apply for warrants where it is necessary in the interest of national security.

76. All law enforcement agencies listed in Bill will be able to apply for a warrant where it is necessary for the prevention and detection of serious crime. A more limited number of law enforcement agencies will also be able to obtain an equipment interference warrant where it is necessary to prevent death or injury to a person's physical or mental health, reflecting existing use of property interference in these circumstances.

77. It will not be possible for a warrant to be issued until the Secretary of State's or law enforcement Chief's decision that the warrant is necessary has been approved by a Judicial Commissioner.

78. The ability of law enforcement agencies and the 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

[13] Privacy International & Others v The Secretary of State for Foreign and Commonwealth Affairs and GCHQ – IPT 14/85/CH – February 2016

[14] The Equipment Interference draft code of practice has been published for consultation alongside the Investigatory Powers Bill: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504238/Equipment_interference_draft_code_of_practice.PDF

evidence in order to detection and prevent of serious crimes and respond to threats to our national security.

79. 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 computers and other devices for the purposes of intelligence and evidence gathering. If equipment interference warrants were not available, the detection and prevention of serious crime and threats to national security could be undermined, leaving law enforcement agencies and security and intelligence agencies unable to access critical information.

Proportionate means of achieving a legitimate aim

80. 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 conduct authorised is proportionate.

81. 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.

82. Safeguards have been included in the Bill to ensure that equipment interference cannot be carried out in an arbitrary way and that any interference with Convention rights is kept to the minimum necessary. Public authorities conducting activity under an equipment interference warrants will be required to ensure that adequate safeguards are in place for information that is acquired. These 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. There will be a duty not to make an unauthorised disclosure under an equipment interference warrant and it will be an offence to make such a disclosure where the person knows that it would be in breach of this duty.

83. The equipment interference regime will contain the same protections for items subject to legal privilege as will exist for targeted interception (see paragraph 47 above). The protections for Parliamentarians will apply to equipment interference as it does for targeted interception (see paragraph 49).

84. The Equipment Interference Code of Practice will contain safeguards regarding access to confidential information, such as journalistic material. The draft code makes it clear that special consideration should be given where such

information is likely to be acquired. Where the intention is to acquire such material, an application for warrant will need to 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

85. 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 34 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

86. 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 Article 1 of the First Protocol for the same reason as targeted equipment interference.

In accordance with the law

87. As for 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

88. The use of bulk powers is necessary for the security and intelligence services to counter effectively threats to national security. The case for the necessity of bulk powers has been set out in detail in the Operational Case for Bulk Powers published alongside the Bill.[15]

89. 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. It will not be possible for a warrant to be issued (subject to the procedure for urgent warrants which can apply to bulk equipment interference warrants) until the Secretary of State's decision that the warrant is necessary has been approved by a Judicial Commissioner.

[15] The Operational Case for Bulk Powers: https://www.gov.uk/government/publications/investigatory-powers-bill-overarching-documents

Proportionate means of achieving a legitimate aim

90. It will only be possible for bulk warrants to be issued in the interests of national security and where the conduct authorised is proportionate to what is sought to be achieved. It will not be possible to issue a bulk interception warrant, bulk equipment interference warrant or a bulk acquisition warrant until a Judicial Commissioner has approved the Secretary of State's decision that the conduct authorised is proportionate.

91. The warrants may result in the acquisition of large volumes of untargeted 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 contains safeguards that apply at the stage that communications are selected for examination, to ensure that material is only selected where it is necessary and proportionate for specific purposes.

92. Each bulk warrant will set out the operational purposes for which the information may be selected for examination. The warrant will therefore authorise the examination of information obtained for only certain specified purposes. It will not be possible for the bulk warrant to be issued until a Judicial Commissioner has approved the Secretary of State's decision that each operational purpose is necessary.

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

94. 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.

95. The regime for bulk interception will contain the same safeguards as for targeted interception, as well as the safeguards common to the bulk powers. In addition, it will only be possible to issue a bulk interception warrant where the main purpose relates to communications sent or received by persons overseas. 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 person who is known to be in the British Islands may not be examined unless the Secretary of State is satisfied that the examination is necessary for one of the statutory purposes and is proportionate, and a Judicial Commissioner has approved that decision.

96. 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).[16]

97. The bulk equipment interference regime will contain the safeguards in place for the targeted regime, plus the safeguards common across the bulk powers. In addition, a bulk equipment interference warrant will be available only where the main purpose is to facilitate the obtaining of communications, information or equipment data which overseas-related.

98. The bulk equipment interference regime will contain a similar safeguard at the point of examination as exists for bulk interception. A targeted examination warrant will be required if criteria used to select material for examination is referable to a person known to be in the British Island and the purpose of using that criteria is to identify communications set by, or intended for, that individual or private information relating to that individual.

Bulk Personal Data

99. 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 datasets 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.

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

In accordance with the law

101. The acquisition and use of bulk personal datasets 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

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

disclosed to an Agency for one of its functions may be used for any of its other functions.

Necessary

102. Bulk personal datasets play an integral role in allowing the intelligence and security agencies to carry out their functions. They are used, for example, to establish links between subjects of interest or to validate information obtained from other sources. Without bulk personal datasets, the security and intelligence agencies would be significantly less effective in protecting the UK against threats such as terrorism, cyber attacks and espionage. Further detail of the critical role played by bulk personal data is included in the Operational Case for Bulk Powers.[17]

103. Under the Bill the security and intelligence agencies' retention and use of bulk personal datasets 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 before the warrant can be issued.

Proportionate means of achieving a legitimate aim

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

105. The use of bulk personal datasets is proportionate in that it can limit the use of intrusive powers in two ways. Firstly, it allows the security and intelligence agencies to obtain information that might otherwise be sought using more intrusive methods. Secondly, it allows the security and intelligence agencies to focus their efforts on individuals who threaten our national security or who may be of intelligence interest whilst limiting the need to interfere with the privacy of innocent people.

106. A statutory code of practice will provide further safeguards regarding how the agencies access, store, destroy and disclose information contained in bulk personal datasets.[18]

[17] The Operational Case for Bulk Powers: https://www.gov.uk/government/publications/investigatory-powers-bill-overarching-documents

[18] The Intelligence and Security Agencies' retention and use of bulk personal datasets draft code of practice has been published for consultation alongside the Investigatory Powers Bill:

The Charter of Fundamental Rights

107. 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.[19] 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).

108. 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.

109. The Divisional Court found in July 2015 that section 1 of DRIPA 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.[20] The Home Secretary appealed to the Court of Appeal.

110. In November 2015 the Court of Appeal set out its provisional disagreement with the Divisional Court's finding that section 1 of DRIPA 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 Court of Appeal expressed serious doubt that the CJEU in Digital Rights Ireland had intended to set out mandatory requirements for domestic legislation or to extend the effect of the Charter Rights beyond the Convention. The Court of Appeal has referred questions as to the interpretation of the Digital Rights Ireland case to the CJEU, which will hear the case together with another preliminary reference from Sweden (Tele2) in April this year.

111. 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' access regimes. Domestic access regimes are not implementing EU law and so subject to EU law and the Charter does not apply. Safeguards in domestic

---

www.gov.uk/government/uploads/system/uploads/attachment_data/file/504237/Bulk_Personal_Datasets_SIA_draft_code_of_practice.PDF

[19] C-293/12 Digital Rights Ireland & C-594/12 Seitlinger.

[20] R. (on the application of Davis) v Secretary of State for the Home Department, [2015] EWHC 2092 (Admin)

access regimes should be a matter or the domestic courts. The requirements of the Charter do not in any event go beyond the requirements of Article 8, and the provisions of DRIPA are compatible with the Convention.

Conclusion

112. The Department recognises that the Bill, and the conduct that may be authorised under warrants and notices issued and given under the Bill, engage Convention rights. It is the Department's view that, for the reasons set out in this Memorandum, the Bill is fully compliant with the Convention.

Home Office

8 March 2016