Case No. IPT/15/110/CH

IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

PRIVACY INTERNATIONAL

Claimant

and

(1) SECRETARY OF STATE FOR FOREIGN AND COMMONWEALTH AFFAIRS
(2) SECRETARY OF STATE FOR THE HOME DEPARTMENT
(3) GOVERNMENT COMMUNICATIONS HEADQUARTERS
(4) SECURITY SERVICE
(5) SECRET INTELLIGENCE SERVICE

Respondents

THE RESPONDENTS' AMENDED OPEN RESPONSE

INTRODUCTION

1. This Open Response to the Claim:

   (a) Summarises the need for the "neither confirm nor deny" policy, and explains its operation in the present case p2.

   (b) Sets out an outline of the Tribunal's procedural regime, insofar as is relevant to the present Claim pp2-4.

   (c) Responds to the complaints made in the proceedings insofar as is possible in an Open Response. In particular, it:

      (a) sets out the Respondents' open position on the factual allegations pp4-7;

      (b) sets out the relevant domestic legal regime in relation to Bulk Personal Datasets and Section 94 of the Telecommunications Act 1984 pp7-36;

      (c) identifies the pure issues of law which are suitable for determination at a public *inter partes* hearing ("a Legal Issues Hearing") p37; ~~and~~

      (d) sets out the Respondents' position on those pure issues of law, pp37-44; and

      (e) responds to further grounds of challenge raised by the

Claimant in its Re-Amended Statement of Grounds, pp.44-47.

~~(d) Suggests directions for the future management of the Claim p44.~~

THE "NEITHER CONFIRM NOR DENY" POLICY, AND ITS OPERATION IN THE PRESENT CASE

2. Secrecy is essential to the necessarily covert work and operational effectiveness of the Intelligence Services, whose primary function is to protect national security. See *e.g. Attorney General v. Guardian Newspapers Ltd (No.2)* [1990] 1 AC 109, *per* Lord Griffiths at 269F.

3. As a result, the mere fact that the Intelligence Services[1] are carrying out an investigation or operation in relation to say, a terrorist group or hold information on a suspected terrorist will itself be sensitive. If, for example, a hostile individual or group were to become aware that they were the subject of interest by the Intelligence Services, they could not only take steps to thwart any (covert) investigation or operation but also attempt to discover, and perhaps publicly reveal, the methods used by the Intelligence Services or the identities of the officers or agents involved. Conversely, if a hostile individual or group were to become aware that they were not the subject of Intelligence Service interest, they would then know that they could engage or continue to engage in their undesirable activities with increased vigour and increased confidence that they will not be detected.

4. In addition, and with particular relevance to the present Claim, an appropriate degree of secrecy must be maintained as regards the intelligence-gathering capabilities and techniques of the Intelligence Services (and any gaps in or limits to those capabilities and techniques). If hostile individuals or groups acquire detailed information on such matters then they will be able to adapt their conduct to avoid, or at least minimise, the risk that the Intelligence Services will be able successfully to deploy those capabilities and techniques against them.

5. It has thus been the policy of successive UK Governments to neither confirm nor deny whether they are monitoring the activities of a particular group or individual, or hold information on a particular group or individual, or have had contact with a particular individual. Similarly, the long-standing policy of the UK Government is to neither confirm nor deny the truth of claims about the operational activities of the Intelligence Services, including their intelligence-gathering capabilities and techniques. That long-standing policy is applied in this Open Response.

THE TRIBUNAL'S PROCEDURAL REGIME[2]

6. The Tribunal's procedure is governed by ss. 67-69 of RIPA and the

[1] The term "Intelligence Services" is used in this Response to refer to the Security Service, Secret Intelligence Service and Government Communications Headquarters.
[2] The Tribunal's jurisdiction and remedial powers are addressed below.

Investigatory Powers Tribunal Rules 2000, SI 2000/2665 ("the Rules"), made under s. 69.

7. In §173 of the Procedural Ruling of 22 January 2003 in IPT/01/62 and IPT/01/77 ("the Procedural Ruling") the Tribunal concluded that r. 9(6) of the Rules[3] was *ultra vires* the rule-making power in s. 69 of RIPA. Further, the Tribunal held that:

   (a) "purely legal arguments, conducted for the sole purpose of ascertaining what is the law and not involving the risk of disclosure of sensitive information" should be heard by the Tribunal in public (Procedural Ruling, §172); and

   (b) the Tribunal's reasons for its ruling on any "pure questions of law" (§195) that are raised at such a hearing may be published without infringing either r. 13 of the Rules or s. 68(4) of RIPA[4] (Procedural Ruling, §§190-191).

8. It follows that, where necessary, the Tribunal may hold a Legal Issues Hearing to consider any relevant (and disputed) pure issues of law,[5] and may subsequently publish its rulings (with its reasoning) on such issues.

9. The Tribunal also concluded in the Procedural Ruling that, with the exception of r. 9(6), the Rules are valid and binding (§148). It follows from this conclusion, and from r. 6(2)-(5) of the Rules, that - prior to the determination of a claim[6] - the Tribunal cannot disclose to a claimant anything that a respondent has decided should only be disclosed to the Tribunal, and similarly cannot order a respondent to make such disclosure itself.

10. The overall effect of the Procedural Ruling is thus that:

   (a) where necessary, the Tribunal first holds a Legal Issues Hearing to determine such relevant pure issues of law as are in dispute between the parties, and publishes its rulings (with reasons) on those pure issues of law;

   (b) the Tribunal then investigates the claim in closed session; and

---

[3] R. 9(6) provides:
"*The Tribunal's proceedings, including any oral hearing, shall be conducted in private.*"

[4] The effect of r. 13 and s. 68(4) is in essence that if the claim is dismissed then the Tribunal may only give to the claimant a statement that "*no determination has been made in his favour*", but that if the claim is upheld then the Tribunal may, subject to r. 6(1), provide a summary of its determination, including any findings of fact.

[5] As the Tribunal confirmed in the subsequent case of *Frank-Steiner v. the Data Controller of the Secret Intelligence Service* (IPT/06/81/CH), 26 February 2008, at §5, the pure issues of law can as necessary be considered on the basis of hypothetical facts.

[6] As noted in footnote 4 above, the Tribunal has power - subject to r. 6(1) - to provide a summary of its determination, including any findings of fact, in the event that the overall claim is upheld.

(c) as necessary,[7] the Tribunal applies its rulings on the pure issues of law to the facts that it has found following its closed session investigation of the claim.

11. This was the approach taken in the two joined cases which gave rise to the Procedural Ruling. Following the Procedural Ruling, the two cases were separated and disputed pure issues of law were identified and determined following Legal Issues Hearings (the ruling on the pure issues of law in IPT/01/77 of 9 December 2004 is considered below). Each claim was then finally determined following the Tribunal's investigation of the cases in closed session. This was similarly the approach taken in *Frank-Steiner v. the Data Controller of the Secret Intelligence Service* (IPT/06/81/CH).[8]

12. The European Court of Human Rights ("the ECtHR") unanimously upheld the lawfulness of the Tribunal's procedural regime as summarised above in *Kennedy v. UK* (2011) 52 EHRR 4, at §§184-191. (*Kennedy* arose out of one of the domestic cases that gave rise to the Procedural Ruling, namely IPT/01/62.)

13. In the Respondents' submission therefore, the approach set out in §10 above is the one prescribed in the Rules, is tailored to the subject matter of the matters falling within the Tribunal's jurisdiction, has been expressly accepted as fair and compatible with the ECHR by the ECtHR; and should be followed by the Tribunal in the present Claim.

14. The Respondents are filing a Closed Response in addition to this Open Response. For the avoidance of doubt, the Respondents' position, with respect to the Tribunal, is that in the light of r. 6 of the Rules, the Procedural Ruling and *Kennedy*, nothing in the Closed Response can be disclosed to the Claimants without the Respondents' consent.

THE RESPONDENTS' OPEN POSITION ON THE FACTUAL ALLEGATIONS

15. The Respondents set out here, so far as is possible in an Open Response, their position on the factual allegations made in the Claim. The Respondents also address those allegations in the Closed Response which is filed herewith.

16. In order to meet the requirements of their statutory functions, the Respondents need to collect a range of information from a variety of sources. They do this in accordance with section 2(2)(a) of the Security Service Act

---

[7] Following its investigation the Tribunal may *e.g.* find that the respondents have not in fact undertaken any activities in relation to a claimant, with the result that the claim will be dismissed without the need to apply the rulings on the pure issues of law to any specific factual findings.

[8] There is a class of Tribunal cases that have not proceeded in this way (see *e.g. Paton v. Poole Borough Council*, IPT/09/01-05/C, determination of 29 July 2010). But that is because, in these cases, the respondents have decided that the entirety of their factual case can be dealt with in open session, with the result that the Legal Issues Hearing becomes in effect indistinguishable from a substantive hearing on all disputed matters. Where, however, a respondent decides that any part of its factual case is closed, then the approach in §10 and §14 applies.

1989 and sections 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994. These provisions are referred to below as the "information gateway provisions".

17. Among the range of information collected are sets of data that contain personal information about a wide range of individuals, the majority of whom are unlikely to be of any intelligence interest. Typically these datasets are very large, and of a size which means they cannot be processed manually. Such datasets have generally been referred to within the Intelligence Services as 'Bulk Personal Datasets'.

18. Such datasets provide information about subjects of intelligence interest, but inevitably also include information about those who are of no direct relevance to operations or investigations by the Intelligence Services. It is not possible to acquire the information that will be of direct value to such operations without also acquiring this additional data; indeed, at the point of acquisition it may not be known exactly which information will prove to be of value.

19. The Intelligence Services draw on this data and use it in conjunction with other data in order to perform their functions, for example, to identify Subjects of Interest, or unknown individuals who surface in the course of investigations; to establish links between individuals and groups, or otherwise improve understanding of a target's behaviour and connections; to validate intelligence obtained through other sources; or to ensure the security of operations or staff. 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 Intelligence Services are correctly and solely focused on those individuals or organisations that are relevant to the performance of their statutory functions.

20. Significant national security benefits arise from integrating bulk personal datasets with information about individual targets from traditional sources of intelligence, or from 'fusing' different datasets to identify common links or matching profiles. Furthermore, the use of Bulk Personal Datasets is of increasing importance to investigations by the Intelligence Services.[9]

21. Examples of the use of Bulk Personal Datasets by the Intelligence Services in their work to protect national security, such as counter-terrorism, include:

    (a) Protection of Major Events: When significant events take place – such as the NATO Summit in Wales in 2014 or the London Olympics in 2012 – the intelligence services work to ensure they pass off safely. This includes tracing the details of individuals with access to venues so as to mitigate the risk that subjects of national security interest might gain access to these events. The majority of individuals in such sets will not be of direct intelligence interest and this data is therefore

[9] As recognised by the Intelligence and Security Committee of Parliament in their Privacy and Security report published in March 2015. See page 59: "These datasets are an increasingly important investigative tool for the Agencies."

categorised as Bulk Personal Data.

(b) Identifying Foreign Fighters: Timely access to travel data has provided advance notice of the unexpected return to the UK of subjects of interest. This helps the Intelligence Services to prepare a tailored response prior to their arrival to better mitigate the threat they pose to national security. Information derived from travel data has also been critical to the ability of the Intelligence Services and their international partners to construct an intelligence picture of individuals travelling to join ISIL in Syria and Iraq.

(c) Identifying Subjects of Interest: The name of an individual reported to be storing a weapon used in a terrorist attack was identified by the Intelligence Services. A combination of three Bulk Personal Datasets were used to fully identify this person from hundreds of possible candidates. This resulted in the recovery of the weapon and aided in the subsequent conviction of the individuals involved in the attack who are now serving lengthy prison sentences.

(d) Focusing Investigative Resources: Intelligence indicated that a partially identified associate of a known Subject of Interest aspired to travel to Syria for extremist purposes. Using Bulk Personal Datasets analysts were able to quickly identify the associate enabling rapid focus of investigative effort on the one individual of concern, discounting hundreds of other potential candidates. Without access to Bulk Personal Datasets, a resource intensive and more intrusive process would have been needed to identify the individual from the hundreds of associates, incurring avoidable collateral intrusion into individuals of no intelligence interest and at significant risk of failing to identify the individual prior to travel.

22. Directions have been issued under section 94 of the Telecommunications Act 1984 requiring communications service providers ("CSPs") to provide bulk communications data ("BCD"), which has subsequently been stored and accessed by the Intelligence Services ("the Section 94 Regime"). See further paragraphs 195-202 below.

23. Similar considerations arise in relation to BCD as in relation to BPD: it involves large amounts of data, most of which relates to individuals who are unlikely to be of any intelligence interest. It is also of significant, and increasing, importance to the Intelligence Services. Fast and secure access to communications data is essential to the Agencies in order to progress investigations. It is often the only investigative lead they have to be able to work from. Communications data has played an important part in every MI5 investigation over the last decade. The use of section 94 to acquire communications data in bulk from CSPs who provide services in the UK is used to deal with the most serious threats facing the UK. It has saved lives and protected national security.

24. For example, in 2010 a group of terrorists were plotting to attack several public locations in the UK, including the London Stock Exchange. Following

an intensive investigation, in which analysis of BCD played a key role, particularly given geographical separate of different parts of the network, the group were all identified and their plot uncovered. The Intelligence Services were able to work with police to disrupt them in time and the group were charged with terrorism offences. All were convicted and sentenced to prison terms.

25. Without this capability, the Intelligence Services would have to undertake many more individual requests or use more intrusive powers to narrow the scope of a search, with far greater intrusion into people's privacy.

26. Beyond these matters, the Respondents maintain the standard "neither confirm nor deny" stance for intelligence matters. Accordingly, they do not provide in this open Response any further indication as to the nature or extent either of the Bulk Personal Datasets that they hold, or as to the communications data accessed pursuant to the section 94 Regime.

Claimant's standing

27. In this Open Response, the Respondents do not address the allegation (at §33 of the Amended Grounds) that it is likely that information about the Claimant, and those that work for it, has been acquired using section 94 of the Telecommunications Act 1984 and is present in at least one Bulk Personal Dataset. The Respondents are unable to confirm or deny such allegations for reasons explained at §§2-5 above. However, the Respondents nevertheless accept that the Claimant may challenge the ECHR/EU-law compatibility of the Bulk Personal Datasets ("BPD") and Section 94 Regimes on the basis that such information might in principle have been so acquired and/or present in a Bulk Personal Dataset.

THE REGIMES FOR BULK PERSONAL DATASETS AND S. 94 OF THE TELECOMMUNICATIONS ACT 1984

28. The regimes in respect of BPD and section 94 of the Telecommunications Act 1984 which are relevant to the activities of the Intelligence Services principally derive from the following statutes:

(a) the Security Services Act 1989 ("the SSA") and the Intelligence Services Act 1994 ("the ISA");

(b) the Counter-Terrorism Act 2008 ("the CTA");

(c) Section 94 of the Telecommunications Act 1984;

(d) the Human Rights Act 1998 ("the HRA");

(e) the Data Protection Act 1998 ("the DPA"); and

(f) the Official Secrets Act 1989 ("the OSA").

29. Also relevant are the Handling Arrangements for BPD and the Handling Arrangements for section 94 of the Telecommunications Act 1984, which were published on 4 November 2015.

The SSA and ISA

Security Service functions

30. By s.1(2) to (4) of the Security Service Act 1989 ("SSA"), the functions of the Security Service are the following:

"the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means."

"to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands."

"to act in support of the activities of police forces, the National Crime Agency and other law enforcement agencies in the prevention and detection of serious crime."

31. The Security Service's operations are under the control of a Director-General who is appointed by the Secretary of State (s.2(1)). By s.2(2)(a) it is the Director-General's duty to ensure:

"...that there are arrangements for securing that no information is obtained by the Service except so far as necessary for the proper discharge of its functions or disclosed by it except so far as necessary for that purpose or for the purpose of the prevention or detection of serious crime or for the purpose of any criminal proceedings;..."

SIS functions

32. By s.1(1) of the ISA, the functions of SIS are:

"(a) to obtain and provide information relating to the actions or intentions of persons outside the British Islands; and
(b) to perform other tasks relating to the actions or intentions of such persons."

33. By s.1(2) those functions are *"exercisable only-*

"(a) in the interests of national security, with particular reference to the defence and foreign polices of Her Majesty's Government in the United Kingdom; or

(b) in the interests of the economic well-being of the United Kingdom; or

(c) in support of the prevention or detection of serious crime."

34. SIS's operations are under the control of a Chief, who is appointed by the

Secretary of State (s.2(1)). The Chief of SIS has a duty under s.2(2)(a) of the ISA to ensure:

"(a) that there are arrangements for securing that no information is obtained by the Intelligence Service except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary-

(i) for that purpose;

(ii) in the interests of national security;

(iii) for the purpose of the prevention or detection of serious crime; or

(iv) for the purpose of any criminal proceedings;..."

GCHQ functions

35. By s. 3(1)(a) of the ISA, the functions of GCHQ include the following:

"... to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material ...."

36. By s. 3(2) of the ISA, these functions are only exercisable:

"(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or
(b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or
(c) in support of the prevention or detection of serious crime."

37. GCHQ's operations are under the control of a Director, who is appointed by the Secretary of State (s. 4(1)). By s. 4(2)(a), it is the duty of the Director to ensure:

"... that there are arrangements for securing that no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings ..."

38. The functions of each of the Intelligence Services, and the purposes for which those functions may properly be exercised, are thus prescribed by statute. In addition, the duty-conferring provisions in section 2(2)(a) of the SSA and sections 2(2)(a) and 4(2)(a) of the ISA, otherwise known as *"the information gateway provisions"*, place specific statutory limits on the information that each of the Intelligence Services can obtain and disclose. These statutory limits apply to the obtaining and disclosing of information from or to other persons both in the United Kingdom and abroad.

Counter-Terrorism Act 2008

39. By s.19(1) of the Counter-Terrorism Act 2008 ("CTA") *"A person may disclose information to any of the intelligence services for the purposes of the exercise by that service of any of its functions."*

40. By s. 19(2) of the CTA:

> *"Information obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions."*

41. By s.19(3) to (5) of the CTA, information obtained by the Intelligence Services for the purposes of any of their functions may:

(a) In the case of the Security Service *"be disclosed by it – (a) for the purpose of the proper discharge of its functions, (b) for the purpose of the prevention or detection of serious crime, or (c) for the purpose of any criminal proceedings."* (s.19(3))

(b) In the case of SIS *"be disclosed by it – (a) for the purpose of the proper discharge of its functions, (b) in the interests of national security, (c) for the purpose of the prevention or detection of serious crime, or (d) for the purpose of any criminal proceedings."* (s.19(4))

(c) In the case of GCHQ *"be disclosed by it - (a) for the purpose of the proper discharge of its functions, or (b) for the purpose of any criminal proceedings."* (s.19(5))

42. By s.19(6) any disclosure under s.19 *"does not breach –*

(a) any obligation of confidence owed by the person making the disclosure, or

(b) any other restriction on the disclosure of information (however imposed)."

43. Furthermore:

(a) s.19 does not affect the duties imposed by the information gateway provisions (s.19(7) and s.20(1) of the CTA).

(b) by s.20(2) of the CTA, nothing in s.19 *"authorises a disclosure that-*

(a) contravenes the Data Protection Act 1998 (c.29), or
(b) is prohibited by Part 1 of the Regulations of Investigatory Powers Act 2000 (c.23)."

44. Thus, specific statutory limits are imposed on the information that the Intelligence Services can obtain, and on the information that it can disclose under the CTA.

Other statutory bases for obtaining information

45. Information contained in a Bulk Personal Dataset may be obtained by other means, including pursuant to:

(a) Warrants issued under section 5 of the ISA in respect of property and equipment interference;

(b) Authorisations issued under section 7 of the ISA in respect of property and equipment interference;

(c) Intrusive surveillance warrants issued under section 43 of the Regulation of Investigatory Powers Act 2000 ("RIPA");

(d) Directed surveillance authorisations issued under section 28 of RIPA;

(e) Covert human intelligence authorisations issued under section 29 of RIPA; and

(f) Warrants for the interception of communications issued under section 5 of RIPA

46. It is important to note that these other statutory means of obtaining information are themselves subject to their own statutory requirements, in addition to any further requirements derived from the Handling Arrangements set out below.

Section 94 of the Telecommunications Act 1984

47. S.94 of the Telecommunications Act 1984 ("TA") provides:

"94.- Directions in the interests of national security etc.

(1) The Secretary of State may, after consultation with a person to whom this section applies, give to that person such directions of a general character as appear to the Secretary of State to be necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom.

(2) If it appears to the Secretary of State to be necessary to do so in the interests of national security or relations with the government of a country or territory outside the United Kingdom, he may, after consultation with a person to whom this section applies, give to that person a direction requiring him (according to the circumstances of the case) to do, or not to do, a particular thing specified in the direction.

(2A) The Secretary of State shall not give a direction under subsection (1) or (2) unless he believes that the conduct required by the direction is proportionate to what is sought to be achieved by that conduct.

(3) A person to whom this section applies shall give effect to any direction given to him by the Secretary of State under this section notwithstanding any other duty imposed on him by or under Part 1 or Chapter 1 of Part 2 of the Communications Act

2003 and, in the case of a direction to a provider of a public electronic communications network, notwithstanding that it relates to him in a capacity other than as the provider of such a network.

(4) The Secretary of State shall lay before each House of Parliament a copy of every direction given under this section unless he is of opinion that disclosure of the direction is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of any person.

(5) A person shall not disclose, or be required by virtue of any enactment or otherwise to disclose, anything done by virtue of this section if the Secretary of State has notified him that the Secretary of State is of the opinion that disclosure of that thing is against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of some other person.

(6) The Secretary of State may, with the approval of the Treasury, make grants to providers of public electronic communications networks for the purposes of defraying or contributing towards any losses they may sustain by reason of compliance with the directions given under this section.

(7) There shall be paid out of money provided by Parliament any sums required by the Secretary of State for making grants under this section.

(8) This section applies to OFCOM and to providers of public electronic communications networks."

48. The Secretary of State's power to give directions under section 94, whether of a general character (s.94(1)) or requiring specific action (s.94(2)) is limited to directions which appear to the Secretary of State to be *"necessary"* in the interests of national security or international relations (s.94(1)) and which the Secretary of State believes to be *"proportionate"* to what is sought to be achieved. The Secretary of State must also first consult with the person to whom the direction is to be given (s.94(1) and (2)).

The HRA

49. Art. 8 of the ECHR is a "Convention right" for the purposes of the HRA: s. 1(1) of the HRA. Art. 8, set out in Sch. 1 to the HRA, provides as follows:

"(1) Everyone has the right to respect for his private and family life, his home and his correspondence.
(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevent of disorder or crime, for the protection of health and morals, or for the protection of the rights and freedoms of others."

50. By s. 6(1):

"It is unlawful for a public authority to act in a way which is incompatible with a

Convention right."

51. Each of the Intelligence Services is a public authority for this purpose. Thus, when undertaking any activity that interferes with Art. 8 rights, the Respondents must (among other things) act proportionately and in accordance with law. In terms of bulk activity relating to Bulk Persona Data and section 94 of the Telecommunications Act 1984, the HRA applies at every stage of the process i.e. authorisation, acquisition, use/access, disclosure, retention and deletion.

52. S. 7(1) of the HRA provides in relevant part:

> *"A person who claims that a public authority has acted (or proposes to act) in a way which is made unlawful by section 6(1) may –*
> *(a) bring proceedings against the authority under this Act in the appropriate court or tribunal ...."*

The DPA

53. Each of the Intelligence Services is a data controller (as defined in s. 1(1) of the DPA) in relation to all the personal data that it holds. "Personal data" is defined in s.1(1) of the DPA as follows:

> *"data which relate to a living individual who can be identified-*
> *i. from those data; or*
> *ii. from those data and other information which is in the possession of, or is likely to come into the possession of the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual."*

54. Insofar as the obtaining of an item of information by any of the Intelligence Services amounts to an interference with Art. 8 rights, that item of information will in general amount to personal data.

55. Consequently as a data controller, the Respondents are in general required by s. 4(4) of the DPA to comply with the data protection principles in Part I of Sch. 1 to the DPA. That obligation is subject to ss. 27(1) and 28(1) of the DPA, which exempt personal data from (among other things) the data protection principles if the exemption "*is required for the purpose of safeguarding national security*". By s. 28(2) of the DPA, a Minister may certify that exemption from the data protection principles is so required. Copies of the ministerial certificates for each of the Intelligence Services are available on request. Those certificates certify that personal data that are processed in performance of the Intelligence Services' functions are exempt from the first, second and eighth data protection principles (and are also exempt in part from the sixth data protection principle). Thus the certificates do <u>not</u> exempt the Intelligence Services from their obligation to comply with the fifth and seventh data protection principles, which provide:

"5. Personal data processed[10] *for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. …*

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."[11]

56. Accordingly, when the Respondents obtain any information which amounts to personal data, they are obliged:

(a) not to keep that data for longer than is necessary having regard to the purposes for which they have been obtained and are being retained / used; and

(b) to take appropriate technical and organisational measures to guard against unauthorised or unlawful processing of the data in question and against accidental loss of the data in question.

The OSA

57. A member of the Intelligence Services commits an offence if *"without lawful authority he discloses any information, document or other article relating to security or intelligence which is or has been in his possession by virtue of his position as a member of any of those services"*: s. 1(1) of the OSA. A disclosure is made with lawful authority if, and only if, it is made in accordance with the member's official duty (s. 7(1) of the OSA). Thus, a disclosure of information by a member of any of the Respondents that is *e.g.* in breach of the relevant "arrangements" (under s. 4(2)(a) of the ISA) will amount to a criminal offence. Conviction may lead to an imprisonment for a term not exceeding two years and/or a fine (s. 10(1) of the OSA).

58. Further, a member of the Intelligence Services commits an offence if he fails to take such care, to prevent the unauthorised disclosure of any document or other article relating to security or intelligence which is in his possession by virtue of his position as a member of any of those services, as a person in his position may reasonably be expected to take. See s. 8(1) of the OSA, as read with s. 1(1). Conviction may lead to an imprisonment for a term not exceeding three months and/or a fine (s. 10(2) of the OSA).

Open Handling Arrangements

59. Arrangements exist for the obtaining, use and disclosure of:

(a) Bulk Personal Datasets ("the BPD Handling Arrangements"); and

(b) Bulk Communications Data pursuant to directions under s.94 of the

---

[10] The term "processing" is broadly defined in s. 1(1) of the DPA to include (among other things), obtaining, recording and using.

[11] The content of the obligation imposed by the seventh data protection principle is further elaborated in §§9-12 of Part II of Sch. 1 to the DPA.

Telecommunications Act 1984 ("the Section 94 Handling Arrangements").

60. Both sets of Handling Arrangements apply to each of the Intelligence Services and were made under s.2(2)(a) of the Security Service Act 1989 and ss.2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994. They came into force on 4 November 2015. They are mandatory and are required to be followed by staff in the Intelligence Services. Failure by staff to comply with the Handling Arrangements may lead to disciplinary action, which can include dismissal and prosecution (see §§1.1 to 1.3 of the BPD Handling Arrangements and §§1.1 to 1.3 of the Section 94 Handling Arrangements).

BPD Handling Arrangements

61. The BPD Handling Arrangements apply to obtaining, use and disclosure of "bulk personal datasets" (§1.2) as defined at §2.2:

"2.2 Among the range of information collected is ***data that contain personal information about a wide range of individuals, the majority of whom are unlikely to be of any intelligence interest****. Typically these datasets are very large, and of a size which means they cannot be processed manually. Such datasets are referred to as* ***bulk personal datasets****. For the purposes of these Handling Arrangements, a 'bulk personal dataset' means any collection of information which:*

(a) Comprises personal data;

(b) Relates to a wide range of individuals, the majority of whom are unlikely to be of intelligence interest; and

(c) Is held, or acquired for the purpose of holding, on one or more analytical systems within the Intelligence Services."

62. "Personal data" is defined as having the meaning given to it in s.1(1) of the Data Protection Act 1998 (§2.3), but additionally includes data related to the deceased.

63. The purpose of the acquisition and use of BPD is explained at §§2.4-2.5:

"2.4 Bulk personal datasets may be acquired through overt and covert channels. Such datasets provide information about subjects of intelligence interest ("subjects of interest"), but inevitably also include information about those who are of no direct relevance to Intelligence Service operations. It is not possible to acquire the information that will be of direct value to these operations without also acquiring this additional data; indeed, at the point of acquisition it may not be known exactly which information will prove to be of value.

2.5 The Intelligence Services draw on this data and use it 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. It may also be used to facilitate the exclusion of individuals from an investigation or in pursuit of other intelligence requirements. This ensures that the activities of the

Intelligence Services are correctly and solely focused on those individuals or organisations that are relevant to the performance of their statutory functions."

64. The requirement that acquisition, use, retention and disclosure of BPD have *"clear justification, accompanied by detailed and comprehensive safeguards against misuse"* and be *"subject to rigorous oversight"* is made clear (§2.6). The BPD Handling Arrangements are intended to provide such safeguards (§2.7) and must be complied with, along with the requirements of the information gateway provisions:

"Staff must ensure that no bulk personal dataset is obtained, used, retained or disclosed ***except in accordance with the information gateway provisions*** *and* ***these Arrangements.***"

65. The BPD Handling Arrangements apply to BPD *"howsoever obtained"*, that is through whichever of the variety of statutory powers by which the Intelligence Services are entitled to obtain it (§§2.8-2.9) without prejudice to *"additional applicable statutory requirements"* which apply in the case of some statutory powers (§2.9).

66. The BPD Handling Arrangements set out provisions in respect of each of the stages of the lifecycle of a Bulk Personal Dataset.

Authorisation and Acquisition

67. The key requirements on staff of the Intelligence Services before obtaining BPD are set out at §4.2:

"based on the information available to them at the time, staff should always:

- *be satisfied that the objective in question falls within the Service's statutory functions;*
- *be satisfied that it is* ***necessary*** *to obtain and retain the information concerned in order to achieve the objective;*
- *be satisfied that obtaining and retaining the information in question is* ***proportionate*** *to the objective;*
- *be satisfied that only as much information will be obtained as is* ***necessary*** *to achieve that objective."*

68. Clear guidance is provided to staff on the considerations of **necessity** and **proportionality**:

"When will acquisition be "necessary"?

4.3 What is ***necessary*** *in a particular case is ultimately a question of fact and judgement, taking all the relevant circumstances into account. In order to meet the '****necessity****' requirement in relation to acquisition and retention, staff must consider why obtaining the bulk personal dataset is 'really needed' for the purpose of discharging a statutory function of the relevant Intelligence Service. In practice this means identifying the intelligence aim which is likely to be met and giving careful consideration as to how the data could be used to support achievement of that aim.*

The obtaining must also be "proportionate"

4.4 The obtaining and retention of the bulk personal dataset must also be ***proportionate*** *to the purpose in question. In order to meet the '**proportionality**' requirement, staff must balance (a) the level of interference with the individual's right to privacy, both in relation to subjects of interest who are included in the relevant data and in relation to other individuals who are included in the data and who may be of no intelligence interest, against (b) the expected value of the intelligence to be derived from the data. Staff must be satisfied that the level of interference with the individual's right to privacy is justified by the value of the intelligence that is sought to be derived from the data and the importance of the objective to be achieved. Staff must also consider whether there is a reasonable alternative that will still meet the proposed objective - i.e. which involves less intrusion.*

4.5 These can be difficult and finely balanced questions of judgement. In difficult cases staff should consult line or senior management and/or legal advisers for guidance, and may seek guidance or a decision from the relevant Secretary of State."

69. A formal procedure must be followed prior to any acquisition or use as set out at §§4.6 to 4.7:

"4.6 Before a new dataset is loaded into an analytical system for use, staff in each Intelligence Service must consider the factors set out in paragraph 4.2 based on the information available to it at the time. Each Agency has a rigorous formal internal authorisation procedure which must be complied with, except in those cases where the acquisition is already authorised by a warrant or other legal authorisation issued by a Secretary of State.

4.7 Staff in each Intelligence Service must always complete the formal internal authorisation procedure before the dataset is loaded into an analytical system for use. The authorisation procedure involves an application to a senior manager designated for the purpose which is required to set out the following:

- *a description of the requested dataset, including details of the personal data requested, and any sensitive personal data;*
- *the operational and legal justification for acquisition and retention, including the purpose for which the dataset is required and the necessity and proportionality of the acquisition;*
- *an assessment of the level of intrusion into privacy;*
- *the extent of political, corporate, or reputational risk;"*

70. Thus, the need to consider the key matters set out at §4.2 of the BPD Handling Arrangements, and explained at §§4.3-4.3, is built into the formal authorisation procedure.

71. There is a requirement to consult the legal advisers of the relevant Intelligence Service *"on all new BPD acquisitions"* and to have *"confirmed the legality of the acquisition and its continued retention before authorisation to use the*

dataset is given." (§4.8)

72. A record of the application for authorisation must be kept:

> *"4.9 Once authorised, the completed application must be stored on a central record by the appropriate Intelligence Service's information governance/compliance team, which will include the date of approval. This record must also contain the date of acquisition of the relevant data, which should be the date used for the review process (for which see paragraph 7.1-7.5 below)."*

73. Thus the reasons why the acquisition was authorised, including the key considerations set out at §4.2, are available to be reviewed or audited in the future.

Use and Access

74. The BPD Handling Arrangements emphasise the high priority that is put on data security and protective security standards, on confidentiality of data, and on preventing/disciplining misuse of such data:

> *"5.1 Each Intelligence Service attaches the highest priority to maintaining data security and protective security standards. Moreover, each Intelligence Service must establish handling procedures so as to ensure that the integrity and confidentiality of the information in the bulk personal dataset held is fully protected, and that there are adequate safeguards in place to minimise the risk of any misuse of such data and, in the event that such misuse occurs, to ensure that appropriate disciplinary action is taken. In particular, each Intelligence Service must apply the following protective security measures:*
>
> - *Physical security to protect any premises where the information may be accessed;*
> - *IT security to minimise the risk of unauthorised access to IT systems;*
> - *A security vetting regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy."*

75. Specific, detailed measures are also set out which are designed to limit access to data to what is necessary and proportionate, to ensure that such access is properly audited, and to ensure that disciplinary measures are in place for misuse:

> *"5.2 In relation to information in bulk personal datasets held, each Intelligence Service is obliged to put in place the following additional measures:*
>
> - *Access to the information contained within the bulk personal datasets must be strictly limited to those with an appropriate business requirement to use these data;*

- *Individuals must only access information within a bulk personal dataset if it is necessary for the performance of one of the statutory functions of the relevant Intelligence Service;*
- *If individuals access information within a bulk personal dataset with a view to subsequent disclosure of that information, they must only access the relevant information if such disclosure is necessary for the performance of the statutory functions of the relevant Intelligence Service, or for the additional limited purposes described in paragraph 3.1.4 above;*
- *Before accessing or disclosing information, individuals must also consider whether doing so would be proportionate (as described in paragraphs 4.4 above and 6.3 below). For instance, they must consider whether other, less intrusive methods can be used to achieve the desired outcome;*
- *Users must be trained on their professional and legal responsibilities, and refresher training and/or updated guidance must be provided when systems or policies are updated;*
- *A range of audit functions must be put in place: users should be made aware that their access to bulk personal datasets will be monitored and that they must always be able to justify their activity on the systems;*
- *Appropriate disciplinary action will be taken in the event of inappropriate behaviour being identified; and*
- *Users must be warned, through the use of internal procedures and guidance, about the consequences of any unjustified access to data, which can include dismissal and prosecution."*

76. In addition, Intelligences Services are required to take specific measures *"to reduce the level of interference with privacy arising from the acquisition and use of bulk personal datasets"* (§5.3). Specifically:

"5.3 The Intelligence Services also take the following measures to reduce the level of interference with privacy arising from the acquisition and use of bulk personal datasets:

- *Data containing sensitive personal data (as defined in section 2 of the DPA) may be subject to further restrictions, including sensitive data fields not being acquired, sensitive fields being acquired but suppressed or deleted, or additional justification required to access sensitive data fields. In addition, the Intelligence Services may expand the list of sensitive data fields beyond those provided for in section 2 of the DPA to provide additional protection where appropriate.*

- *Working practice seeks to minimise the number of results which are presented to analysts by framing queries in a proportionate way, although this varies in practice depending on the nature of the analytical query;*

- *If necessary, the Intelligence Services can - and will - limit access to specific data to a very limited number of analysts."*

<u>*Disclosure*</u>

77. The disclosure of BPD outside the Intelligence Service which holds it can only occur if certain conditions are complied with:

"6.1 Information in bulk personal datasets held by an Intelligence Service may only be disclosed to persons outside the relevant Service if the following conditions are met:

- *that the objective of the disclosure falls within the Service's statutory functions or is for the additional limited purposes set out in sections 2(2)(a) and 4(2)(a) of the ISA 1994 and section 2(2)(a) of the SSA 1989;*
- *that it is **necessary** to disclose the information in question in order to achieve that objective;*
- *that the disclosure is **proportionate** to the objective;*
- *that only as much of the information will be disclosed as is **necessary** to achieve that objective."*

78. Again, guidance is given to staff on the requirements of **necessity** and **proportionality**. This is in terms which are similar to those set out at §§4.3-4.4 in relation to acquisition, but with particular reference to disclosure:

*"**When will disclosure be necessary?***

*6.2 In order to meet the '**necessity**' requirement in relation to disclosure, staff must be satisfied that disclosure of the bulk personal dataset is 'really needed' for the purpose of discharging a statutory function of that Intelligence Service.*

The disclosure must also be "proportionate"

*6.3 The disclosure of the bulk personal dataset must also be **proportionate** to the purpose in question. In order to meet the 'proportionality' requirement, staff must be satisfied that the level of interference with the individual's right to privacy is justified by the benefit to the discharge of the Intelligence Service's statutory functions which is expected as a result of disclosing the data and the importance of the objective to be achieved. Staff must consider whether there is a reasonable alternative that will still meet the proposed objective - i.e. which involves less intrusion. For example, this could mean disclosure of individual pieces of data or of a subset of data rather than of the whole bulk personal dataset."*

79. Prior to any disclosure of BPD, staff must also take reasonable steps to ensure the intended recipient organisation *"has and will maintain satisfactory arrangements for safeguarding the confidentiality of the data and ensuring that it is securely handled"* or have received satisfactory assurances from the intended recipient with respect to such arrangements (§6.4). This applies to all disclosure, including to other Agencies (§6.5), and whether disclosure is of an entire BPD, a subset of a BPD or an individual piece of data from a BPD (§6.6).

80. Disclosure of the whole or subset of a BPD is subject to internal authorisation procedures in addition to those that apply to an item of data (§6.7):

"The authorisation process requires an application to a senior manager designated for the purpose, describing the dataset it is proposed to disclose (in whole or in part) and

setting out the operational and legal justification for the proposed disclosure along with the other information specified in paragraph 4.7, and whether any caveats or restrictions should be applied to the proposed disclosure. This is so that the senior manager can then consider the factors in paragraph 6.1, with operational, legal and policy advice taken as appropriate. In difficult cases, the relevant Intelligence Service may seek guidance or a decision from the Secretary of State."

Review of Retention and Deletion

81. The Intelligence Services are each required to keep the justification for continued retention and use of BPD under review, as set out at §§7.1-7.2:

"7.1 Each Intelligence Service must regularly review the operational and legal justification for its ***continued retention and use*** *of each bulk personal dataset. Where the continued retention of any such data no longer meets the tests of necessity and proportionality, all copies of it held within the relevant Intelligence Service must be deleted or destroyed.*

7.2 The retention and review process requires consideration of the following factors:

- *The operational and legal justification for continued retention, including its necessity and proportionality;*
- *Whether such information could be obtained elsewhere through less intrusive means;*
- *An assessment of the value and examples of use;*
- *Frequency of acquisition;*
- *The level of intrusion into privacy;*
- *The extent of political, corporate, or reputational risk;*
- *Whether any caveats or restrictions should be applied to continued retention."*

82. Thus, the justification for the retention of BPD, including whether it remains necessary and proportionate, the level of intrusion into privacy, and whether such information could be obtained elsewhere less intrusively, is not simply considered at the stages of acquisition, use or disclosure, but is kept under continuing review.

Other management controls

83. §§8.1-8.2 set out the requirement for each Agency to have an internal Review panel which scrutinises the acquisition, disclosure and retention of BPD:

"8.1 The acquisition, retention and disclosure of a bulk personal dataset is subject to scrutiny in each Intelligence Service by an internal Review Panel, whose function is to ensure that each bulk personal dataset has been properly acquired, that any disclosure is properly justified, that its retention remains necessary for the proper discharge of the relevant Service's statutory functions, and is proportionate to achieving that objective.

8.2 The Review Panel in each Intelligence Service meets at six-monthly intervals and are comprised of senior representatives from Information Governance/Compliance, Operational and Legal teams."

84. In addition, use of BPD is monitored by an audit team within each Agency:

"8.3 Use of bulk personal data by staff is monitored by the relevant audit team in each Intelligence Service in order to detect misuse or identify activity that may give rise to security concerns. Any such identified activity initiates a formal investigation process in which legal, policy and HR (Human Resources) input will be requested where appropriate. Failure to provide a valid justification for a search may result in disciplinary action, which in the most serious cases could lead to dismissal and/or the possibility of prosecution."

85. §8.4 notes that all reports on audit investigations are made available to the Intelligence Services Commissioner for scrutiny.

86. Staff within each Agency are also required to keep their senior leadership *"apprised as appropriate of the relevant Service's bulk personal data holdings and operations."* (§8.5)

<u>*Oversight*</u>

87. The BPD Handling Arrangements also set out provisions in relation to the oversight of BPD.

88. §9.1 concerns Ministerial oversight. Each of the Intelligence Services must report as appropriate on its BPD holdings and operations to the relevant Secretary of State.

89. §§10.1 to 10.4 address oversight by the Intelligence Services Commissioner:

"10.1 The acquisition, use, retention and disclosure of bulk personal datasets by the Intelligence Services, and the management controls and safeguards against misuse they put in place, will be overseen by the Intelligence Services Commissioner on a regular six-monthly basis, or as may be otherwise agreed between the Commissioner and the relevant Intelligence Service, except where the oversight of such data already falls within the statutory remit of the Interception of Communications Commissioner.

***<u>Note</u>**: The Prime Minister's section 59A RIPA direction was issued on 11 March 2015. Paragraph 3 of this makes it clear that the Commissioner's oversight extends not only to the practical operation of the Arrangements, but also to the adequacy of the Arrangements themselves.*

10.2 The Intelligence Services must ensure that they can demonstrate to the appropriate Commissioner that proper judgements have been made on the necessity and proportionality of acquisition, use, disclosure and retention of bulk personal datasets. In particular, the Intelligence Services should ensure that they can establish to the satisfaction of the appropriate Commissioner that their policies and procedures in this area (a) are sound and provide adequate safeguards against misuse and (b) are strictly complied with, including through the operation of adequate protective monitoring arrangements.

10.3 The Intelligence Services Commissioner also has oversight of controls to prevent and detect misuse of bulk personal data, as outlined in paragraph 8.3 and 8.4 above.

10.4 The Intelligence Services must provide to the appropriate Commissioner all such documents and information as the latter may require for the purpose of enabling him to exercise the oversight described in paragraph 10.1 and 10.2 above."

Section 94 Handling Arrangements

90. The Section 94 Handling Arrangements apply to the acquisition, use and disclosure of bulk communications data under section 94 of the Telecommunications Act 1984. As already noted (at §60 above) they are mandatory and required to be followed by staff in the Intelligence Services. Failure to comply may lead to disciplinary action, which can include dismissal and prosecution (§§1.1-1.3).

91. The Section 94 Handling Arrangements expressly relate to communications data which is limited to "traffic data" and "service use information" (§2.2). These terms are defined at §3.5.1 and §3.5.2 by reference to s.21(4) and (6) of RIPA:

*"3.5.1 **Section 21(4)** of **RIPA** defines 'communications data' as meaning any of the following:*

- ***Traffic Data** – this is data that is or has been comprised in or attached to a communication for the purpose of its transmission [section 21(4)(a)];*
- ***Service Use Information** – this is the data relating to the use made by a person of a communications service [section 21(4)(b)];*

..."

*3.5.2 **Section 21(6)** defines 'traffic data' for these purposes, in relation to any communication, as meaning:*

- *any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted;*
- *any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted;*
- *any data comprising signals for the actuation of apparatus used for the purposes of a telecommunications system for effecting (in whole or in part) the transmission of any communication; and*
- *any data identifying the data or other data as data comprised in or attached to a particular communication, but that expression includes data identifying a computer file or computer program access to which is obtained, or which is*

run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored."

92. The data provided does not contain communication content or Subscriber Information or Internet Connection Records (§2.3). Subscriber Information is defined at §3.5.1:

*"**Subscriber Information** – this relates to information held or obtained by a communications service provider about persons to whom the communications service provider provides or has provided communications services [section 21(4)(c)]."*

93. §2.4 sets out the requirements contained in section 94 itself that the Secretary of State must be satisfied that a Section 94 direction is **necessary** and **proportionate**:

"2.4 Any section 94 Directions under which this communications data is acquired requires the relevant Secretary of State to be satisfied that acquisition is necessary in the interests of national security or international relations and that the level of interference with privacy involved in doing so is proportionate to what it seeks to achieve."

94. The requirement that acquisition, use, retention and disclosure of BCD have *"clear justification, accompanied by detailed and comprehensive safeguards against misuse"* and be *"subject to rigorous oversight"* is made clear (§4.0.1). The Section 94 Handling Arrangements are intended to provide such safeguards (§4.0.2).

95. The Section 94 Handling Arrangements set out provisions in respect of each of the stages of the lifecycle of BCD.

Authorisation

96. §§4.1.1-4.1.2 sets out the key considerations which must be presented to the Secretary of State when he/she considers whether to make a Section 94 Direction. These include the family considerations of necessity and proportionality, including whether a less intrusive method of obtaining the information is available, and the level of collateral intrusion involved:

"4.1.1 Where the head of the relevant Intelligence Service has decided to request a Section 94 Direction from the relevant Secretary of State, it is essential that a submission is then presented to the Secretary of State by the Home Office/Foreign Office in order to enable them to consider:

- *whether acquisition and retention of the BCD to be authorised by the Direction is necessary in the interests of national security or international relations;*
- *whether the acquisition and retention of the BCD would be proportionate to what is sought to be achieved;*
- *whether there is a less intrusive method of obtaining the BCD or achieving the national security objective;*

- *the level of collateral intrusion caused by acquiring and utilising the requested BCD.*

4.1.2 The submission must also outline any national security or international relations argument as to why the Secretary of State cannot lay the Direction before each House of Parliament in accordance with 94(4) of the Act."

97. Clear guidance is provided to staff on the considerations of **necessity** and **proportionality**:

"When will acquisition be "necessary"?

*4.1.3 What is **necessary** in a particular case is ultimately a question of fact and judgement, taking all the relevant circumstances into account. In order to meet the '**necessity**' requirement in relation to acquisition and retention, before presenting the submission referred to in paragraph 4.1.1 above, staff in the relevant Intelligence Service must consider why obtaining the BCD in question is 'really needed' for the purpose of discharging a statutory function of that Intelligence Service. In practice this means identifying the intelligence aim which is likely to be met and giving careful consideration as to how the data could be used to support achievement of that aim.*

The obtaining must also be "proportionate"

*4.1.4 The obtaining and retention of the bulk communications dataset must also be **proportionate** to the purpose in question. In order to meet the '**proportionality**' requirement, before presenting the submission referred to in paragraph 4.1.1 above, staff in the relevant Intelligence Service must balance (a) the level of interference with the right to privacy of individuals whose communications data is being obtained (albeit that at the point of initial acquisition of the BCD the identity of the individuals will be unknown), both in relation to subjects of intelligence interest and in relation to other individuals who may be of no intelligence interest, against (b) the expected value of the intelligence to be derived from the data. Staff must be satisfied that the level of interference with the individual's right to privacy is justified by the value of the intelligence that is sought to be derived from the data and the importance of the objective to be achieved. Staff must also consider whether there is a reasonable alternative that will still meet the proposed objective - i.e. which involves less intrusion."*

<u>Acquisition</u>

98. Once made, a Section 94 Direction must be served on the CNP concerned in order that the relevant Agency can receive the requested dataset (§4.2.1).

99. Safeguards against unauthorised access are set out at §4.2.2:

"4.2.2 It is essential that any BCD is acquired in a safe and secure manner and that Intelligence Services safeguard against unauthorised access. Intelligence Services <u>must</u> therefore adhere to the controls outlined in the CESG[12] Good Practice Guide for transferring and storage of data electronically or physically."

[12] UK Government's National Technical Authority for Information Assurance.

Use and Access

100. The Section 94 Handling Arrangements emphasise the importance of data security and protective security standards, confidentiality of data and preventing/disciplining misuse of such data:

"4.3.1 Each Intelligence Service must attach the highest priority to maintaining data security and protective security standards. Moreover, each Intelligence Service must establish handling procedures so as to ensure that the integrity and confidentiality of the information in BCD held is fully protected, and that there are adequate safeguards in place to minimise the risk of any misuse of such data and, in the event that such misuse occurs, to ensure that appropriate disciplinary action is taken."

101. As with BPD, specific, detailed measures are also set out which are designed to limit access to data to what is necessary and proportionate, to ensure that such access is properly audited, and to ensure that disciplinary measures are in place for misuse:

"4.3.2 In particular, each Intelligence Service must apply the following protective security measures:

- *Physical security to protect any premises where the information may be accessed;*
- *IT security to minimise the risk of unauthorised access to IT systems;*
- *A security vetting regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy.*

4.3.3 Furthermore, each Intelligence Service is obliged to put in place the following additional measures:

- *Access to BCD must be strictly limited to those with an appropriate business requirement to use these data and managed by a strict authorisation process;*
- *Requests to access BCD must be justified on the grounds of* ***necessity*** *and* ***proportionality*** *and must demonstrate consideration of collateral intrusion and the use of any other less intrusive means of achieving the desired intelligence dividend.*
- *Intelligence Service staff who apply to access BCD must have regard to the further guidance on the application of the* ***necessity*** *and* ***proportionality*** *tests set out in paragraph 4.1.3 - 4.1.4 above.*
- *Where Intelligence Service staff intend to access BCD relating to the communications of an individual known to be a member of a profession that handles privileged information or information that is otherwise confidential (medical doctors, lawyers, journalists, Members of Parliament, Ministers of religion), they must give* ***special consideration*** *to the necessity and proportionality justification for the interference with privacy that will be involved;*

- *In addition, Intelligence Service staff must take particular care when deciding whether to seek access to BCD and must consider whether there might be unintended consequences of such access to BCD and whether the public interest is best served by seeking such access;*
- *In all cases where Intelligence Service staff intentionally seek to access and retain BCD relating to the communications of individuals known to be members of the professions referred to above, they must record the fact that such communications data has been accessed and retained and must flag this to the Interception of Communications Commissioner at the next inspection;*
- *In the exceptional event that Intelligence Service staff were to seek access to BCD specifically in order to determine a journalist's source, they should only do this if the proposal had been approved beforehand at Director level. Any communications data obtained and retained as a result of such access must be reported to the Interception of Communications Commissioner at the next inspection;*
- *Users must be trained on their professional and legal responsibilities, and refresher training and/or updated guidance must be provided when systems or policies are updated;*
- *A range of audit functions must be put in place: users should be made aware that their access to BCD will be monitored and that they must always be able to justify their activity on the systems;*
- *Appropriate disciplinary action will be taken in the event of inappropriate behaviour being identified;*
- *Users must be warned, through the use of internal procedures and guidance, about the consequences of any unjustified access to data, which can include dismissal and prosecution.*
- *In the exceptional event that Intelligence Service staff were to abuse their access to BCD – for example, by seeking to access the communications data of an individual without a valid business need – the relevant Intelligence Service must report the incident to the Interception of Communications Commissioner at the next inspection."*

<u>Disclosure</u>

102. The disclosure of BCD outside the Agency which holds can only occur if certain conditions are complied with:

"4.4.1 The disclosure of BCD must be carefully managed to ensure that it only takes place when it is justified on the basis of the relevant statutory disclosure gateway. The disclosure of an entire bulk communications dataset, or a subset, outside the Intelligence Service may only be authorised by a Senior Official[13] or the Secretary of State.

4.4.2 Disclosure of individual items of BCD outside the relevant Intelligence Service may only be made if the following conditions are met:

[13] Equivalent to a member of the Senior Civil Service.

- *that the objective of the disclosure falls within the Service's statutory functions or is for the additional limited purposes set out in sections 2(2)(a) and 4(2)(a) of the ISA 1994 and section 2(2)(a) of the SSA 1989;*
- *that it is **necessary** to disclose the information in question in order to achieve that objective;*
- *that the disclosure is **proportionate** to the objective;*
- *that only as much of the information will be disclosed as is **necessary** to achieve that objective."*

103. Again, guidance is given to staff on the requirements of **necessity** and **proportionality**, in terms similar to those relating to acquisition, but with specific reference to disclosure:

*"**When will disclosure be necessary?***

*4.4.3 In order to meet the '**necessity**' requirement in relation to disclosure, staff in the relevant Intelligence Service and (as the case may be) the Secretary of State must be satisfied that disclosure of the BCD is 'really needed' for the purpose of discharging a statutory function of that Intelligence Service.*

The disclosure must also be "proportionate"

*4.4.4 The disclosure of the BCD must also be **proportionate** to the purpose in question. In order to meet the 'proportionality' requirement, staff in the relevant Intelligence Service and (as the case may be) the Secretary of State must be satisfied that the level of interference with the right to privacy of individuals whose communications data is being disclosed, both in relation to subjects of intelligence interest and in relation to other individuals who may be of no intelligence interest, is justified by the benefit to the discharge of the Intelligence Service's statutory functions which is expected as a result of disclosing the data and the importance of the objective to be achieved. Staff must consider whether there is a reasonable alternative that will still meet the proposed objective - i.e. which involves less intrusion. For example, this could mean disclosure of individual pieces of communications data or of a subset of the bulk communications data rather than of the whole bulk communications dataset."*

104. Prior to any disclosure of BCD, staff must also take reasonable steps to ensure the intended recipient organisation *"has and will maintain satisfactory arrangements for safeguarding the confidentiality of the data and ensuring that it is securely handled"* or have received satisfactory assurances from the intended recipient with respect to such arrangements (§4.4.5). This applies to all disclosure, including to other Agencies (§4.4.6), and whether disclosure is of an entire BCD, a subset of a BCD or an individual piece of data from a BCD (§4.4.6).

105. Disclosure of the whole or subset of a BCD may only be authorised by a Senior Official (equivalent to a member of the Senior Civil Service) or the Secretary of State (§4.4.1).

Review of Retention and Deletion

106. The requirement on each of the Intelligence Services to review the justification for continued retention and use of BCD is set out at §§4.5.1-4.5.2:

"4.5.1 Each Intelligence Service must regularly review, i.e. at intervals of no less than six months, the operational and legal justification for its continued retention and use of BCD. This should be managed through a review panel comprised of senior representatives from Information Governance/Compliance, Operational and Legal teams.

4.5.2 The retention and review process requires consideration of:

- *An assessment of the value and use of the dataset during the period under review and in a historical context;*
- *the operational and legal justification for ongoing acquisition, continued retention, including its necessity and proportionality;*
- *The extent of use and specific examples to illustrate the benefits;*
- *The level of actual and collateral intrusion posed by retention and exploitation;*
- *The extent of corporate, legal, reputational or political risk;*
- *Whether such information could be acquired elsewhere through less intrusive means.*

4.5.3 Should the review process find that there remains an ongoing case for acquiring and retaining BCD, a formal review will be submitted at intervals of no less than six months for consideration by the relevant Secretary of State. In the event that the Intelligence Service or Secretary of State no longer deem it to be necessary and proportionate to acquire and retain the BCD, the Secretary of State will cancel the relevant Section 94 Direction and instruct the CNP concerned to cease supply. The relevant Intelligence Service must then task the technical team[s] responsible for Retention and Deletion with a view to ensuring that any retained data is destroyed and notify the Interception of Communications Commissioner accordingly. Confirmation of completed deletion must be recorded with the relevant Information Governance/Compliance team."

Oversight

107. The Section 94 Handling Arrangements also set out provisions in relation to internal and external oversight.

108. §§4.6.1-4.6.2 concern internal oversight. A senior member of an Intelligence Service's internal review panel (see §106 above) must keep that Service's Executive Board apprised of BCD holdings (§4.6.1). In addition internal audit teams must monitor use of IT systems:

"4.6.2 Use of IT systems is monitored by the audit team in order to detect misuse or identify activity that may give rise to security concerns. Any such identified activity initiates a formal investigation process in which legal, policy and HR (Human Resources) input will be requested where appropriate. Disciplinary action may be taken, which in the most serious cases could lead to dismissal and/or the possibility of

prosecution under the Computer Misuse Act 1990, the Data Protection Act 1998, the Official Secrets Act 1989 and Misfeasance in Public Office depending on circumstances."

109. All reports on audit investigations are made available to the Interception of Communications Commissioner (§4.6.3).

110. §§4.6.4 to 4.6.7 address oversight by the Interception of Communications Commissioner:

"4.6.4 The ***Interception of Communications Commissioner*** *has oversight of:*

a) the issue of Section 94 Directions by the Secretary of State enabling the Intelligence Services to acquire BCD;

b) the Intelligence Services' arrangements in respect of acquisition, storage, access, disclosure, retention and destruction; and

c) the management controls and safeguards against misuse which the Intelligence Services have put in place.

4.6.5 This oversight is exercised by the Interception of Communications Commissioner on at least an annual basis, or as may be otherwise agreed between the Commissioner and the relevant Intelligence Service.

4.6.6 The purpose of this oversight is to review and test judgements made by the Secretary of State and the Intelligence Services on the necessity and proportionality of the Section 94 Directions and on the Intelligence Services' acquisition and use of BCD, and to ensure that the Intelligence Services' policies and procedures for the control of, and access to BCD are (a) are sound and provide adequate safeguards against misuse and (b) are strictly observed.

4.6.7 The Interception of Communications Commissioner also has oversight of controls to prevent and detect misuse of data acquired under Section 94, as outlined in paragraph 4.6.2 and 4.6.3 above."

111. The Secretary of State and the Intelligence Services must provide the Interception of Communications Commissioner with *"all such documents and information as he may require for the purpose of enabling him to exercise the oversight described…"* (§4.6.8)

Oversight mechanisms

112. There are three principal oversight mechanisms in respect of Bulk Personal Datasets and section 94 of the Telecommunications Act 1984:

(a) The Intelligence Services Commissioner and Interception of Communications Commissioner;

(b) The ISC; and

(c) The Tribunal.

The Intelligence Services Commissioner

113. The Prime Minister is under a duty to appoint an Intelligence Services Commissioner (see s. 59(1) of RIPA). By s. 59(5), the person so appointed must hold or have held high judicial office, so as to ensure that he is appropriately independent from the Government. The Commissioner is currently Sir Mark Waller.

114. The Intelligence Services Commissioner's remit under s.59(2) of RIPA is to provide independent oversight of the use of the powers contained within ss. 5 and 7 of ISA and Parts II and III of RIPA.

115. On 11 March 2015 the Prime Minister issued the Intelligence Services Commissioner (Additional Review Functions) (Bulk Personal Datasets) Direction 2015 ("the Direction") pursuant to section 59A of RIPA. This was sent to the Intelligence Services Commissioner on 12 March 2015 and came into force on 13 March 2015.

116. Paragraph 5 of the Direction defines *"bulk personal dataset"* as meaning:

> *"any collection of information which:*
>
> > *a. Comprises personal data as defined by section 1(1) of the Data Protection Act 1998;*
> >
> > *b. Relates to a wide range of individuals, the majority of whom are unlikely to be of intelligence interest;*
> >
> > *c. Is held, or acquired for the purpose of holding, on one or more analytical systems within the Security and Intelligence Services."*

117. By paragraph 3 of the Direction, the Intelligence Services Commissioner is required to *"continue to keep under review the acquisition, use, retention and disclosure"* by the Intelligence Services of bulk personal datasets, *"as well as the adequacy of safeguards against misuse"*.

118. Paragraph 4 of the Direction provides that the Intelligence Services Commissioner must specifically *"seek to assure himself that the acquisition, use, retention and disclosure of bulk personal datasets does not occur except in accordance with section 2(2)(a) of the Security Service Act 1989, sections 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994"*. Paragraph 4 requires that, as part of this, the Intelligence Services Commissioner must also *"seek to assure himself of the adequacy of the* [Respondents'] *handling arrangements and their compliance therewith."*

119. Prior to the Direction being issued, the Intelligence Service Commissioner had overseen the acquisition, use, retention and disclosure of BPD on a non-statutory basis. This was acknowledged in paragraph 3 of the Direction (*"shall*

continue to keep under review…").

120. Under s. 59(7) of RIPA, the Intelligence Services Commissioner must be provided with such staff as are sufficient to ensure that he can properly carry out his functions.

121. A duty is imposed on, among other persons, every person holding office under the Crown to disclose and provide to the Intelligence Services Commissioner all such documents and information as he may require for the purpose of enabling him to carry out his functions: s. 60(1) of RIPA.

122. In practice, the Intelligence Services Commissioner visits each of the Intelligence Services and the main Departments of State twice a year. Written reports and recommendations are produced after his inspections of the Intelligence Services. The Intelligence Services Commissioner also meets with the relevant Secretaries of State. In addition to the formal inspections, there is also regular engagement between the Intelligence Services Commissioner (and his office) and the Intelligence Services and relevant Departments of State on, for example, responding to Commissioner-led investigations or consulting on new guidance, draft legislation or any novel or contentious issue that would benefit from a view from the Commissioner.

123. S. 60 of RIPA imposes important reporting duties on the Intelligence Services Commissioner. (It is an indication of the importance attached to this aspect of the Intelligence Services Commissioner's functions that reports are made to the Prime Minister.)

124. The Intelligence Services Commissioner is by s. 60(2) of RIPA under a duty to make an annual report to the Prime Minister regarding the carrying out of his functions. He may also, at any time, make any such other report to the Prime Minister as he sees fit (s. 60(3)). Pursuant to s. 60(4), a copy of each annual report (redacted, where necessary under s.60(5)), must be laid before each House of Parliament. In this way, the Intelligence Services Commissioner's oversight functions help to facilitate Parliamentary oversight of the activities of the Intelligence Services (including by the ISC). The Intelligence Services Commissioner's practice is to make annual reports in open form, with a closed confidential annex for the benefit of the Prime Minister going into detail on any matters which cannot be discussed openly.

125. In addition, the Intelligence Services Commissioner is required by s. 59(3) to give the Tribunal:

> "*…such assistance (including his opinion as to any issue falling to be determined by the Tribunal) as the Tribunal may require-*
> *(a) in connection with the investigation of any matter by the Tribunal; or*
> *(b) otherwise for the purposes of the Tribunal's consideration or determination of any matter.*"

126. The Tribunal is also under a duty to ensure that the Intelligence Services Commissioner is apprised of any relevant claims / complaints that come before it: s. 68(3).

127. It is to be noted that in the IPT judgment in the recent Liberty/Privacy proceedings, [2014] UKIPTrib 13_77-H dated 5 December 2014 (referred to in this Response as "the Liberty/Privacy IPT judgment") the Tribunal placed considerable emphasis on the important oversight which is provided by the Interception Commissioner (see in particular §§24, 44, 91, 92 121 and 139 of the judgment) and a similarly important role is provided by the Intelligence Services Commissioner in the present context.

The Interception of Communications Commissioner

128. The Prime Minister must also appoint an Interception of Communications Commissioner (see s. 57(1) of RIPA). The statutory provisions in relation to the Interception of Communications Commissioner (hereafter referred to as "the Interception Commissioner") largely mirror those in respect of the Intelligence Services Commissioner, but are summarised below for the sake of convenience and because they differ in some respects from those relating to the Intelligence Services Commissioner.

129. By s. 57(5), the person appointed as Interception Commissioner must hold or have held high judicial office, so as to ensure that he is appropriately independent from the Government. The Interception Commissioner is Sir Stanley Burnton.

130. The Interception Commissioner's remit under s.59(2) of RIPA is to provide independent oversight of the use of the powers contained within Part I of RIPA. He also has non-statutory oversight over the issue of directions pursuant to section 94 of the Telecommunications Act 1984.

131. Under s. 57(7) of RIPA, the Secretary of State must, after consultation with the Interception Commissioner, provide the Commissioner with such technical facilities available and staff as are sufficient to secure that the Commissioner can properly carry out his functions.

132. A duty is imposed on, among other persons, every person holding office under the Crown to disclose and provide to the Interception Commissioner all such documents and information as he may require for the purpose of enabling him to carry out his functions: s. 58(1) of RIPA.

133. In practice, the Interception Commissioner visits each of the Intelligence Services and the main Departments of State twice a year. Written reports and recommendations are produced after his inspections of the Intelligence Services. The Interception Commissioner also meets with the relevant Secretaries of State. As with the Intelligence Services Commissioner, in addition to the formal inspections there is also regular engagement between the Interception Commissioner (and his office) and the Intelligence Services and relevant Departments of State: see §122 above.

134. S. 58 of RIPA imposes important reporting duties on the Interception Commissioner. Again, as with the Intelligence Services Commissioner's reports, reports are made to the Prime Minister.

135. The Interception Commissioner is by s. 58(2) of RIPA under a duty to make an annual report to the Prime Minister regarding the carrying out of his functions. He must also make a report to the Prime Minister of any contravention of the provisions of RIPA in relation to any matter with which he is concerned, if it has not been the subject of a report made to the Prime Minister by the Tribunal (s. 58(2)) or if arrangements made under, inter alia, s.15 of RIPA (in relation to the use of intercept material and related communications data) have proved inadequate in respect of a matter with which he is concerned (s.58(3)). He may also, at any time, make any such other report to the Prime Minister as he sees fit (s. 58(5)(3)). Pursuant to s. 58(6), a copy of each annual and half-yearly report (redacted, where necessary under s.58(7)), must be laid before each House of Parliament. Again as in the case of the Intelligence Services Commissioner, in this way, the Interception Commissioner's oversight functions help to facilitate Parliamentary oversight of the activities of the Intelligence Services (including by the ISC). The Interception Commissioner's practice is to make his reports in open form, with a closed confidential annex for the benefit of the Prime Minister going into detail on any matters which cannot be discussed openly.

136. In addition, the Interception Commissioner is required by s. 57(3) to give the Tribunal:

> *"…such assistance (including his opinion as to any issue falling to be determined by the Tribunal) as the Tribunal may require-*
> *(a) in connection with the investigation of any matter by the Tribunal; or*
> *(b) otherwise for the purposes of the Tribunal's consideration or determination of any matter."*

137. The Tribunal is also under a duty to ensure that the Interception Commissioner is apprised of any relevant claims / complaints that come before it: s. 68(3).

138. The considerable emphasis placed by the Tribunal on the important oversight provided by the Interception Commissioner in the Liberty/Privacy IPT judgment, has already been noted (see in particular §§24, 44, 91, 92 121 and 139 of the judgment).

The ISC

139. The Security Service is responsible to the Home Secretary.[14] GCHQ and SIS are responsible to the Foreign Secretary.[15] The Foreign Secretary and Home Secretary are in turn responsible to Parliament. In addition, the ISC plays an important part in overseeing the activities of the Intelligence Services. In

[14] The Director-General of the Security Service must make an annual report on the work of the Security Service to the Prime Minister and Home Secretary (s. 2(4) of the SSA).
[15] The Director of GCHQ and the Chief of SIS must make annual reports on the work of GCHQ and SIS respectively to the Prime Minister and Foreign Secretary (see s. 4(4) and 2(4) of the ISA).

particular, the ISC is the principal method by which scrutiny by Parliamentarians is brought to bear on those activities.

140. The ISC was established by s. 10 of the ISA. As from 25 June 2013, the statutory framework for the ISC is set out in ss. 1-4 of and Sch. 1 to the Justice and Security Act 2013 ("the JSA").

141. The ISC consists of nine members, drawn from both the House of Commons and the House of Lords. Each member is appointed by the House of Parliament from which the member is to be drawn (they must also have been nominated for membership by the Prime Minister, following consultation with the leader of the opposition). No member can be a Minister of the Crown. The Chair of the ISC is chosen by its members. See s. 1 of the JSA.

142. The executive branch of Government has no power to remove a member of the ISC: a member of the ISC will only vacate office if he ceases to be a member of the relevant House of Parliament, becomes a Minister of the Crown or a resolution for his removal is passed by the relevant House of Parliament. See §1(2) of Sch. 1 to the JSA.

143. The current chair is Dominic Grieve QC MP. He is a former Attorney-General.

144. The ISC may examine the expenditure, administration, policy and operations of each of the Intelligence Services: s. 2(1). Subject to certain limited exceptions, the Government (including each of the Intelligence Services) must make available to the ISC information that it requests in the exercise of its functions. See §§4-5 of Sch. 1 to the JSA. The ISC operates within the "ring of secrecy" which is protected by the OSA. It may therefore consider classified information, and in practice takes oral evidence from the Foreign and Home Secretaries, the Director-General of the Security Service, the Chief of SIS and the Director of GCHQ, and their staff. The ISC meets at least weekly whilst Parliament is sitting. Following the extension to its statutory remit as a result of the JSA, the ISC is further developing its investigative capacity by appointing additional investigators.

145. The ISC must make an annual report to Parliament on the discharge of its functions (s. 3(1) of the JSA), and may make such other reports to Parliament as it considers appropriate (s. 3(2) of the JSA). Such reports must be laid before Parliament (see s. 3(6)). They are as necessary redacted on security grounds (see ss. 3(3)-(5)), although the ISC may report redacted matters to the Prime Minister (s. 3(7)). The Government lays before Parliament any response to the reports that the ISC makes.

146. The ISC sets its own work programme: it may issue reports more frequently than annually and has in practice done so for the purposes of addressing specific issues relating to the work of the Intelligence Services.

147. It is to be noted that in the *Liberty/Privacy* judgment, the Tribunal placed considerable emphasis on the important oversight which is provided by the ISC (see in particular §44 and §121 of the judgment); the Tribunal describing

the ISC as "*robustly independent*" at §121.

The Tribunal

148. The Tribunal was established by s. 65(1) of RIPA. Members of the Tribunal must either hold or have held high judicial office, or be a qualified lawyer of at least 7 years' standing (§1(1) of Sch. 3 to RIPA). The President of the Tribunal must hold or have held high judicial office (§2(2) of Sch. 3 to RIPA).

149. The Tribunal's jurisdiction is broad. As regards the BPD and Section 94 regimes, the following aspects of the Tribunal's jurisdiction are of particular relevance:

(a) The Tribunal has exclusive jurisdiction to consider claims under s. 7(1)(a) of the HRA brought against any of the Intelligence Services or any other person in respect of any conduct, or proposed conduct, by or on behalf of any of the Intelligence Services (ss. 65(2)(a), 65(3)(a) and 65(3)(b) of RIPA).

(b) The Tribunal may consider and determine any complaints by a person who is aggrieved by any conduct by or on behalf of any of the Intelligence Services which he believes to have taken place in relation to him, to any of his property, to any communications sent by or to him, or intended for him, or to his use of any telecommunications service or system (ss. 65(2)(b), 65(4) and 65(5)(a) and (b) of RIPA).

150. Complaints of the latter sort must be investigated and then determined "by applying the same principles as would be applied by a court on an application for judicial review" (s. 67(3)).

151. Thus the Tribunal has jurisdiction to consider any claim against any of the Intelligence Services that it has obtained, used, accessed, retained or disclosed information in breach of the ECHR. Further, the Tribunal can entertain any other public law challenge to any such alleged acts or omissions in relation to information.

152. Any person, regardless of nationality, may bring a claim in the Tribunal. Further, a claimant does not need to be able to adduce cogent evidence that some step has in fact been taken by the Intelligence Services in relation to him before the Tribunal will investigate.[16] As a result, the Tribunal is perhaps one of the most far-reaching systems of judicial oversight over intelligence matters in the world.

153. Pursuant to s. 68(2), the Tribunal has a broad power to require a relevant

[16] The Tribunal may refuse to entertain a claim that is frivolous or vexatious (see s. 67(4)), but in practice it has not done so merely on the basis that the claimant is himself unable to adduce evidence to establish *e.g.* that the Intelligence Services have taken some step in relation to him. There is also a 1 year limitation period (subject to extension where that is "equitable"): see s. 67(5) of RIPA and s. 7(5) of the HRA.

Commissioner (as defined in s. 68(8)) to provide it with assistance. Thus, in the case of a claim of the type identified in §151 above, the Tribunal may require the Intelligence Services Commissioner (see ss. 59-60 of RIPA) and/or the Interception Commissioner (see ss. 57-58 of RIPA) to provide it with assistance.

154. S. 68(6) imposes a broad duty of disclosure to the Tribunal on, among others, every person holding office under the Crown.

155. Subject to any provision in its rules, the Tribunal may - at the conclusion of a claim - make any such award of compensation or other order as it thinks fit, including, but not limited to, an order requiring the destruction of any records of information which are held by any public authority in relation to any person. See s. 67(7).

ISSUES OF PURE LAW SUITABLE FOR DETERMINATION AT A LEGAL ISSUES HEARING

156. It is submitted that the following issues of pure law can be identified from the Grounds advanced by the Claimants:

(a) Issue 1: Does the BPD Regime satisfy the "in accordance with the law" requirement in Art. 8(2)?

(b) Issue 2: Does the Section 94 Regime satisfy the "in accordance with the law" requirement in Art. 8(2)?

(c) Issue 3: Is the Section 94 Regime unlawful as a matter of EU law on the ground that there is no requirement for judicial authorisation prior to accessing data?

157. The remaining ground, namely that "any retention of the Claimant's details on a Bulk Personal Dataset, or using section 94 is not necessary or proportionate." (Grounds, §48) does not give rise to a pure issue of law which is suitable for determination at a Legal Issues Hearing. It turns on factual assertions which are neither confirmed nor denied and which must therefore be investigated and considered by the Tribunal in closed session in the light of such relevant closed evidence, if any, as is filed by the Respondents. The Respondents invite the Tribunal to investigate this ground of claim in closed session after holding a Legal Issues Hearing.

"In accordance with law": the test to be applied

158. The expression "in accordance with the law" requires:

> *"... firstly, that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him, and compatible with the rule of law ..."* (*Weber*, at §84.)

Article 8 ECHR

159. In relation to 'foreseeability' in this context, the essential test, as recognised in §68 of *Malone v. UK* (1984) 7 EHRR 14 and in §37 and §118 of the *Liberty/Privacy* judgment, 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*". As the Grand Chamber confirmed in the eavesdropping case of *Bykov v. Russia*, appl. no. 4378/02, judgment of 21 January 2009, this test remains the guiding principle when determining the foreseeability of intelligence-gathering powers (see §78, as quoted at §37 of the *Liberty/Privacy* judgment).[17]

160. Consequently the key question when considering whether the BPD regime satisfies the "in accordance with the law" test under Art. 8(2) is whether there are:

> "*...adequate arrangements in place to ensure compliance with the statutory framework and the Convention and to give the individual adequate protection against arbitrary interference, which are sufficiently accessible, bearing in mind the requirements of national security and that they are subject to oversight.*" (see §125 of the *Liberty/Privacy* judgment)

161. As noted by the Tribunal in the *Liberty/Privacy* judgment, in the field of national security much less is required to be put into the public domain and therefore the degree of foreseeability must be reduced, because otherwise the whole purpose of the steps taken to protect national security would be put at risk (see §38-40 and §137). That was made very clear by the Strasbourg Court at §§67-68 of *Malone* and in *Leander v Sweden* [1987] 9 EHRR 433 at §51 and *Esbester v UK* [1994] 18 EHRR CD 72, as quoted at §§38-39 of the Tribunal's judgment in *Liberty/Privacy*.

162. Thus, as held by the Tribunal in the *British Irish Rights Watch* case dated 9 December 2004 (a decision which was expressly affirmed in the *Liberty/Privacy* judgment at §87):

> "*foreseeability is only expected to a degree that is reasonable in the circumstances, and the circumstances here are those of national security...*" (§38)

163. Consequently the national security context and the particular national security justification for the activity/conduct which is impugned is highly relevant to any assessment of what is reasonable in terms of the clarity and precision of the law in question and the extent to which the safeguards against abuse must be accessible to the public (see §§119-120 of the

[17]The "necessity" requirement also calls for adequate and effective safeguards against abuse. But the Tribunal is sufficient for this purpose: §59 of *Rotaru v. Romania* (2000) 8 BHRC 449 ("*effective supervision ... should normally be carried out by the judiciary, at least in the last resort, since judicial control affords the best guarantees of independence, impartiality and a proper procedure* ..."). *A fortiori*, the combination of the Tribunal, the ISC and the Commissioner satisfies this aspect of the "necessity" requirement.

Liberty/Privacy judgment)[18].

164. Moreover, the ECtHR has consistently recognised that the foreseeability requirement "*cannot mean that an individual should be enabled to foresee when the authorities are likely to resort to secret measures so that he can adapt his conduct accordingly*": *Malone v. UK* (1984) 7 EHRR14, at §67; *Leander v. Sweden* at §51; and *Weber*, at §93.

165. As to the procedures and safeguards which are applied, two important points should be noted.

166. First it is not necessary for the detailed procedures and conditions which are observed to be incorporated in rules of substantive law. That was made clear at §68 of *Malone* and in *Bykov* at §78 and was reiterated by the Tribunal at §§118-122 of *Liberty/Privacy*.

167. Secondly it is permissible for the Tribunal to consider rules, requirements or arrangements which are "below the waterline" i.e. which are not publicly accessible. In *Liberty/Privacy* the Tribunal came to the clear conclusion that it is "*not necessary that the precise details of all of the safeguards should be published, or contained in legislation, delegated or otherwise*" (§122), in order to satisfy the "in accordance with the law" requirement and that the Tribunal could permissibly consider the "*below the waterline*" rules, requirements or arrangements when assessing the ECHR compatibility of the regime (see §§50, 55, 118, 120 and 139 of the judgment). At §129 of the judgment in Liberty/Privacy the Tribunal stated:

> "*Particularly in the field of national security, undisclosed administrative arrangements, which by definition can be changed by the Executive without reference to Parliament, can be taken into account, provided that what is disclosed indicates the scope of the discretion and the manner of its exercise...This is particularly so where:*
>
> *(i) The Code...itself refers to a number of arrangements not contained in the Code...*
>
> (ii) *There is a system of oversight, which the ECtHR has approved, which ensures that such arrangements are kept under constant review.*"

168. Although these conclusions were reached in the context of the s. 8(4) RIPA interception regime, they are equally applicable to the BPD and Section 94 regimes and where there is similar oversight by the Intelligence Services Commissioner and Interception Commissioner.

169. In terms of oversight mechanisms, it is important to note the extent to which the Tribunal in *Liberty/Privacy* placed reliance on these mechanisms when concluding that the intelligence sharing regime and the s.8(4) RIPA regime were Article 8(2) complaint. Thus the Tribunal highlighted the advantages of

---

[18] See also the recent judgment of the Tribunal in *Lucas and Jones v Security Service* [2015] UKIPTrib 14_79-CH, where the Tribunal referred to "*the well-established proposition as to the reduced* foreseeability *required in the field of national security...*" (at §32).

the Tribunal as an oversight mechanism at §46 and the importance of these oversight mechanisms in the s. 8(4) regime at §122. Therefore, as the ECtHR recognised in §95 of *Weber*, account should be taken of all the relevant circumstances, including:

> *"the authorities competent to ... supervise [the measures in question], and the kind of remedy provided by the national law ..."* (*Association for European Integration and Human Rights v. Bulgaria*, Appl. no. 62540/00, judgment of 28 June 2007, at §77.)

Issue 1: Does the BPD Regime satisfy the "in accordance with the law" requirement in Art. 8(2)?

170. In terms of the criticisms which are made of the legal framework in the Claimant's Grounds, the Respondents make the following points in this response.

171. **First**, contrary to the assertion made in the Grounds, there is a clear legal framework governing any BPD activities, as set out in detail earlier in this Response. The SSA, ISA, CTA and BPD Handling Arrangements do provide a firm legal framework which is supplemented in important respects by the HRA, the DPA and the OSA.

172. The BPD regime is therefore "accessible" and has a basis in domestic law, in that it consists of provisions in primary legislation and in relevant internal arrangements/safeguards which are applied by the Respondents. The Claimant's argument to the contrary is therefore untenable.

173. **Secondly** it is wrong to suggest that there is no "code of practice" governing BPD. As has been set out in detail above at §§61-89, BPD Handling Arrangements have been published, which contain important safeguards including, *inter alia*:

(a) Detailed guidance on the requirements of necessity and proportionality and the considerations which apply in the BPD context, including issues such as collateral intrusion and the need to consider less intrusive alternatives;
(b) Guidance on reviews of the justification for acquisition, use and retention of BPD, and the need for an internal review panel within each Intelligence Service;
(c) Detailed and comprehensive procedures for the authorisation of BPD activity;
(d) Important record keeping requirements in respect of any BPD activity;
(e) Detailed requirements in relation to ensuring data security and protective security standards;
(f) Comprehensive safeguards and guidance as regards the acquisition, use, access, disclosure, review, deletion and destruction of any BPD obtained by the Intelligence Services, and oversight over each of these stages.

174. **Thirdly** it is submitted that the BPD Regime does indicate the scope of any discretion and the manner of its exercise with sufficient clarity "*to give the individual adequate protection against arbitrary interference*" (*Malone*, at §68). The regime is sufficiently clear as regards the circumstances in which BPD can be acquired, used and disclosed. These activities can only be undertaken if clear criteria are satisfied, including the requirements of necessity and proportionality and such permission can only be given by a senior official.

175. Further, if some version of the list of "safeguards" in *e.g.* §95 of *Weber* applies to the BPD Regime, the present regime satisfies the requirements for such "safeguards", insofar as it is feasible to do so.

(a) The first and second requirements in *Weber* i.e. the "offences" which may give rise to BPD activity and the categories of people liable to be involved, are clearly satisfied by the information gateway provisions and the BPD Handling Arrangements. It is also to be noted that the term "*national security*" is a sufficient description (see §116 of the *Liberty/Privacy* judgment).

(b) The third to sixth *Weber* requirements, namely (3) duration, (4), examination, usage and storage, (5) disclosure and (6) destruction are addressed, in particular, in the Handling Arrangements, the CTA, the DPA, the HRA and the OSA.

176. **Fourthly** the Tribunal can take into account the "*below the waterline*" rules, requirements and arrangements which regulate any BCD activities which may be conducted by the Respondents. These are addressed separately in the Respondents' Closed Response to the complaints. Those rules, requirements and arrangements fully support the contentions set out above about the lawfulness of the regime.

177. **Finally** there are important oversight mechanisms which are relevant to the Article 8(2) compatibility of the regime including the Tribunal, the ISC and the Intelligence Services Commissioner. These oversight mechanisms are centrally relevant to the question whether the regime provides for adequate protection against abuse. The combination of these oversight mechanisms is a very important safeguard in the context of the Art 8(2) compatibility of the regime.

178. In conclusion the BPD Regime is sufficiently accessible and "foreseeable" for the purposes of the "in accordance with the law" requirement in Art. 8(2).

179. For the avoidance of doubt the Respondents additionally contend that the BPD Regime satisfied both elements of the "in accordance with law" requirement prior to the date on which the Handling Arrangements came into force. Prior to that BPD was handled in accordance with internal guidance or practice which was similar to the Handling Arrangements, and was sufficiently foreseeable.

Issue 2: Does the Section 94 Regime satisfy the "in accordance with the law" requirement in Art. 8(2)?

180. The Respondents respond as follows to the criticisms which are made of the Section 94 Regime in the Claimant's Grounds.

181. **First**, contrary to the assertion made in the Grounds, as in the case of BPD there is a clear legal framework governing any Section 94 activities, as set out in detail earlier in this Response. The information gateway provisions and Section 94 Handling Arrangements do provide a firm legal framework which is supplemented in important respects by the HRA, the DPA and the OSA.

182. The Section 94 regime is therefore "accessible" and has a basis in domestic law, in that it consists of provisions in primary legislation and in relevant internal arrangements/safeguards which are applied by the Respondents.

183. **Secondly** it is wrong to suggest that there is no "code of practice" governing Section 94 of the Telecommunications Act 1984. As has been set out in detail above at §§90-111, Section 94 Handling Arrangements have been published, which contain important safeguards (which are very similar to those in place in the BPD Regime) including, *inter alia*:

(a) Detailed guidance on the requirements of necessity and proportionality and the considerations which apply in the Section 94 context, including issues such as collateral intrusion and the need to consider less intrusive alternatives;
(b) Guidance on reviews of the justification for acquisition, use and retention of BCD, and the need for an internal review panel within each Intelligence Service;
(c) Detailed and comprehensive procedures for the authorisation of BCD activity;
(d) Important record keeping requirements in respect of any BCD activity;
(e) Detailed requirements in relation to ensuring data security and protective security standards;
(f) Comprehensive safeguards and guidance as regards the acquisition, use, access, disclosure, review, deletion and destruction of any BCD obtained by the Intelligence Services, and oversight over each of these stages.

184. **Thirdly** it is submitted that the Section 94 Regime does indicate the scope of any discretion and the manner of its exercise with sufficient clarity "*to give the individual adequate protection against arbitrary interference*" (*Malone*, at §68). The regime is sufficiently clear as regards the circumstances in which BCD can be acquired, used and disclosed. These activities can only be undertaken if clear criteria are satisfied, including the requirements of necessity and proportionality. A Section 94 Direction can only be issued by a Secretary of State. Disclosure of BCD can only be authorised by a Secretary of State or senior official.

185. Further, if some version of the list of "safeguards" in *e.g.* §95 of *Weber* applies

to the Section 94 Regime, the present regime satisfies the requirements for such "safeguards", insofar as it is feasible to do so.

(a) The first and second requirements in *Weber* i.e. the "offences" which may give rise to Section 94 activity and the categories of people liable to be involved, are clearly satisfied by the statutory information gateway provisions and the Section 94 Handling Arrangements. It is also to be noted that the term "*national security*" is a sufficient description (see §116 of the *Liberty/Privacy* judgment).

(b) The third to sixth *Weber* requirements, namely (3) duration, (4), examination, usage and storage, (5) disclosure and (6) destruction are addressed, in particular, in the Section 94 Handling Arrangements, the DPA, the HRA and the OSA.

186. **Fourthly** the Tribunal can take into account the "*below the waterline*" rules, requirements and arrangements which regulate any Section 94 activities which may be conducted by the Respondents. These are addressed separately in the Respondents' Closed Response to the complaints. Those rules, requirements and arrangements fully support the contentions set out above about the lawfulness of the regime.

187. **Finally** there are important oversight mechanisms which are relevant to the Article 8(2) compatibility of the regime including the Tribunal, the ISC and the Interception of Communications Commissioner. These oversight mechanisms are centrally relevant to the question whether the regime provides for adequate protection against abuse. The combination of these oversight mechanisms is a very important safeguard in the context of the Art 8(2) compatibility of the regime.

188. In conclusion the Section 94 Regime is sufficiently accessible and "foreseeable" for the purposes of the "in accordance with the law" requirement in Art. 8(2).

189. For the avoidance of doubt the Respondents additionally contend that the Section 94 Regime satisfied both elements of the "in accordance with law" requirement prior to the date on which the Section 94 Handling Arrangements came into force. Prior to that BCD was handled in accordance with internal guidance or practice which was similar to the Section 94 Handling Arrangements, and was sufficiently foreseeable.

Issue 3: Is the Section 94 Regime unlawful as a matter of EU law on the ground that there is no requirement for judicial authorisation prior to accessing data?

190. The assertions at paragraph 36 of the Claimant's Grounds that the Section 94 Regime is within the scope of EU law and that it is subject to the Charter are not accepted.

191. Further and in any event, the issue of prior judicial authorisation was addressed by this Tribunal in the *Liberty/Privacy* case, in the context of

warrants under s.8(4) RIPA. At §116(vi) of its judgment, the Tribunal concluded that the absence of prior judicial authorisation in that context gave *"no basis for objection."* The Respondents rely on that conclusion and contend that the same applies in this, related, context.

192. Properly understood, the judgment of the CJEU in the *Digital Rights Ireland* case does not assist the Claimant. The judgment addressed the validity of the Data Retention Directive, and focused in that regard on the lack of guarantees that had been established at EU level under the Directive to protect retained data against the risk of abuse and unlawful access. The judgment did not consider the detail of any national data retention and access regimes, nor did it prescribe any express requirements as to the content of such regimes. The Respondents rely in this regard on the analysis of the Court of Appeal in its recent decision in *SSHD v Davis & Watson* [2015] EWCA Civ 1185, by which it allowed an appeal against the earlier decision of the Divisional Court in that case.

193. The Respondents note that the Court of Appeal has referred questions as to the correct interpretation of the *Digital Rights Ireland* judgment to the CJEU. Further, the British government has intervened in [Case-203/15 *Tele2 Sverige AB*], a case raising similar issues that is pending before the CJEU.

194. As to paragraphs 49 to 52 of the Re-Amended Statement of Grounds:

(a) The Claimant's allegations as to the lack of proportionality in the BPD and section 94 regimes and also in any retention of the Claimant's details pursuant to either regime are noted, together with the authorities that are relied upon in this respect.

(b) The said allegations are denied. It is denied in particular, and as aforesaid, that either EU law or the Convention requires prior judicial authorisation as asserted at paragraph 51 of the Re-Amended Grounds.

(c) In order to rule on these allegations, it will be necessary for the Tribunal to consider CLOSED evidence regarding the operation of the two regimes. For that reason, these allegations are not suitable for determination as a preliminary issue of law. At the directions hearing held on 15 January 2016, those acting for the Claimant suggested that this issue could be addressed in OPEN proceedings by reference to assumed facts. Such facts would need to be agreed between the parties and the Claimant's further proposals in this regard are awaited.

195. As to paragraphs 53 to 58 of the Re-Amended Statement of Grounds, the Respondents plead as follows.

196. As pleaded at paragraph 22 above, directions made under section 94 of the Telecommunications Act 1984 have been issued to CSPs requiring the provision of Bulk Communications Data. More particularly:

(a) GCHQ has acquired BCD by means of a number of section 94 directions. Two such directions were made in the period 1998-1999, both of which were cancelled in 2001. All other such directions have been made since 2001.

(b) The Security Service has acquired BCD by means of a number of section 94 directions. The earliest of these directions was made in 2005.

(c) SIS has not used section 94 directions to obtain BCD.

197. The Respondents make the following further averments regarding the said section 94 directions and the BCD acquired pursuant to the directions.

(a) All the directions have been made personally by a Secretary of State following prior consultation with the CSP concerned.

(b) All BCD provided pursuant to the said directions has been added to secure databases.

(c) Access to the BCD has thereafter been closely controlled. Since 2000, such access has only been permitted if justified on necessity and proportionality grounds. The procedure at the Security Service is that BCD can only be accessed by following the authorisation process set out at sections 22 and 23 of RIPA. Since 2000, GCHQ has required any access to the BCD to be justified on the same grounds and to the same standards as access to related communications data obtained pursuant to section 8(4) of RIPA.

(d) The ongoing need for each of the directions has been subject to review both within the Security Service and GCHQ and also by the Home Secretary and the Foreign Secretary.

198. For the avoidance of doubt, no directions have ever been made under section 94 authorising the obtaining of the content of communications and/or the carrying out of equipment or property interference. The Respondents contend that such conduct can only be lawfully undertaken when authorised under the relevant provisions of (respectively) RIPA 2000, ISA 1994, and Part III of the Police Act 1997.[19] For completeness, the Respondents do contend that directions under section 94 can lawfully be made to require CSPs to facilitate conduct that has already been made lawful by authorisations under the aforesaid provisions.

199. It is averred that the section 94 directions by which GCHQ and the Security Service have obtained BCD were lawfully made.

200. At all material times the powers conferred by section 94 included a power to require CSPs to provide BCD. The principle of legality does not arise; given

---

[19] absent relevant consent – see, e.g., RIPA section 3(1)

the statutory context, the use of the power in this way was plainly within the contemplation of Parliament. Moreover, it is denied that the power to acquire BCD under section 94 was subject to implied repeal as a result of the enactment of RIPA 2000. The effect of the latter statute (in particular Part I, Chapter II thereof) was to create a separate regime for the acquisition of communications data. The RIPA regime differed in important respects from the section 94 power and no question of implied repeal can therefore arise.

201. In the case of the aforesaid section 94 BCD directions, the decision to use the section 94 power notwithstanding the availability of section 22 of RIPA 2000 was lawful in light in particular of the fact that the use of the section 94 power required the direction to be made personally by a Secretary of State. This amounted to an additional safeguard that would not have been present had the section 22 power been exercised. The safeguards set out at paragraph 197 above were also of relevance in this regard.

202. As to paragraph 57 of the Re-Amended Grounds, the existence of the aforesaid section 94 directions was not disclosed in any of the court proceedings referred to by the Claimant because the existence of the said directions was not relevant to the issues in those proceedings and in those circumstances such disclosure was not necessary. Both *Liberty v UK* and *Kennedy v UK* were cases about the interception of the content of communications. Since section 94 has not been and cannot be used to authorise such activity, and since neither *Liberty* nor *Kennedy* raised issues regarding the acquisition of communications data, no disclosure relating to the section 94 power was necessary. Whilst the *Davis & Watson* proceedings did concern communications data, the focus of those proceedings was on the retention of such data by CSPs rather than on the means by which such data might be acquired from the CSPs; there was accordingly no requirement to disclose the existence of the section 94 directions in those proceedings either.

~~SUGGESTED DIRECTIONS~~

~~203. The Respondents invite the Tribunal to make the following directions, prior to the directions hearing:~~

~~(a) Within 21 days of service of this Response, the Claimant shall confirm in writing whether the Issues for the Legal Issues Hearing that are identified in this Response are agreed and, to the extent that they are not, shall set out the pure issues of law which they propose should be determined at that hearing.~~

(b) ~~No later than three working days before the directions hearing the parties to file and serve their suggested directions for the management of the Claim up to and including the Legal Issues Hearing.~~

27 November 2015

JAMES EADIE QC
ANDREW O'CONNOR QC
RICHARD O'BRIEN

19 February 2016

JAMES EADIE QC
ANDREW O'CONNOR QC
RICHARD O'BRIEN