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

RESPONDENTS' SKELETON ARGUMENT FOR OPEN PRELIMINARY ISSUES HEARING 26-29 JULY 2016

This skeleton is served with two appendices setting out the relevant legal and policy regimes for Section 94 Bulk Communications Data (Appendix A) and Bulk Personal Datasets (Appendix B). References to documents in the five hearing bundles ("Core", "1", "2", "3" and "4") are in the form e.g. ***[Core/tab name or number/page].*** *References to the authorities in the bundles lodged with the Tribunal are in the form:* ***[Auths/tab]***

INTRODUCTION

1. This skeleton argument addresses the OPEN preliminary issues of law numbered 1-4 on the Amended Agreed List of Issues annexed to the Tribunal's order of 7 July 2016 [**Core/A/10**]. Issue 1 concerns the legality in domestic law of the Respondents' use of directions under s.94 of the Telecommunications Act 1984 to obtain communications data ('CD'). Issues 2-4 concern the compatibility of the s.94 regime and also the Respondents' Bulk Personal Data ('BPD') regimes with Article 8 ECHR. The Tribunal has directed that issues 5-8, which raise related questions of EU law, are to be heard at a subsequent hearing.

2. The threat to the UK from international terrorism has continued to increase. The threat level currently stands at SEVERE, which means that an attack in the UK is highly likely. Six alleged terror plots targeting the UK were stopped in the year prior to September

2015.[1] As is more than apparent from recent tragic events in Tunisia, Paris and Brussels, the principal terrorist threat derives from militant Islamist extremists, particularly in Syria and Iraq. Even before these events, it was clear that ISIL had emerged as the most violent of the terrorist groups operating in that region and that it was supported by foreign fighters from European countries. But Islamist terrorism is not the only threat to the UK. There remains a threat from Northern Ireland-related terrorism. The threat in Northern Ireland itself is assessed to be SEVERE, and the threat from Northern Ireland-related terrorism to Great Britain was recently raised (on 11 May 2016) from MODERATE to SUBSTANTIAL, meaning a terrorist attack is a strong possibility.[2] The UK also faces threats from the aggressive behaviour of authoritarian regimes, including hostile operations conducted against UK interests by foreign intelligence agencies,[3] as well as from serious and organised crime.[4]

3. The Security and Intelligence Agencies ('SIAs'), who are the Third, Fourth and Fifth Respondents to these proceedings, are centrally involved in defending the UK's interests and protecting its citizens from these threats. As the witness evidence that has been served explains, that task has become increasingly complicated and challenging as a result of a combination of factors including the increasing use of the internet and social media by groups like ISIL, the unprecedented security of terrorist communications and the advent of ubiquitous encryption.

4. The agencies have sought to adopt new methods in response to these challenges, including an increased reliance on the exploitation of both BPD and also bulk communications data ('BCD'). The Security Service witness states:

> *"In the face of this significant and enduring threat from terrorism, serious and organised crime and other national security threats there is a pressing need for the SIA and law enforcement agencies to be able to secure valuable intelligence in order to pursue their statutory objectives. It is in this context that BPD and BCD are so important to the SIA. In particular and to the extent that we do not now receive information (that previously we could obtain) then such information as we derive from other sources, such as BPD and BCD, is that much more crucial."*[5]

5. The Respondents' evidence as to the value of the use of both BPD and BCD is unequivocal.

   a. The statement of the GCHQ witness states:

---

1 Witness Statement of Security Service witness, §11 **[Core/B/2]**
2 Ibid, § 13 **[Core/B/2]**
3 Ibid, § 18 **[Core/B/2]**
4 Ibid, §§19-21 **[Core/B/2]**
5 Ibid, § 30 **[Core/B/2]**

"Exploitation of BPD is an essential tool that is used on a daily basis, in combination with other capabilities, right across the Intelligence Services' operations. It plays an integral role in enabling the intelligence Services to exercise their statutory functions. Without it, the Intelligence Services would be significantly less effective in protecting the UK against threats such as terrorism, cyber threats or espionage."[6]

b. The Security Service witness states:

"152…the use of BCD has stopped terrorist attacks and has saved lives many times.

153. The acquisition of BCD enables MI5 to identify threats and investigate in ways that, without this capability, would be either impossible or considerably slower ..."[7]

6. The Respondents submit that both the BPD and the s.94 regimes have at all times been necessary, proportionate and lawful.

7. As to the specific preliminary legal issues to be addressed in this OPEN hearing, the respondents' position on each is in summary as follows:

Issue 1: The section 94 regime is and has at all material times been lawful as a matter of domestic law.

Issues 2-4: The regime which governs BPD / BCD is "in accordance with the law / prescribed by law" under Article 8(2) ECHR. It is sufficiently foreseeable, contains sufficient safeguards to protect against arbitrary conduct, it is proportionate and this has been the case at all material times.

ISSUE 1 – DOMESTIC LAW LEGALITY OF SECTION 94 REGIME

8. Issue 1 on the Amended Agreed List of Issues [**Core/A/10**] states:

"Is and was:
- *a. the obtaining of communications data,*
- *b. any obtaining of the content of communications,*
- *c. any carrying out of equipment interference, or*
- *d. any other kind of property interference*

under s.94 of the TA 1984, unlawful as a matter of domestic law?"

---

6 Witness statement of GCHQ witness, § 16 **[Core/B/2]**

7 Witness statement of Security Service witness, §§ 152-153 **[Core/B/2]**

9. The Claimant has raised a further issue of domestic law relating to the sharing of material obtained under s.94 directions. The parties have agreed that this issue be tested by reference to the following assumed facts:

> *"It is to be assumed for the purposes of this hearing:*
>
> *(a) that a Programme exists by which GCHQ discloses information to domestic law enforcement agencies ("LEAs"); and*
>
> *(b) that this disclosure might take place either*
>
> *(i) by GCHQ permitting the LEAs to access and search data that it holds, including communications data obtained pursuant to section 94 directions; or*
>
> *(ii) by GCHQ providing the LEAs with information derived from the data that it holds, including communications data obtained pursuant to section 94 directions."*

For the avoidance of any doubt, the Respondents neither confirm nor deny whether a 'Programme' of the type referred to exists, or whether in general terms the type of data sharing referred to in the assumed facts takes place.

10. The issue is whether, on the basis of these assumed facts, it would be lawful for GCHQ to share information that it had obtained for national security purposes under s.94 with law enforcement agencies, who required the information for a different purpose, namely combating serious crime.

The s.94 regime

11. No directions under s.94 of the Telecommunications Act 1984 [**Auths/tab 1**] have ever been made authorising the obtaining of the content of communications and/or authorising the carrying out of equipment or property interference.[8] Sub-issues (b), (c) and (d) do not therefore arise.

12. In relation to sub-issue (a), it has been publicly avowed that s.94 directions have been made to obtain BCD. The making of these directions, and the procedures under which the BCD has subsequently been dealt with, is referred to as 'the s.94 regime'.

13. The core facts relating to the domestic legality of the s.94 regime are as follows:

---

[8] Respondents' Amended Open Response, §198 **[Core/A/2]**

a. Section 94 directions issued to communications service providers ('CSPs'), requiring the production of BCD, have been made by both the Foreign Secretary and the Home Secretary.
b. Section 94 directions made by the Foreign Secretary have required the provision of BCD to GCHQ. The Foreign Secretary made two s.94 directions in the period 1998-1999, both of which were cancelled in 2001; all other such directions have been made since 2001.
c. The Home Secretary's s.94 directions have required the provision of BCD to MI5. The earliest of the Home Secretary's s.94 directions was made in 2005.[9]

14. Section 94 was amended by the Communications Act 2003.[10] The provisions of s.94 **[Auths/tab 1]** that are material for present purposes are set out below, showing the amendments made by the 2003 Act.

> ***"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 ~~requisite or expedient~~ necessary in the interests of national security or relations with the government of a country or territory outside the United Kingdom. …*
>
> *(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. …*
>
> *(8) This section applies to OFCOM and to providers of public electronic communications networks ~~the Director and to any person who is a public telecommunications operator or approved contractor (whether in his capacity as such or otherwise); and in this subsection "approved contractor" means a person approved under section 20 above~~."*

The Claimant's *vires* challenges to the s.94 regime

15. The Respondents make three central submissions in response to the Claimant's challenges:

a. The use of s.94 to make directions requiring the production of communications data is not prohibited by the principle of legality.
b. Section 94 was not impliedly repealed by RIPA.
c. It was and is not unlawful for directions requiring the production of communications data to be made under s.94 rather than RIPA.

---

9 Respondents' Amended Open Response, §196 **[Core/A/2]**

10 Communications Act 2003, section 406 and Schedule 17, paragraph 70 **[Auths/tab 8]**

(1) Section 94 directions not barred by the principle of legality

16. In *R v Secretary of State for the Home Department, ex parte Simms* [2000] 2 AC 115 [**Auths/tab 25**], 131 F-G, Lord Hoffman described the principle of legality as follows:

> *"... the principle of legality means that Parliament must squarely confront what it is doing and accept the political cost. Fundamental rights cannot be overridden by general or ambiguous words ... In the absence of express language or necessary implication to the contrary, the courts therefore presume that even the most general of words were intended to be subject to the basic rights of the individual. In this way the courts of the United Kingdom, though acknowledging the sovereignty of Parliament, apply principles of constitutionality little different from those which exist in countries where the power of the legislature is expressly limited by a constitutional document."*

17. The principle is thus a guide to statutory interpretation. As such, it is part of the set of principles that are designed to assist the Court to discern the intention of Parliament. It does not alter the nature of the exercise of interpretation, which remains one of faithfully seeking to ascertain Parliament's intention. Nor does it supplant the possibility that Parliament's true intention when using broad empowering words was that their natural meaning and breadth was indeed to confer a power that was broad – reflecting the possibility that the power would need to be exercised and could usefully and properly be exercised in a wide range of circumstances which it would be neither desirable nor practically possible to enumerate specifically.

18. The first question that arises is whether the principle of legality is engaged by, or applicable in, the present context at all.

19. The principle plainly does not apply on every occasion that a Secretary of State may act in what is judged to be the public interest in reliance on a generally phrased statutory power. Rather, it is reserved for serious infringements of rights, in which the Executive act *'overrides'* (to use the language of Lord Hoffman in *Simms*) fundamental or constitutional rights. It is submitted that this threshold of seriousness is important to avoid the principle becoming overbroad and reaching beyond the limits of its rationales (again as described by Lord Hoffmann). It cannot and does not apply in any context in which action is taken under broadly expressed powers which could be characterised as in some way touching or interfering with say a qualified right under the ECHR – almost anything can be so characterised. To put the same point by reference to Parliamentary intention (which is what is being searched for in the exercise of interpretation), Parliament cannot properly be taken to have intended in effect to exclude from the ambit of generally expressed power a field as broad as that approach would entail.

20. The need for the principle to be properly confined in its application is emphasised by the fact that its effect ultimately is to remove power or *vires*. Its effect as a principle is not just to control the manner in which the power is exercised across the fields apparently covered by the natural breadth of the language Parliament has chosen to use. It is to remove swathes of power entirely. This point is given particular force because since the Human Rights Act 1998 [**Auths/tab 6**] any exercise of power by any public authority has to be compatible with the scheduled ECHR rights anyway. That provides significant protection against overriding fundamental rights in any event.

21. The cases illustrate that the principle applies when fundamental rights are indeed '*overridden*' (rather than merely when they might be affected in some way which may be minimal, despite qualifying as some form of interference and might be obviously justifiable in any event). The facts of *Simms* itself provide an example. Likewise in *Ahmed v HM Treasury*[11], the Al Qaida Order was held to be *ultra vires* pursuant to the principle of legality because its immediate effect was to impose asset freezing measures without providing any means by which the individuals subject to those measures might challenge them in court. Thus, as the Supreme Court held, the executive act constituted an immediate and serious violation of the right of access to the court.

22. It is also to be noted relatedly that the principle of legality is a common law principle that has been developed to protect so-called 'constitutional rights' that have been recognised by the common law. Many of the cases in which the principle has been invoked concern the right of access to courts.[12] Others have concerned the related right of legal professional privilege[13] and also the right not to be searched by the police unless reasonably suspected of having committed a criminal offence.[14] These are all rights recognised by the common law. And whilst it is clear from these examples that the category of 'fundamental' or 'constitutional' rights recognised by the common law overlaps with the rights protected by the ECHR, there is no complete overlap. It is plainly not the case that all the rights listed in the ECHR have been recognised as fundamental rights at common law. The rights that (it is assumed) the Claimant contends are affected by the s.94 directions that have been made to obtain CD are qualified privacy rights. These are not rights that have ever acquired the status of 'constitutional' or 'fundamental' rights under the common law.

23. Turning to the present context, the immediate effect of the issuing of a s.94 direction is limited to requiring a CSP to provide CD. This step engages the privacy rights of those

---

11 [2010] 2 AC 534 **[Auths/tab 36]**.

12 For example, *Raymond v Honey* [1983] 1 AC 1 **[Auths/tab 21]**, *R v Lord Chancellor, ex p Witham* [1998] QB 575 **[Auths/tab 23]**, *Ahmed v HM Treasury* [2010] 2 AC 534 **[Auths/tab 36]**

13 *General Mediterranean Holdings SA v Patel* [2000] 1 WLR 272 **[Auths/tab]**

14 *SSHD v GG* [2010] 1 QB 585 **[Auths/tab 37]**

involved (in the sense that it amounts to an interference with those rights). However, the context involves privacy. That is neither a core constitutional right of the kind previously held to have triggered the principle of legality; nor an unqualified ECHR right. Moreover, it could not properly be said that the direction '*overrides*' those rights. It simply interferes with such rights – leaving untouched the question for example whether such interference is justified as necessary and proportionate. Privacy rights are qualified, so that interferences with those rights can be justified. Put another way, they are not '*overridden*' by interference, simply because they are engaged or affected by the exercise of a power conferred by Parliament. It is accordingly submitted that, for these reasons, the principle of legality simply does not arise in this case.

24. The alternative submission is that the extent to which the presumption that underpins the principle of legality is in play depends upon the context. The presumption that Parliament would have specified clearly if it intended to override fundamental rights applies more weightily in circumstances in which the interference is more serious.

25. It is submitted in any event that s.94 clearly expresses Parliament's intention and included the power to make s.94 directions to CSPs to obtain CD.

26. **First**, the natural meaning of the words is to confer power which can be exercised in a broad range of circumstances. There is, in context, good and obvious reason for that. It would have been wholly impractical to seek to specify precisely when and in what circumstances the power might be exercised. That point applies with equal force to circumstances in which the power might be exercised in a way that could be said to interfere with say Article 8 rights and freedoms.

27. **Secondly**, it is necessary to have regard to '*the whole statutory context*' (see per Dyson LJ in *SSHD v GG* [2010] 1 QB 585 **[Auths/tab 37]** at §44[15]) in order to determine whether Parliament in fact intended to permit the act which might be said to affect fundamental rights.

28. Here, it is evident that the power was conferred so that it could be used *inter alia* in order to secure and protect national security. The statute identifies only two statutory purposes for which a direction can be given – i.e. the interests either of national security or of relations with the government of a country or territory outside the United Kingdom. So it is plain that Parliament intended to permit a s.94 direction to be given if it was judged appropriate to do so for the national security purpose. In common with the legislation governing the activities of the SIAs more generally that purpose provides

---

15 "*In my judgment, these cases demonstrate that general statutory words will not suffice to permit an invasion of fundamental rights unless it is clear from the whole statutory context that Parliament intended to achieve that result.*" See also, to a similar effect, effect, *R v Lord Chancellor, ex parte Lightfoot* [2000] QB 597, CA **[Auths/tab 26]** at 624H – 629B.

the key legislative constraint and control on the exercise of power. It is entirely unsurprising that the constraint and control should be expressed at that level – what precisely might be needed from time to time effectively to protect the public through the protection of national security will depend upon the current circumstances. But for present purposes the important point is that if the question is asked – did Parliament intend to permit the Secretary of State to make a direction requiring CSPs to provide information about customers' communications if that was considered to be necessary and proportionate for the protection of national security – the answer is entirely obvious: of course it did.

29. It is all the more plain that that was Parliament's intention when consideration is given to the fact that the exercise of the power is constrained in other ways. Specifically:

    a. the category of those to whom directions can be given is also very limited – essentially the operators of public electronic communications networks;
    b. the category of those who can make a direction is extremely limited – directions can only be made by a Secretary of State.

30. Given these factual limitations that the statute imposes on the circumstances in which a s.94 direction can be given, it must have been clear to Parliament that one of the practical situations in which the power to make a direction would be exercised would be when a Secretary of State wished to direct a telecommunications provider to provide information that it held relating to the details of telephone calls in the interests of national security.

31. The logic of the Claimant's position would appear to be to exclude from the scope of the s.94 power any act or direction which might interfere in any way with ECHR rights (eg Article 8 but presumably also A1P1) however minimal and however obviously justifiable. That is an untenable intention to ascribe to Parliament.

32. **Thirdly**, Parliamentary intention is to be judged as at the time that the statute in question was enacted – in this case, 1984. It is impossible to imagine that this obvious use of the power would not have been appreciated by Parliament in 1984, particularly since at that time there was no other statutory power that could be used for this purpose.[16]

---

[16] The fact that BT could and did obtain communications data was a matter of public record in 1984. See in this regard paragraph 56 of the ECtHR's judgment in *Malone v UK* (1984) 7 EHRR 14 **[Auths/tab 46]**, which refers to the process that was then known as 'metering'. The judgment also records that this practice had been the subject of Parliamentary discussion from as early as 1978.

33. It is to be noted however that there is an extra dimension to this point here, because substantive amendments were made to s.94 in 2003 to add requirements of necessity and proportionality to the exercise of the power. It is necessary also to give weight to the Parliamentary intention underlying those amendments. It is an inevitable inference from these amendments that Parliament recognised at that time that s.94 would be used to make directions that would have the effect of interfering with rights protected by the ECHR. An obvious example of such a direction was a direction requiring the provision of communications data, which would amount to an interference with Article 8 rights. These amendments made express in the particular legislation the requirement, which in any event flowed from s.6 of the HRA, that any such interference be justified against the well-known ECHR standards for such interferences.

(2) No implied repeal

34. Part I Chapter II of RIPA is entitled *'Acquisition and disclosure of communications data'* **[Auths/tab 7]**. Pursuant to s.22(4), a *'designated person'* may require a telecommunications operator to disclose CD to him. Such a requirement must be made on one of a number of statutory grounds specified in s.22(2). The permissible grounds include the interests of national security.

35. There is a strong presumption against implied repeal. In *Kutner v Phillips*[17], AL Smith J stated:

> *"… a repeal by implication is only effected when the provisions of a later enactment are so inconsistent with or repugnant to the provisions of an earlier one that the two cannot stand together ... Unless two Acts are so plainly repugnant to each other that effect cannot be given to both at the same time a repeal will not be implied"*

That strict test was repeated (by the same judge) in *West Ham Wardens v Fourth City*.[18] It has been applied ever since – see eg the more recent decisions of the Court of Appeal in *O'Byrne v Secretary of State for Environment, Transport and the Regions & another*[19], *Henry Boot Construction (UK) Ltd v Malmaison Hotel (Manchester) Ltd*[20] and *Snelling v Burstow Parish Council*.[21]

---

17 [1891] 2 QB 267 **[Auths/tab 19]**, at p.271

18 [1892] 1 QB 654 **[Auths/tab 20]**, at p.658

19 [2001] EWCA Civ 499; [2002] HLR 30 **[Auths/tab 28]**. The House of Lords upheld the Court of Appeal's decision on different grounds – *Secretary of State for the Environment, Transport and the Regions v O'Byrne* [2002] 1 WLR 3250.

20 [2001] QB 388 **[Auths/tab 29]**

21 [2014] 1 WLR 2388 **[Auths/tab 40]**

36. It has been held, moreover, that the presumption against implied repeal applies with more force to modern statutes. In *Henry Boot*, Waller LJ quoted an observation of Lord Roskill expressing caution about very early authorities on implied repeal, on the basis that *"[u]ntil comparatively late in the last century statutes were not drafted with the same skill as today."*[22]

37. The Court of Appeal in *O'Byrne* emphasised the demanding nature of the test for implied repeal. Buxton LJ rejected (at §§25-26) a suggestion that an implied repeal could arise where the combined result of two statutes created a merely anomalous situation. He stated, rather, that an implied repeal could only arise where it was *"impossible to operate the two Acts simultaneously"*.[23] Laws LJ stated (at §68) that implied repeal required an *"inescapable logical contradiction between the earlier and the later statute"*. On a similar theme, Patten LJ held in *Snelling* (§39) that the mere redundancy of the earlier provision was not enough to lead to implied repeal.

38. The Respondents make the following submissions on implied repeal.

39. **First**, RIPA is a modern and extremely detailed statute. It is striking in this context that RIPA does not include any provision repealing or amending s.94. Parliament could have amended or repealed s.94 at the time that it enacted RIPA, but it did not do so. Against that background, and applying Lord Roskill's dictum, the Tribunal should be very slow to find an implied repeal.

40. **Secondly**, the power to make directions for the production of CD under s.94 and the power to make orders under s.22 of RIPA are properly understood as parallel regimes. The regimes could both lead to the production of CD for use for national security purposes. However, those who can exercise the powers are distinct:

    a. A direction under s.94 can only be made by a Secretary of State. A s.94 direction cannot be made in the name of an official.
    b. An order under s.22(4) of RIPA **[Auths/tab 7]**, by contrast, can only be made by a 'designated person'. Section 25(1) of RIPA specifies a number of 'relevant public authorities', including the police and the intelligence agencies, and s.25(2) provides that *"persons designated for the purposes of this Chapter are the individuals holding such offices, ranks or positions with relevant public authorities as are prescribed for the purposes of this subsection by an order made by the Secretary of State."*
    c. The power to prescribe the *'offices, ranks or positions'* within *'relevant public authorities'*, with the effect of conferring upon the holders of those *'offices, rank or*

[22] paragraph 16
[23] paragraphs 41-42

positions' the status of *'designated persons'* for the purposes of s.22 was first exercised by the Regulation of Investigatory Powers (Communications Data) Order 2003.[24] The effect of that Order was to authorise a large number of officials at a range of organisations to make orders for the production of communications data under s.22 of RIPA. Neither the Home Secretary nor any other Secretary of State has any power to make orders under s.22.

41. There is a further respect in which the powers under section 94 and section 22 are properly understood as creating parallel regimes. A direction under section 94 can be made not only for national security reasons, but also because such a direction is *"necessary in the interests of … relations with the government of a country or territory outside the United Kingdom"*. The statutory purposes for which the section 22 power can be exercised are set out at section 22(2) of RIPA and also at paragraph 2 of the Regulation of Investigatory Powers (Communications Data) Order 2010.[25] International relations is not amongst those specified statutory purposes.

42. To adopt the terminology used by the Court of Appeal in the *O'Byrne* case, it cannot be said that it is "*impossible to operate the two Acts simultaneously*", nor is there an "*inescapable logical contradiction between the earlier and the later statute*".

43. **Thirdly**, the statutory safeguards prescribed in RIPA do not automatically apply to material obtained pursuant s.94 directions. However:

    a. At the level of substantive protection, the differences must not be overstated. For example, when making a direction under s.94 the statutory purpose must be served and the direction must be considered to be necessary and proportionate. The same essential safeguards apply in a national security context where the s.22 power is being exercised. Moreover, at the later stages of handling and using the data, the series of safeguards dealt with in more detail below apply to provide adequate safeguarding.
    b. To the extent that there is greater specificity of safeguards in the RIPA context, that is explicable by reason of the fact that under that regime directions are made by a large number of different officials in a wide range of different organisations throughout the country. It does not follow that the same system is needed in the s.94 context, where a much smaller number of directions are made and then only by a Secretary of State (ie at the highest level of Government). Nor does it follow that the safeguarding that applies in that s.94 context is in any way insufficient. As the evidence in this case demonstrates, the fact that RIPA safeguards do not apply automatically does not mean that

[24] SI 2003/3172 **[Auths/tab 13].**
[25] SI 2010/480 **[Auths/tab 15]**.

substantially similar safeguards either cannot be or have not been applied to the material in question.

44. **Fourthly**, it will be noted that what the Claimant contends for is only a *partial* repeal of s.94. The Claimant does not suggest that s.94 was impliedly repealed *in toto* by RIPA, but only to the extent that it authorised the making of directions requiring CSPs to produce communications data. It is of course possible in principle for there to be a *pro tanto* implied repeal of a statutory power. But the greater the subtlety of the statutory change said to have been effected by implied repeal, the more improbable it becomes that Parliament would not have made its intention overtly clear – particularly given the points made about the sophistication of modern legislation highlighted above.

45. **Fifthly**, it is illuminating to consider the date on which any implied (partial) repeal of s.94 may have taken effect. This could not have been earlier than 5 January 2004, which was the date on which RIPA s.22 was commenced. However, by this date, the amendments to s.94 by the Communications Act 2003 (adding necessity and proportionality requirements) had already been made and commenced.[26] Moreover, the wording of the new s.94(2A) of the 1984 Act **[Auths/tab 1]** that was added a few months before RIPA s.22 was commenced is in almost identical terms to RIPA s.22(5) **[Auths/tab 7]**. These are very strong indicators that Parliament intended the two regimes to run in parallel. The case that s.94 was impliedly repealed by RIPA does not sit well or consistently with the fact that Parliament was giving specific attention to and amending (but, of course, not repealing) s.94 at just the time when Part I Chapter II of RIPA was coming into force.

46. Finally, the cases that are relied upon by the Claimant (*R v Direction of SFO, ex p Smith* [1993] AC 1 **[Auths/tab 22]** and *Re McE* [2009] 1 AC 908 **[Auths/tab 34]**) do not assist. Neither was a case in which it was even argued that an earlier statutory power was impliedly repealed by RIPA.

(3) Not unlawful for directions requiring the production of communications data to be made under s.94 rather than s.22 RIPA

47. The Claimant's contention is that "*where specific powers with relevant safeguards exist, it would absent a good reason be a misuse of power to use a general power without such safeguards*". The premises on which this issue arises are that (a) properly interpreted, s.94 confers power to make directions requiring the production of CD; and (b) the existence of that power was not affected by the commencement of s.22 of RIPA.

---

[26] The Communications Act 2003 received Royal Assent on 17 July 2003. §70 of Schedule 17 of the 2003 Act, which contained the amendments to s.94, was commenced in two stages in July and September 2003 – see SI 2003/1900 **[Auths/tab 14].**

48. **First**, no authority is cited for the contention made by the Claimant. It is inconsistent with dicta in at least two decisions of the Court of Appeal. In *Snelling*, Patten LJ stated at §41:"*The better view is that these are different, although overlapping provisions, and the council may choose between them.*" **[Auths/tab 40]** In *RK (Nepal) v SSHD* [2009] EWCA Civ 359 **[Auths/tab 35]**, Aikens LJ referred (at §35) to the fact that the Secretary of State might have made a particular immigration decision under one or other of two separate powers, notwithstanding that one of the powers carried an in country right of appeal, whilst the other carried only an out of country appeal right.

49. **Secondly**, the Claimant's argument again overlooks the fact that there is no overlap between the categories of those who can make the two types of orders. A Secretary of State cannot make an order under RIPA s.22, and the array of law enforcement officers and officials who are 'designated persons' for the purposes of s.22 have no power to make a direction under s.94.

50. **Thirdly**, it is inherent in the Claimant's argument that there is a simple dichotomy between directions made under s.94 (no safeguards) and those made under RIPA s.22 (detailed safeguards). The fact that s.94 directions are made personally in the name of a Secretary of State is in itself an important safeguard that cannot be replicated in a s.22 direction. Moreover, the fact that the other safeguards specified by RIPA do not automatically apply to s.94 directions and information obtained pursuant to them does not mean that substantially similar safeguards are not in place, as the facts of this case demonstrate.

51. **Fourthly**, depending on the facts of particular situations, there may be other, entirely rational and appropriate, reasons for favouring an order made under s.94 to one made under s.22: see, for example, of the Witness Statement of the Security Service Witness at §§110-112 **[Core/B/2]**.

(4) Purposive construction of s.94 under section 3 HRA / the *Marleasing* principle

52. The Claimant suggests that s.94 should be read down pursuant either to s.3 HRA or the *Marleasing* principle. The Claimant does not explain or develop either how the conditions for such an approach are met, or how it contends the provision should be interpreted. It is submitted that there is no warrant for reading down. It is noted that s.3 HRA would only be triggered if a '*possible*' reading down was necessary in order to avoid actual incompatibility between the legislation and a scheduled HRA right: see the decision of the Court of Appeal in *Donoghue v Poplar Housing* [2002] QB 48 **[Auths/tab 30]**, at §75a ("*unless the legislation would otherwise be in breach of the Convention section 3 can be ignored; (so courts should always first ascertain whether, absent section 3, there would be any*

breach of the Convention)"), approved by Lord Hope of Craighead in *R v A* [2002] 1 AC 45 **[Auths/tab 31]**, at §58. The same approach applies to trigger the *Marleasing* principle under EU law.

Provision of s.94 data to law enforcement agencies

53. It is submitted that it would be lawful for GCHQ to provide data, obtained by means of s.94 directions to other government law enforcement agencies ('LEAs'), on the basis that those other LEAs required the data for the purposes of combating serious crime. This issue is to be tested against the following assumed facts:

> *"It is to be assumed for the purposes of this hearing:*
>
> *(a) that a Programme exists by which GCHQ discloses information to domestic law enforcement agencies ("LEAs"); and*
>
> *(b) that this disclosure might take place either*
>
> *(i) by GCHQ permitting the LEAs to access and search data that it holds, including communications data obtained pursuant to section 94 directions; or*
>
> *(ii) by GCHQ providing the LEAs with information derived from the data that it holds, including communications data obtained pursuant to section 94 directions."*

As stated above, the Respondents neither confirm nor deny whether a 'Programme' of the type referred to exists, or whether in general terms the type of data sharing referred to in the assumed facts takes place.

54. Obtaining CD produced by CSPs pursuant to directions issued under s.94 falls within GCHQ's statutory functions set out at s.3(1)(a) of the Intelligence Services Act 1994 ('ISA') **[Auths/tab 4]**:

> ***"3 The Government Communications Headquarters.***
>
> *(1)There shall continue to be a Government Communications Headquarters under the authority of the Secretary of State; and, subject to subsection (2) below, its functions shall be –*
>
> *(a) 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;…"*

55. The purpose for which GCHQ obtains s.94 data is the interests of national security, which is one of its statutory functions as listed at s.3(2) of ISA:

"(2) The functions referred to in subsection (1)(a) above shall be exercisable only –

(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."

56. Section 19(2) of the Counter-Terrorism Act 2008 ('CTA') **[Auths/tab 9]** then expressly provides:

"(2) Information obtained by any of the intelligence services[27] *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*."

Given GCHQ's statutory function of supporting the prevention or detection of serious crime (s.3(2)(c) of ISA), GCHQ is entitled to use s.94 data for that other statutory purpose, as well as in the interests of national security.

57. Section 19(5) of the CTA provides that:

"(*5) Information obtained by GCHQ for the purposes of any of its functions may be disclosed by it –*

(a) for the purpose of the proper discharge of its functions, or

(b) for the purpose of any criminal proceedings."

Since GCHQ's functions include supporting the prevention or detection of serious crime, GCHQ is entitled to disclose s.94 data to LEAs for that purpose.

58. Finally, s.4(2) of ISA **[Auths/tab 4]** provides that it is the duty of the Director of GCHQ 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..."*

59. It follows that any disclosure of such information must satisfy the constraints imposed in ss.3-4 of the ISA, as read with s.19(5) of the CTA **[Auths/tab 9]**. Additionally any such

---

[27] Section 21(1) of CTA provides that *"In sections 19 and 20 "the intelligence services" means the Security Service, the Secret Intelligence Service and GCHQ."* **[Auths/tab 9]**

disclosure must comply with the necessity and proportionality requirements imposed b and s.6(1) of the HRA. Thus specific statutory limits are imposed on the information that GCHQ can disclose.

60. The Claimant's Re-Amended Statement of Grounds does not contain any pleaded case as to the respects in which a "Programme" of the sort described in the assumed facts would be unlawful. The Respondents will respond in due course to the points raised in the Claimant's skeleton argument.

ISSUES 2-3 – ARTICLE 8 ECHR

Article 8 ECHR – the principles

61. Issues 2-3 concern whether or not the s.94 and BPD Regimes are in accordance with the law under Article 8(2) ECHR. The relevant principles relating to Article 8(2) are as follows.

62. As the Tribunal held at §37 of its judgment in *Liberty/Privacy* **[Auths/tab 38]**, in order for an interference to be "*in accordance with the law*":

> "*i) there must not be an unfettered discretion for executive action. There must be controls on the arbitrariness of that action.*
>
> *ii) the nature of the rules must be clear and the ambit of them must be in the public domain so far as possible, an "adequate indication" given (Malone v UK [1985] 7 EHRR 14 at paragraph 67), so that the existence of interference with privacy may in general terms be foreseeable...*"

See also *Bykov v. Russia*[28], at §78, quoted at §37 of *Liberty/Privacy*.

63. As the Tribunal also noted in *Liberty/Privacy*, 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). See also in that respect, *Malone v UK*[29] (at §§67-68m), *Leander v Sweden*[30] at §51 and *Esbester v UK*[31], quoted at §§38-39 of *Liberty/Privacy*. Thus, as held by the Tribunal in the

[28] Appl. no. 4378/02, 21 January 2009 **[Auths/tab 57]**.
[29] (1984) 7 EHRR 14 **[Auths/tab 46]**.
[30] [1987] 9 EHRR 433 **[Auths/tab 47]**.
[31] [1994] 18 EHRR CD 72 **[Auths/tab 49]**.

British Irish Rights Watch case[32] (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)

64. Thus, the national security context 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 *Liberty/Privacy* judgment). That is not least because 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*, §67; *Leander v. Sweden*, §51; and *Weber and Saravia v Germany*[33], §93.

65. Further, in *Privacy/Greennet v (1) SSFCA (2) GCHQ*[34] ("the *Malware* judgment") the CNE Regime was held to be foreseeable before any admission had been made that the respondent (GCHQ) carried out CNE (see §§78(i) and 81). The Tribunal held that, notwithstanding that there had been no such admission or avowal:

> "*Nevertheless it was quite clear that at least since 1994 the powers of GCHQ have extended to computer interference (under s.3 of ISA). It was thus apparent in the public domain that there was likely to be interference with computers, 'hacking' being an ever more familiar activity, namely interference with property by GCHQ..., and that if it occurred it would be covered by the Property Code. Use of it was thus foreseeable, even if the precise form of it and the existence of its use was not admitted.*"

66. This applies with equal force to the present case where:

a. although the use of s.94 to obtain BCD had not been publicly avowed, it was nonetheless foreseeable because (i) GCHQ and MI5's acquisition of communications data in more general terms *was* publicly known (albeit pursuant to a warrant issued under s.8(4) of RIPA or by an authorisation under Part 1 Chapter II of RIPA). There was therefore nothing secret about the essential activity of acquisition of such data by those agencies; and (ii) s.94 itself clearly extended to requiring CSPs to provide BCD in the interests of national security; and
b. although the use by the SIA of Bulk Personal Datasets had not been avowed, the acquisition of personal data in bulk was foreseeable because (i) the Respondents' powers to obtain information clearly extend to obtaining personal data; (ii) the acquisition of large volumes of such personal information was also foreseeable,

[32] IPT decision of 9 December 2004 **[Auths/tab 33]**.
[33] (2008) 46 EHRR SE5 **[Auths/tab 53]**.
[34] [2016] UKIP Trib 14_85-CH **[Auths/tab 44]**.

albeit subject to statutory requirements of necessity and proportionality; and (iii) the inclusion within such bulk personal data of information relating to individuals who were unlikely to be of intelligence interest (which would include, for instance, a telephone directory or electoral roll) was also foreseeable, again subject to the requirement that any acquisition of such data was necessary and proportionate; and

c. in both cases, the use of BCD/BPD was foreseeable *"even if the precise form of it and the existence of its use was not admitted."*

67. As to the procedures and safeguards which are applied, two points are to be noted.

a. 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 §78 of *Bykov* **[Auths/tab 57]**; and was reiterated by the Tribunal at §§118-122 of *Liberty/Privacy*. Hence the reliance on the Code in *Kennedy v United Kingdom*[35] at §156 and its anticipated approval in *Liberty v United Kingdom*[36] at §68 (see §118 of *Liberty/Privacy* and also *Silver v United Kingdom*[37]).

b. 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 concluded 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 *Liberty/Privacy*). At §129 of *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 ECHR has approved, which ensures that such arrangements are kept under constant review.*"

68. Those conclusions were reached in the context of the s.8(4) RIPA interception regime. They are equally applicable to the s.94 and BPD regimes to which published Handling Arrangements and *"below the waterline"* arrangements apply and where there is similar oversight by the Intelligence Services Commissioner and the Interception of Communications Commissioner.

---

[35] [2011] 52 EHRR 4 **[Auths/tab 59]**.
[36] [2009] 48 EHRR **[Auths/tab 55]**.
[37] [1983] 5 EHRR 347 **[Auths/tab 45]**.

69. In the context of interception, the ECtHR has developed a set of minimum safeguards in order to avoid abuses of power. These are referred to as 'the *Weber* requirements'. At §95 of *Weber*[38], the ECtHR stated:

> "*In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: (1) the nature of the offences which may give rise to an interception order; (2) a definition of the categories of people liable to have their telephones tapped; (3) a limit on the duration of telephone tapping; (4) the procedure to be followed for examining, using and storing the data obtained; (5) the precautions to be taken when communicating the data to other parties; and (6) the circumstances in which recordings may or must be erased or the tapes destroyed*." (numbered items added for convenience, see §33 of *Liberty/Privacy*)

(And see also *Valenzuela Contreras v Spain*[39] at §59)

70. However it is important to recognise what underpins the *Weber* requirements, as highlighted at §119 of the *Liberty/Privacy* judgment. In particular, §106 of *Weber* states as follows:

> "*The Court reiterates that when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life,* ***it has consistently recognised that the national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security*** *(see, inter alia, Klass and Others, cited above, p. 23, § 49; Leander, cited above, p. 25, § 59; and Malone, cited above, pp. 36-37, § 81).* ***Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse*** *(see Klass and Others, cited above, pp. 23-24, §§ 49-50; Leander, cited above, p. 25, § 60; Camenzind v. Switzerland, judgment of 16 December 1997, Reports 1997-VIII, pp. 2893-94, § 45; and Lambert, cited above, p. 2240, § 31).* ***This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law*** *(see Klass and Others, cited above, pp. 23-24, § 50).*" (emphasis added)

71. This emphasis on the need to consider all the circumstances of the case was recently reiterated by the ECtHR in *RE v United Kingdom*[40] at §127. In that case, because of the "*extremely high degree of intrusion*" involved in the surveillance of legal consultations,

[38] (2008) 46 EHRR SE5 **[Auths/tab 53]**.
[39] (1999) 28 EHRR **[Auths/tab 50]**.
[40] Application No. 62498/11, 27 October 2015 **[Auths/tab 60]**.

the ECtHR held that the same safeguards should be in place as would be required in an interception case, at least insofar as those principles could be applied to the surveillance in question (see §131). On the specific facts of that case, a breach of Article 8(2) ECHR was found given that the surveillance regime as it applied to legal consultations did not contain sufficient provisions as regards the examination, use and storage of the material obtained and the precautions to be taken when communicating the material to other parties or erasing/destroying the material (see §§138-141). The ECtHR contrasted the provisions in Part I of RIPA and the Interception Code, which it had approved in *Kennedy*, and concluded that they provided an example of the type of provisions which were required in this context.

72. The Tribunal in *Liberty/Privacy* placed considerable reliance on **oversight mechanisms** in reaching their conclusion that the intelligence sharing regime and the s.8(4) RIPA regime were Article 8 compliant. In particular:

a. The role of the Commissioner and "*his clearly independent and fully implemented powers of oversight and supervision*" have been long recognised by the ECtHR, as is evident from *Kennedy* **[Auths/tab 59]** at §§57-74, 166, 168-169 (see *Liberty/Privacy* at §§91-92). This is a very important general safeguard against abuse. In *Liberty/Privacy* the Tribunal relied, in particular, on his duty to keep under review the adequacy of the arrangements required by statute and by the Code, together with his duty to make a report to the Prime Minister if at any time it appeared to him that the arrangements were inadequate.
b. The advantages of the Tribunal as an oversight mechanism were emphasised at §§45-46 of *Liberty/Privacy*, including the "*very distinct advantages*" over both the Commissioner and the ISC for the reasons given at §46 of the judgment.
c. In addition the ISC was described as "*robustly independent and now fortified by the provisions of the JSA*" (see §121 of *Liberty/Privacy*) and therefore constituted another important plank in the oversight arrangements.

73. Consequently there is a need to look at all the circumstances of the case and the central question 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)

ISSUE 2

74. Issue 2 on the Amended Agreed List of Issues [**Core/A/10**] states:

"Is or was the s.94 Regime in accordance with the law under Article 8(2) ECHR:

a. prior to the avowal of the use of s.94 to obtain communications data and the publication of the s.94 handling arrangements on 4 November 2015;

b. from 4 November 2015 to the date of the hearing; and

c. as at the date of hearing?"

75. The s.94 regime was in accordance with law under Article 8(2) ECHR throughout the whole period under consideration. The regime was sufficiently foreseeable (for reasons given at §66(a) above) and subject to safeguards which provided adequate protection against arbitrary interference as set out below.

GCHQ

a. Prior to the avowal of the use of s.94 to obtain CD and the publication of the s.94 handling arrangements on 4 November 2015

Weber (1) and (2)

76. As noted by the Tribunal at §115 of *Liberty/Privacy*, *Weber* (1) and (2) overlap and therefore can be taken together. As noted in *RE v United Kingdom*, although sufficient detail should be provided of the nature of the offences in question, the condition of foreseeability does not require States to set out exhaustively by name the specific offences which may give rise to the activity (see §132). Consequently, terms such as *"national security"* are sufficient (see *RE* at §133 and §116 of the *Liberty/Privacy* judgment). In addition it was also accepted in *RE* that it may not be necessary to know in advance precisely what individuals will be affected eg by the surveillance measures in each case.

77. It is therefore submitted that the regime is sufficiently clear both as to the nature of the circumstances which may give rise to a s.94 direction in relation to BCD, and use of that data and the categories of person liable to be subject to such measures.

Weber (3) to (6)

78. The third to sixth *Weber* requirements are dealt with in the combination of the ISA, SSA, CTA, DPA, HRA, OSA and GCHQ's internal arrangements, together with the fact that GCHQ handles all operational data as if it had been obtained under RIPA, and accordingly applies the provisions of the Safeguards section of the Interception of Communications Code of Practice to all BCD datasets. Weber (3) to (6) are addressed here by reference to the headings set out at §6 of the Tribunal's order of 7 July 2016, namely "Access", "Use", "Disclosure", "Retention Period", "Review", "Destruction" and "Oversight", as well as by reference to "Acquisition".

Acquisition

79. A direction under s.94(1) can only be given where it *"appear[s] 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."* **[Auths/tab 1]** Further, the Secretary of State can only give such a direction if *"he believes that the conduct required by the direction is proportionate to what is sought to be achieved by that conduct."* Thus there are, and at all relevant times have been, safeguards in the form of *statutory requirements* that the giving of a s.94 direction must be, in the independent judgment of a Secretary of State, both **necessary** for one of the permitted purposes and **proportionate**.

80. Consultation with the CSP is also required under s.94(1). The Secretary of State will thus be informed of any material factors, including those relating to necessity and proportionality, which the CSP wishes to bring to his/her attention.

81. There are further statutory safeguards in relation to the acquisition of information, including BCD: see s.4(2)(a) of ISA 1994 **[Auths/tab 4]**, and the requirements of necessity and proportionality under the HRA **[Auths/tab 6]**.

82. In this period, GCHQ's internal arrangements were set out in its Compliance Guide, relevant extracts from which are set out at Appendix A, §§66-73. In relation to acquisition**,** the Compliance Guide emphasised and explained the requirements to consider the necessity and proportionality of the interference with privacy at the acquisition stage: see Appendix A, §67.

Access/Use

83. Any s.94 BCD can be used by GCHQ only in accordance with s.19(2) of the CTA **[Auths/tab 9]** as read with the statutory definition of GCHQ's functions (in s.3 of the ISA **[Auths/tab 4]**) and only insofar as that is proportionate under s.6(1) of the HRA **[Auths/tab 6]** (see Appendix A, §§7-8, 12, 19-22).

84. Pursuant to the DPA **[Auths/tab 5]**, GCHQ is not exempt from an obligation to comply with the seventh data principle, which provides:

> *"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."*

Accordingly when GCHQ obtains any s.94 BCD which amounts to personal data, it is obliged 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.

85. Further, GCHQ's Compliance Guide also made clear throughout the relevant period the requirements that access/use of BCD must be both necessary and proportionate: see Appendix A, §68-70.

Disclosure

86. A member of an intelligence service will commit an offence if he fails to take such care to prevent the unauthorised disclosure of any document or other article relating to security and intelligence which is in his possession by virtue of his position as a member of any of those services (see s.8(1) of the OSA read with s.1(1) **[Auths/tab 2]**). Conviction may lead to imprisonment of up to 3 months. Consequently this statutory obligation is relevant to the publicly available safeguards for the handling and security arrangements for s.94 BCD (see Appendix A, §28).

87. Members of the intelligence services could also be liable for misfeasance in public office if they acted unlawfully and with the necessary state of knowledge (see the constituent elements of the test as discussed in *Three Rivers DC v Bank of England (No. 3)* [2003] 2 AC 1 **[Auths/tab 32]** at §§191-194).

88. Finally any disclosure of such information must satisfy the constraints imposed in ss.3-4 of the ISA **[Auths/tab 4]**, as read with s.19(5) of the CTA **[Auths/tab 9]** and s.6(1) of the HRA **[Auths/tab 6]**. Thus specific statutory limits are imposed on the information that GCHQ can disclose.

89. In addition, the Compliance Guide set out strict safeguards requiring any **disclosure** to be necessary and proportionate: see Appendix A, §71. The safeguards set out in the Interception of Communications Code of Practice were also applied as a matter of policy: see Appendix A, §117.

Retention/review/destruction

90. Under the DPA **[Auths/tab 5]**, and in particular the fifth data protection principle (see Appendix A, §25) GCHQ is, and throughout the material period, has been obliged not to keep data, including BCD, for longer than is necessary having regard to the purposes for which the data has been obtained and are being retained / used.

91. In addition, the Compliance Guide included safeguards in relation to retention/review/destruction: see Appendix A, §72-73. These included clear statements that material should be destroyed "*as soon as it can be determined reasonably*

that its retention is no longer necessary". Time limits for retention were stated, which applied "*unless retention beyond that time can be justified, after review, in acceptable terms*" (*ibid.*); and "*Retention of material beyond these default periods must be formally approved. Continued retention must be reviewed and rejustified, in most cases annually.*" (Appendix A, §72(d)). The safeguards set out in the Interception of Communications Code of Practice were also applied as a matter of policy: see Appendix A, §117.

Oversight

92. At GCHQ, external oversight over the issuing of s.94 directions was conducted by Sir Swinton Thomas, the Interception of Communications Commissioner, between 2004 and 2006, and by the Intelligence Services Commissioner (Sir Peter Gibson, and subsequently Sir Mark Waller) between 2006 and 2015.

93. As a matter of practice in advance of each inspection visit the Commissioner was provided with a list setting out details of all the extant s.94 Directions and any that had been cancelled since the previous inspection. On the basis of the list the Commissioner selected one or more Directions. During the visit the Commissioner examined the relevant Direction or Directions, the applications to the Secretary of State for those Directions (which included the necessity and proportionality justifications), and the correspondence with the organisations on whom the Directions were served. Sessions were scheduled to give him the opportunity to question those members of GCHQ involved in applying for the relevant Direction or Directions, those responsible for putting them into effect, and analysts who made use of the data obtained under them. The Commissioner was also provided with information on the extent to which s.94 data contributed to intelligence reporting. The GCHQ witness statement set out details of the oversight provided by the Commissioners over s.94 BCD at §§133-152 **[Core/B/2]**.

94. As far as the *use* of s.94 data was concerned, it is important to bear in mind that BCD obtained by means of s.94 is and was held by GCHQ alongside CD obtained by means of interception under a s.8(4) warrant. Use of the *combined* data fell to be overseen by the Interception of Communications Commissioner. In addition, the Intelligence Services Commissioner considered the safeguards put in place to identify and address potential abuse of GCHQ's systems. Those systems included, but were not restricted to, those holding s.94 data.[41]

95. GCHQ's Compliance Guide referred to the external oversight of the Commissioner (see "Oversight" at **[2/GCHQ1/153; 15]**) and set out a process for handling

[41] See Respondents' Amended Response to Claimant's Supplement Request for Further Information and Disclosure, response to request 81 **[Core/A/9]**.

errors/non-compliance, and made clear that "*We are obliged to investigate them and report to our oversight authorities*": **[2/GCHQ1/152; 14]**.

> "*If you have any concern over legal compliance or you identify an error that could breach GCHQ's legal requirements or safeguards you should inform the relevant policy team straight away. The relevant policy team will help and advise, if necessary coordinating GCHQ's response.*"

96. Further, GCHQ's Compliance Guide, which contained the safeguards set out above which were applied to s.94 data, were approved by the Interception of Communications Commissioner and Intelligence Services Commissioner: see Compliance Guide for June 2005-2010 [**2/GCHQ1/113/§1**]. The Compliance Guide was reviewed again in 2013 by Sir Anthony May, as Interception of Communications Commissioner.

97. In addition, internal oversight was provided by means of audit processes: see Compliance Guide for June 2005-2010: **[2/GCHQ1/98-99]** ("the Responsibilities of Line Managers for Audit"]; and **[2/GCHQ1/132-134]** ("Auditing GCHQ's targeting")**;** for 2010 to June 2014: **[2/GCHQ1/149-150]** ("Audit") and for June 2014 onwards: **[2/GCHQ1/6-7]** and GCHQ witness statement, §127 and §60 **[Core/B/2]**.

b. from 4 November 2015 to the date of the hearing

98. On 4 November 2015, there were three material developments, namely:
    a. The avowal of the s.94 regime;
    b. The publication of s.94 Handling Arrangements[42] (common to all Intelligence Services), and
    c. The coming into force of the Closed GCHQ s.94 Handling Arrangements.[43]

Weber (1) and (2)

99. These criteria are satisfied for the same reasons given above in respect of the period pre-avowal on 4 November 2015 and in view of the avowal of the s.94 regime and the publication of the s.94 Handling Arrangements on 4 November 2015.

Weber (3) to (6)

100. The statutory safeguards referred to in the preceding section remain unchanged. However, in addition since 4 November 2015 the s.94 Handling Arrangements have applied to the acquisition, use and disclosure of BCD under s.94. They are mandatory

[42] **[2/GCHQ1/195-204].**
[43] **[2/GCHQ1/pp. 81-88].**

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). The key provisions are set out at Appendix A, §§87-108, but in summary, they provide detailed arrangements for each of the stages of the lifecycle of s.94 BCD, including:

(a) Acquisition: Appendix A, §§93-96;
(b) Access/use: *ibid.* §§97-98;
(c) Disclosure: *ibid.* §§99-102;
(d) Retention/review/deletion: *ibid.* §103; and
(e) Oversight: *ibid.* §§104-108.

101. In addition, GCHQ has additional "*below the waterline*" arrangements which also came into force on 4 November 2015. These are available to the Tribunal in CLOSED evidence, but as a result of the disclosure process in these proceedings, a partly disclosed/gisted version is also available in OPEN: see **[2/GCHQ1/81-88]**. The "*below the waterline*" arrangements essentially reflect and supplement the s.94 Handling Arrangements, albeit with specific reference to GCHQ.

102. GCHQ's Compliance Guide also remains in force. The most recent versions of the applicable sections of the Compliance Guide are set out in Appendix A, §§67-73. The safeguards set out in the Interception of Communications Code of Practice were also applied as a matter of policy: see Appendix A, §117.

c. as at the date of hearing

Weber (1) to (6)

103. The position as at the date of the hearing is essentially the same as that since avowal, save that (i) GCHQ's "*below the waterline*" handling Arrangements are formally in evidence, and thus public; and (ii) the s.94 Regime is under the scrutiny of the Tribunal.

Security Service

a. Prior to the avowal of the use of s.94 to obtain communications data and the publication of the s.94 handling arrangements on 4 November 2015

Weber (1) and (2)

104. Weber (1) and (2) are satisfied in relation to MI5 for the same reasons as given in relation to GCHQ at §§76-77 above.

Weber (3) to (6)

Acquisition

105. As stated above (at §§79-80 above) in respect of GCHQ, s.94(1) itself contains statutory safeguards requiring that the giving of a s.94 direction be, in the independent judgment of a Secretary of State, both necessary and proportionate. Consultation with the CSP is also required under s.94(1). The Secretary of State will thus be appraised of any material factors, including those relating to necessity and proportionality, which the CSP wishes to bring to his/her attention.

106. As a matter of regular practice, the Security Service has provided updates/briefings to the Home Secretary in relation to the database.[44]

107. There are further statutory safeguards in relation to the acquisition of information, including BCD: see s.2(2)(a) of SSA **[Auths/tab 3]**, and the requirements of necessity and proportionality under the HRA **[Auths/tab 6]**.

Access/Use

108. As set out above in relation to GCHQ, any s.94 BCD can be used by MI5 only in accordance with s.19(2) of the CTA **[Auths/tab 9]** as read with the statutory definition of MI5's functions (in s.1 of the SSA **[Auths/tab 3]**) and only insofar as that is proportionate under s.6(1) of the HRA **[Auths/tab 6]** (see Appendix A, §§5, 12, 19-22).

109. Pursuant to the DPA **[Auths/tab 5]**, MI5 is not exempt from an obligation to comply with the seventh data principle, which provides:

> *"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."*

110. Accordingly when MI5 obtains any s.94 BCD which amounts to personal data, it is obliged 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.

111. In addition, as explained at §130 of the MI5 statement **[Core/B/2]**, the authorisation process for access to the database was from the outset the same as for requests to CSPs for CD under Part 1 Chapter II of RIPA. As a matter of practice and policy, MI5 has applied the

[44] MI5 statement, §117 **[Core/B/2]**.

applicable Codes of Conduct for the acquisition of communications data to the regime that it has operated for access to the database. In particular, investigators would – when completing requests for CD – be expected to comply with applicable parts of the Code of Practice relating to the acquisition of CD: see Appendix A, §§112-116.

112. Further, from 31 March 2006 (prior to the database becoming operational and functional in May 2006: MI5 statement, §120 **[Core/B/2]**) onwards internal guidance was in place in relation to authorisation of access to the database: see Appendix A, §§74-75.

113. It is also important to note that since the database became operational in May 2006 access to it has required authorisation to be granted through an electronic system for processing CD requests. This is explained at §§121-123 of the MI5 statement **[Core/B/2]**:

> *"121. Access to the data in the database is controlled – technically – in such a way that requests of the database can only take effect if an authorisation is granted through the electronic system for processing CD requests. Accordingly, although our internal CD guidance (see further below) also refers to the possible use of forms for the making of CD requests, access to the database would additionally require processing a request (dealt with on paper) on the electronic system.*
>
> *122. The electronic authorisation process that we have used to enable requests to be made of the database has been in place from when the database was first commissioned and used in May 2006 and is the same electronic system as is used for all CD requests that require CSP action. Thus, an investigator or analyst will always need to use MI5's electronic system for the processing of CD requests, whether that CD request is then answered by interrogation of the database of BCD or whether that request is then forwarded to the CSP.*
>
> *123. All CD requests (whether through the electronic system or on paper) require a necessity and proportionality justification."*

114. Thus throughout the entire operational lifetime of the database the requirement to obtain authorisation for access, and to complete necessity and proportionality justifications, has been integrated into the Security Service's systems.

Retention/review/destruction

115. Under the DPA **[Auths/tab 5]**, and in particular the fifth data protection principle (see Appendix A, §25) MI5 is, and throughout the material period, has been obliged not to keep data, including BCD, for longer than is necessary having regard to the purposes for which the data has been obtained and are being retained / used.

116. The appropriate retention period was initially six months, before being revised upwards, and then fixed in November 2009 at one year. Any data that is older than one year was automatically deleted: see Appendix A, §86.

Disclosure

117. As set out above,

a. A member of an intelligence service will commit an offence if he fails to take such care to prevent the unauthorised disclosure of any document or other article relating to security and intelligence which is in his possession by virtue of his position as a member of any of those services (see s.8(1) of the OSA read with s.1(1) **[Auths/tab 2]**). Conviction may lead to imprisonment of up to 3 months. Consequently this statutory obligation is relevant to the publicly available safeguards for the handling and security arrangements for s.94 BCD (see Appendix A, §28).
b. Further, members of the intelligence services could also be liable for misfeasance in public office if they acted unlawfully and with the necessary state of knowledge: see *Three Rivers DC v Bank of England (No. 3)* [2003] 2 AC 1 **[Auths/tab 32]** at §§191-194.
c. Finally any disclosure of such information must satisfy the constraints imposed in ss.1-2 of the SSA **[Auths/tab 3]**, as read with s.19(3) of the CTA **[Auths/tab 9]** and s.6(1) of the HRA **[Auths/tab 6]**. Thus specific statutory limits are imposed on the information that MI5 can disclose. Further, the Acquisition and Disclosure of Communications Data Code of Practice applied, as a matter of practice and policy, to disclosure of s.94 BCD: see Appendix A, §§112-116.

Oversight

118. The database became operational in May 2006 and, following the pilot phrase, became fully adopted in October 2006.[45] Oversight from that period until avowal in November 2015 involved the Interception Commissioner (Sir Paul Kennedy, Sir Anthony May, and, most recently, IOCCO inspectors on the Commissioner's behalf) overseeing samples of requests for authorisation for access to the database and the related authorisations. [46]

119. In January 2015 the Prime Minister asked Sir Anthony May to extend his oversight of MI5's database capability. In particular, it was agreed that the Commissioner's oversight would be extended to cover the issuing, by the Secretary of State, of the s.94 directions and of MI5's storage and destruction arrangements for the data.

120. In addition, there is a system of internal oversight at MI5: see MI5 internal handling arrangements, §§4.6.1-4.6.3.[47] This has existed since September 2009.

---

[45] See MI5 statement, §136 [**Core/B/2**].
[46] See MI5 statement, §§135-140 **[Core/B/2]**; see also the Respondents' Amended Response to the Claimant's Supplemental Request for Further Information and Disclosure, response to request 88 **[Core/A/9]**.
[47] **[1/MI51/174]**

b. from 4 November 2015 to the date of the hearing

Weber (1) to (6)

121. The submissions made in respect of GCHQ at §§100-101 above apply equally to MI5. For the Tribunal's reference, MI5's *"below the waterline"* handling arrangements from 4 November 2015 are at **[1/MI51/163-175]**. See also the additional internal guidance referred to at Appendix A, §111.

c. as at the date of hearing

Weber (1) to (6)

122. As in relation to GCHQ, the position as at the date of the hearing is essentially the same as that since avowal, save that (i) MI5's *"below the waterline"* handling Arrangements are formally in evidence, and thus public; and (ii) the s.94 Regime is under the scrutiny of the Tribunal.

Conclusion on Issue 2

123. For the reasons given above, the section 94 regime was in accordance with law under Article 8(2) ECHR in all of the periods under consideration.

ISSUE 3:

124. Issue 3 on the Amended Agreed List of Issues [**Core/A/10**] states:

> *"Is or was the BPD Regime in accordance with the law under Article 8(2) ECHR:*
> *a. prior to the avowal of BPDs in the ISC's Privacy and Security report on 12 March 2015;*
> *b. from 12 March 2015 until the publication of the BPD Handling Arrangements on 4 November 2015;*
> *c. from 5 November 2015 to the date of the hearing; and*
> *d. as at the date of hearing?"*

125. The BPD regime was in accordance with law under Article 8(2) ECHR throughout the whole period under consideration. The regime was sufficiently foreseeable (for reasons given at §66(b) above) and subject to safeguards which provided adequate protection against arbitrary interference as set out below.

Government Communications Headquarters

a. prior to the avowal of BPDs in the ISC's Privacy and Security report on 12 March 2015

Weber (1) & (2)

126. These requirements overlap and can be taken together, as above (at §76) in relation to the section 94 Regime.

127. BPDs are obtained either from providers on a voluntary basis, or are obtained by means of RIPA/ISA powers. In either case, the **purpose** for their acquisition was at the material times defined by the SIAs' statutory functions, read with the Counter-Terrorism Act 2008 (see Appendix B, §§4-18). In the case of BPDs obtained under RIPA or ISA powers, the bases for such acquisition were set out in the relevant RIPA/ISA authorising sections[48], again read with the SIAs' statutory functions, and in the statutory Codes of Practice (see Appendix, §75).

128. Thus the BPD regime was sufficiently clear both as to the nature of the circumstances which may give rise to the acquisition/use of BPD, and the categories of person liable to be subject to such measures.

Weber (3) to (6)

129. The third to sixth *Weber* requirements are dealt with in the combination of the ISA, SSA, CTA, DPA, HRA, OSA, the relevant Codes of Practice and GCHQ's internal arrangements. They are addressed here by reference to the headings set out at §6 of the Tribunal's order of 7 July 2016, namely "Access", "Use", "Disclosure", "Retention Period", "Review", "Destruction" and "Oversight", as well as by reference to "Acquisition".

Acquisition

130. Acquisition of BPDs was subject to necessity and proportionality safeguards set out in (i) the relevant RIPA/ISA powers (in cases of covert acquisition of BPDs) and the relevant Codes of Practice: see Appendix B, §75 and; (ii) GCHQ's internal arrangements: see Appendix B, §78. In addition, from February 2015 a joint SIA BPD Policy came into force which included safeguards relating to acquisition: see Appendix B, §120.

[48] See Appendix B, §19.

Access/Use

131. Any BPDs can be used by GCHQ only in accordance with s.19(2) of the CTA **[Auths/tab 9]** as read with the statutory definition of GCHQ's functions (in s.3 of the ISA **[Auths/tab 4]**) and only insofar as that is proportionate under s.6(1) of the HRA **[Auths/tab 6]** (see Appendix B, §§9-10**,** 14, 21-24).

132. Pursuant to the DPA **[Auths/tab 5]**, GCHQ is not exempt from an obligation to comply with the seventh data principle, which provides:

> *"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."*

Accordingly, when GCHQ obtains any BPDs it is obliged 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.

133. Further, GCHQ's Compliance Guide also made clear throughout the relevant period the requirements that access/use must be both necessary and proportionate: see Appendix B, §§79-80. In addition, from February 2015 the joint SIA BPD Policy applied, and included safeguards relating to use: see Appendix B, §120.

Disclosure

134. A member of an intelligence service will commit an offence if he fails to take such care to prevent the unauthorised disclosure of any document or other article relating to security and intelligence which is in his possession by virtue of his position as a member of any of those services (see s.8(1) of the OSA read with s.1(1) **[Auths/tab 2]**). Conviction may lead to imprisonment of up to 3 months. Consequently this statutory obligation is relevant to the publicly available safeguards for the handling and security arrangements for BPD (see Appendix B, §§29-30).

135. Members of the intelligence services could also be liable for misfeasance in public office if they acted unlawfully and with the necessary state of knowledge (see the constituent elements of the test as discussed in *Three Rivers DC v Bank of England (No. 3)* [2003] 2 AC 1 **[Auths/tab]** at §§191-194).

136. Finally any disclosure of such information must satisfy the constraints imposed in ss.3-4 of the ISA **[Auths/tab 32]**, as read with s.19(5) of the CTA **[Auths/tab 9]** and s.6(1) of the

HRA **[Auths/tab 6]**. Thus specific statutory limits are imposed on the information that GCHQ can disclose.

137. In addition, the Codes of Practice and GCHQ's Compliance Guide set out strict safeguards relating to **disclosure**: see Appendix B, §§75 and 81. In addition, from February 2015 the joint SIA BPD Policy applied, and included safeguards relating to disclosure/sharing: see Appendix B, §120.

Retention/Review/Destruction

138. Under the DPA **[Auths/tab 5]**, and in particular the fifth data protection principle (see Appendix B, §27) GCHQ is, and throughout the material period, has been obliged not to keep data, including BPD, for longer than is necessary having regard to the purposes for which the data has been obtained and are being retained / used.

139. In addition, the relevant Codes of Practice and GCHQ's Compliance Guide included safeguards in relation to retention/review/destruction: see Appendix B, §§75 and 82-83. These included clear statements that material should be destroyed "*as soon as it can be determined reasonably that its retention is no longer necessary*" . Time limits for retention were stated, which applied "*unless retention beyond that time can be justified, after review, in acceptable terms*" (*ibid.*); and "*Retention of material beyond these default periods must be formally approved. Continued retention must be reviewed and rejustified, in most cases annually.*" (Appendix A, §82(a)-(b)). In addition, from February 2015 the joint SIA BPD Policy applied, and included safeguards relating to retention/review/destruction: see Appendix B, §120.

Oversight

140. The Intelligence Services Commissioner has provided independent oversight of GCHQ's handling of BPDs since 2010, following the Prime Minister's request that the Commissioner take on oversight of each of the SIAs' use of BPDs on a non-statutory footing.

141. At GCHQ the Commissioner inspected BPD twice each year, selecting which BPDs he wished to focus on from a full list of all current BPDs held by GCHQ. He checked that the documentation was in order, gave a good case for acquisition and retention of the dataset including necessity, proportionality and risk of collateral intrusion. He also made clear the need for full deletion of a dataset when it was no longer required and for proper recording of the deletion. He also discussed the operational use of those BPDs he had selected with those who own the dataset, and asks questions particularly around the issues of necessity, proportionality and collateral intrusion. The Commissioner looked at the overall use and purpose of the data rather than specific requests made of the data.

142. See the GCHQ witness statement, §§67-101 **[Core/B/2]** and responses to requests 56 to 72 in the Respondent's Amended Response to the Claimants' Supplemental Request for Further Information and Disclosure **[Core/A/9]**.

143. In addition, there was internal oversight of BPDs within GCHQ: see the GCHQ statement, para. 10 **[Core/B/2]**.

b. from 12 March 2015 until the publication of the BPD Handling Arrangements on 4 November 2015

Weber (1) & (2)

144. These criteria are satisfied for the same reasons given above in respect of the period prior to avowal on 12 March 2015 and because avowal of the use of BPDs provided more relevant detail about BPDs, and in particular the categories of persons affected by use of BPDs. In particular, the ISC's report *"Privacy and Security: A modern and accountable legal framework"* **[Auths/tab 79]** made clear that BPDs contain *"personal information about a wide range of people"* (p.9) but that they are used to identify subjects of interest, establish links between individuals and groups and improve understanding of a target's behaviour and connections, and to verify information obtained from other sources (*ibid.*, p.55).

Weber (3) to (6)

145. The safeguards derived from statute, common law, relevant Codes of Practice, joint SIA BPD Policy and GCHQ's internal arrangements set out at §§129-143 above continued to be applicable in this period. Further, on 11 March 2015 the existing oversight by the Intelligence Services Commissioner over BPDs was put on a statutory footing under a direction issued by the Prime Minister.[49] This directed the Commissioner (at §§3-4) to:

> *"continue to keep under review the acquisition, use, retention and disclosure by the Security Service, the Secret Intelligence Service and the Government Communications Headquarters ("the Security and Intelligence Agencies") of bulk personal datasets, as well as the adequacy of safeguards against misuse."*
>
> *"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. As part of this, the*

[49] The Intelligence Services Commissioner (Additional Review Functions) (Bulk Datasets) Direction 2015 **[Auths/tab 16]** and **[2/SIS/135-136]**.

Intelligence Services Commissioner must seek to assure himself of the adequacy of the Security and Intelligence Agencies' handling arrangements and their compliance therewith."

c. from 5 November 2015 to the date of the hearing

Weber (1) & (2)

146. These criteria are satisfied for the same reasons given above in respect of the period between avowal and 4 November 2015.

Weber (3) to (6)

147. The statutory safeguards referred to in the preceding section remain unchanged. However, in addition, since 4 November 2015, the BPD Handling Arrangements[50] (common all Intelligence Services) have applied to the acquisition, use and disclosure of BPD. 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). The key provisions are set out at Appendix B, §§129-157, but in summary, they provide detailed arrangements for each of the stages of the lifecycle of BPD, including:

(f) Acquisition: Appendix B, §§135-141;

(g) Access/use: *ibid.* §§142-144;

(h) Disclosure: *ibid.* §§145-148;

(i) Retention/review/deletion: *ibid.* §§149-154; and

(j) Oversight: *ibid.* §§155-157.

148. In addition, GCHQ has additional *"below the waterline"* arrangements which also came into force on 4 November 2015. These are available to the Tribunal in CLOSED evidence, but as a result of the disclosure process in these proceedings, a partly disclosed/gisted version is also available in OPEN: see **[2/GCHQ1/71-80]**. The *"below the waterline"* arrangements essentially reflect and supplement the BPD Handling Arrangements, albeit with specific reference to GCHQ.

149. GCHQ's Compliance Guide also remains in force. The most recent versions of the applicable sections of the Compliance Guide are referred to in Appendix B, §159**.**

[50] **[2/GCHQ1/183-193]**

d. as at the date of hearing?

Weber (1) to (6)

150. The position as at the date of the hearing is essentially the same as that immediately before the hearing, save that (i) GCHQ's *"below the waterline"* handling Arrangements are formally in evidence, and thus public; and (ii) the BPD Regime is under the scrutiny of the Tribunal.

Security Service

a. prior to the avowal of BPDs in the ISC's Privacy and Security report on 12 March 2015

Weber (1) & (2)

151. These criteria were satisfied in relation to MI5 for the same reasons as given in respect of GCHQ at §§126-128 above.

Weber (3) to (6)

Acquisition

152. Acquisition of BPDs was subject to necessity and proportionality safeguards set out in (i) the relevant RIPA/ISA powers (in cases of covert acquisition of BPDs) and the relevant Codes of Practice: see Appendix B, §75 and; (ii) MI5's internal arrangements: see Appendix B, §85-90.[51] In addition, from February 2015 a joint SIA BPD Policy came into force which included safeguards relating to acquisition: see Appendix B, §120.

Access/Use

153. In the relevant period, BPDs could be accessed/used by MI5 only in accordance with s.19(2) of the CTA **[Auths/tab 9]** as read with the statutory definition of MI5's functions and only insofar as that is proportionate under s.6(1) of the HRA **[Auths/tab 6]** (see Appendix B, §§4-5, 14, 21-24). MI5 was also obliged to comply with the seventh data principle, as set out in respect of GCHQ at §132 above. Further, MI5's internal arrangements set out clear safeguards in relation to necessity and proportionality: see Appendix B, §91. In addition,

[51] The MI5 statement **[Core/B/2]** notes at §77 that from Autumn 2013 BPDs acquired covertly under RIPA/ISA powers should be included within the BPD regime. The effect from that time onwards was that such BPDs are subject both to the Codes of Practice and to MI5's internal arrangements.

from February 2015 the joint SIA BPD Policy applied, and included safeguards relating to use: see Appendix B, §120.

Disclosure

154. The safeguards set out at §§134-136 above in respect of GCHQ also applied to MI5.[52] In addition, the Codes of Practice and MI5's internal arrangements set out strict safeguards in relation to disclosure, as did the joint SIA BPD Policy in force from February 2015: see Appendix B, §§75, 92-93 and 120.

Retention/Review/Destruction

155. MI5 was also obliged to comply with the fifth data principle, as set out in respect of GCHQ at §138 above. In addition, the relevant Codes of Practice and MI5's internal arrangements included safeguards in relation to retention/review/destruction, as did the joint SIA BPD Policy in force from February 2015: see Appendix B, §§75, 94-99 and 120.

Oversight

156. As stated above, in 2010 the Prime Minister asked the Intelligence Services Commissioner to provide independent oversight of each of the SIAs' use of BPDs on a non-statutory footing. The MI5 statement **[Core/B/2]** sets out (at §§99-101) the nature of that oversight.

b. from 12 March 2015 until the publication of the BPD Handling Arrangements on 4 November 2015

Weber (1) & (2)

157. These criteria were satisfied for the same reasons as given in respect of GCHQ at §144 above.

Weber (3) to (6)

158. The safeguards derived from statute, common law, statutory Commissioner oversight, relevant Codes of Practice, joint SIA BPD Policy and MI5's internal arrangements referred to at §§152-156 above continued to be applicable in this period.

[52] Save that the relevant sub-section of s.19 CTA in the context of MI5 is s.19(3), not s.19(5) **[Auths/tab 9]**.

c. from 5 November 2015 to the date of the hearing

Weber (1) to (6)

159. These criteria were satisfied for the same reasons as given in respect of GCHQ at §§146-149 above apply equally to MI5. For the Tribunal's reference, MI5's *"below the waterline"* handling arrangements from 4 November 2015 are at **[1/MI51/101-114]**. See also Appendix B, §160.

d. as at the date of hearing?

Weber (1) to (6)

160. The position as at the date of the hearing is essentially the same as that immediately before the hearing, save that (i) MI5's *"below the waterline"* handling Arrangements are formally in evidence, and thus public; and (ii) the BPD Regime is under the scrutiny of the Tribunal.

Secret Intelligence Service

a. prior to the avowal of BPDs in the ISC's Privacy and Security report on 12 March 2015

Weber (1) & (2)

161. These criteria were satisfied in relation to SIS for the same reasons as given in respect of GCHQ at §§126-128 above.

Weber (3) to (6)

Acquisition

162. Acquisition of BPDs was subject to necessity and proportionality safeguards set out in (i) the relevant RIPA/ISA powers (in cases of covert acquisition of BPDs) and the relevant Codes of Practice: see Appendix B, §75 and; (ii) SIS's internal arrangements: see Appendix B, §101-107. In addition, from February 2015 a joint SIA BPD Policy came into force which included safeguards relating to acquisition: see Appendix B, §120.

Access/Use

163. In the relevant period, BPDs could be accessed/used by SIS only in accordance with s.19(2) of the CTA **[Auths/tab 9]** as read with the statutory definition of SIS's functions and

only insofar as that is proportionate under s.6(1) of the HRA (see Appendix B, §§6-8, 14, 21-24). SIS was also obliged to comply with the seventh data principle, as set out in respect of GCHQ at §132 above. Further, SIS's internal arrangements set out clear safeguards in relation to necessity and proportionality: see Appendix B, §108-113. In addition, from February 2015 the joint SIA BPD Policy applied, and included safeguards relating to use: see Appendix B, §120.

Disclosure

164. The safeguards set out at §§134-136 above in respect of GCHQ also applied to SIS.[53] In addition, the Codes of Practice, joint SIA BPD Policy and SIS's internal arrangements set out strict safeguards in relation to disclosure: see Appendix B, §§75, 114-116 and 120.

Retention/Review/Destruction

165. SIS was also obliged to comply with the fifth data principle, as set out in respect of GCHQ at §138 above. In addition, the relevant Codes of Practice and SIS's internal arrangements included safeguards in relation to retention/review/destruction as did the joint SIA BPD Policy in force from February 2015: see Appendix B, §§75, 117-118 and 120.

Oversight

166. As stated above, in 2010 the Prime Minister asked the Intelligence Services Commissioner to provide independent oversight of each of the SIAs' use of BPDs on a non-statutory footing. The SIS statement **[Core/B/2]** sets out (at §58) the nature of that oversight.

b. from 12 March 2015 until the publication of the BPD Handling Arrangements on 4 November 2015

Weber (1) & (2)

167. These criteria were satisfied for the same reasons as given in respect of GCHQ at §144 above.

Weber (3) to (6)

168. The safeguards derived from statute, common law, statutory Commissioner oversight, relevant Codes of Practice, joint SIA BPD Policy and SIS's internal arrangements set out at §§162-166 above continued to be applicable in this period.

[53] Save that the relevant sub-section of s.19 CTA in the context of SIS is s.19(4), not s.19(5).

c. from 5 November 2015 to the date of the hearing

Weber (1) to (6)

169. The submissions made in respect of GCHQ at §§146-149 above apply equally to SIS. For the Tribunal's reference, SIS's *"below the waterline"* handling arrangements from 4 November 2015 are at **[2/SIS/65-78]**. See also Appendix B, §161.

d. as at the date of hearing?

Weber (1) to (6)

170. The position as at the date of the hearing is essentially the same as that immediately before the hearing, save that (i) SIS's *"below the waterline"* handling Arrangements are formally in evidence, and thus public; and (ii) the BPD Regime is under the scrutiny of the Tribunal.

Conclusion on Issue 3

171. For the reasons given above, the BPD regime was in accordance with law under Article 8(2) ECHR in all of the periods under consideration.

ISSUE 4:

172. Issue 4 on the Amended Agreed List of Issues [**Core/A/10**] states:

> *"Is and was the BPD Regime and the section 94 Regime proportionate under Article 8(2) ECHR:*
> *a. (for BPD) prior to the avowal of BPDs in the ISC's Privacy and Security report on 12 March 2015;*
> *b. (for BPD) from 12 March 2015 until the publication of the BPD Handling Arrangements on 4 November 2015;*
> *c. (for section 94) prior to the avowal of the use of section 94 to obtain communications data and the publication of the section 94 handling arrangements on 4 November 2015;*
> *d. (for both section 94 and BPD) from 4 November 2015 to the date of the hearing; and*
> *e. (for both section 94 and BPD) as at the date of hearing?"*

173. There are considerable limits on the Respondents' ability to address in OPEN the matters which are relevant to an assessment of the proportionality of their activities. However the following brief OPEN submissions are made at this stage.

174. As is made clear eg. in *Leander v Sweden* **[Auths/tab 47]**, in the field of national security the Government has a wide margin of appreciation in assessing the pressing social need and in choosing the means for achieving the legitimate aim of protecting national security (see §§58-59 and see also the Tribunal's conclusions in *Liberty/Privacy* **[Auths/tab 38]** at §§33-39).

175. As explained in detail in the MI5 witness statement **[Core/B/2]** at §§6-33 the threat from international terrorism throughout the relevant period, from the July 2005 London transport attacks onwards, has been significant. The current threat level is SEVERE. Serious threats are also posed by hostile states and serious and organised crime (§§18-21). Developments in technology, in particular the increasing use of encryption (§§22-33), and the increased difficulty in intercepting communications, make other capabilities, such as BCD and BPD, much more important to the SIAs.

176. There is a clear value to **BCD** obtained by s.94 directions:

a. For GCHQ: "*The specific value of communications data obtained form CSPs under section 94 direction is that it provides more comprehensive coverage than is possible by means of interception under section 8(4) of RIPA*" (GCHQ statement **[Core/B/2]**, §115). This provides "*a higher level of assurance that it can identify e.g. patterns of communications than it could be means of interception alone.*" (*ibid.*). Examples of the usefulness of BCD to GCHQ's activities are set out at §§120 of the GCHQ statement (e.g. enabling GCHQ to "tip off" the Security Service when a subject of interest arrives in the UK), and §§155-162 (e.g. where an analysis of BCD assisted in identifying a terrorist group and understanding the links between members in a way which "*would not have been possible…at speed by relying on requests for targeted communications data*" (§156); see also §159 for an example involving the disruption of a bomb plot against multiple passenger aircraft).
b. The MI5 statement **[Core/B/2]** also emphasises the need for a database of BCD: "*in complex and fast-moving investigations, having access to a database of BCD would enable MI5 to carry out more sophisticated and timely analysis, by joining the dots in a manner that would not be possible through individual CD requests made to CSPs.*" (MI5 statement, §110). See also *ibid.*, §§152-3, and the emphasis on the speed of BCD techniques compared with other techniques.

177. It is also important to note that the BCD capability in fact leads to a significant *reduction* of the intrusion into privacy of individuals of no intelligence interest: GCHQ statement, §116; MI5 statement, §153. Analysis of BCD, and the resultant identification of patterns of communication and potential subjects of interest, enables specific individuals to be identified *without* having first to carry out more intrusive investigations into a wider range of individuals.

178. **BPD** is a highly important capability for each of the SIAs. Examples of its usefulness are given at:

a. MI5 witness statement **[Core/B/2]**, §38 (Al-Qaida operative identified from fragmentary information; searching a BPD, and matching with two others reduced possible candidates from 27,000 to one), §108;
b. GCHQ statement **[Core/B/2]**, §§16-18, §§106-114;
c. SIS statement **[Core/B/2]**, §8, §21 (identification of an individual planning to travel to Syria out of hundreds of possible candidates).

The speed of analysis as a result of the use of electronic BPDs is of particular importance: MI5 statement, §§39-40; §107; GCHQ statement, §111.

179. The BPD capability also significantly reduces the need for *more* intrusive techniques to be used. The MI5 statement gives an example of how searches of BPD enabled the identity of a suspect for whom a general description had been provided, but no name, to one strong match. More intrusive methods could then be justified *in respect of that individual alone*. Without BPD MI5's would have had to investigate a wider range of individuals in a more intrusive manner: MI5 statement **[Core/B/2]**, §108; see also GCHQ statement **[Core/B/2]**, §§107, 114; SIS statement **[Core/B/2]**, §17, §21.

180. Furthermore, the *electronic* nature of searches of BPD reduces the intrusion into privacy ("*any data which is searches but which does not produce a "hit" will not be viewed by the human operator of the system, but only searched electronically.*": MI5 statement **[Core/B/2]**, §48). In reality "*the personal data of the vast majority of persons on a BPD will never, in fact, be seen read or considered by MI5 because it will never feature as a search result.*" (*ibid.*, §105). See also the GCHQ Statement **[Core/B/2]**, §19 ("*Using BPD also enables the Intelligence Services to use their resources more proportionately because it helps them exclude potential suspects from more intrusive investigations.*" (§19)), and the example at §107.

181. It is therefore submitted that the Respondents' s.94 BCD and BPD activities are proportionate and have been throughout each of the relevant periods.

20 July 2016
Replacement skeleton with references served 25 July 2016

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