

[2014] UKIPTrib 13_77-H

Case Nos: IPT/13/77/H, IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH, IPT/13/204/CH

IN THE INVESTIGATORY POWERS TRIBUNAL

P.O. Box 33220
London
SW1H 9ZQ

Date: 05/12/2014

Before :

MR JUSTICE BURTON (PRESIDENT)

MR ROBERT SEABROOK QC

MRS JUSTICE CARR

THE HON CHRISTOPHER GARDNER QC

HIS HONOUR GEOFFREY RIVLIN QC

- -

Between :

Liberty (The National Council of Civil Liberties)	**First Claimant**
- and -	
The Government Communications Headquarters & Others	**Respondents**
- and -	
Privacy International	**Second Claimant**
- and -	
The Secretary of State for the Foreign and Commonwealth Office & Others	**Respondents**
- and -	
American Civil Liberties Union & Others	**Third Claimants**
- and -	

The Government Communications Headquarters & Others	**Respondents**
- and -	
Amnesty International Limited	**Fourth Claimant**
- and -	
The Security Service & Others	**Respondents**
- and -	
Bytes For All	**Fifth Claimant**
- and -	
The Secretary of State for Foreign and Commonwealth Affairs & Others	**Respondents**

- -
- -

Mr Matthew Ryder QC, Dr Eric Metcalfe and Mr Edward Craven (instructed by **James Welch of Liberty**) for the **First and Third Claimants and Others**
Mr Dan Squires and Mr Ben Jaffey (instructed by **Bhatt Murphy Solicitors**) for the **Second and Fifth Claimants**
Ms Kirsty Brimelow QC and Mr Jude Bunting (instructed by **Amnesty International Ltd**) for the **Fourth Claimant**
Mr James Eadie QC, Mr Ben Hooper and Mr Julian Milford (instructed by **the Treasury Solicitor**) for **All Respondents**
Mr Martin Chamberlain QC and Mr David Manknell (instructed by **the Treasury Solicitor**) as **Counsel to the Tribunal**

Hearing dates: 14, 15, 16, 17 & 18 July, 31 October and 5 December 2014

- -

Approved Judgment

I direct that pursuant to CPR PD 39A para 6.1 no official shorthand note shall be taken of this Judgment and that copies of this version as handed down may be treated as authentic.

.....

MR JUSTICE BURTON

Mr Justice Burton (President) :

1. This is the judgment of the Tribunal.

2. The Claimants before the Tribunal are all Non-Governmental Organisations working in the field of defending human rights at both the national and/or international levels. Three of them, Privacy International ("Privacy"), Liberty and Amnesty International Limited ("Amnesty") are based in the United Kingdom. The other organisations, which are named in the title to the action but which we do not need to identify separately in this judgment, are international organisations based in a variety of countries, including the United States, Canada, Egypt, Pakistan and Ireland. The case put forward by the various Claimants was shared out amongst the counsel representing them in order to make the best use of the five days of open hearing which had been set aside, and four counsel in the end made the various submissions on their behalf, Mr Matthew Ryder QC, leading counsel for Liberty and others, Mr Ben Jaffey and Mr Dan Squires on behalf of Privacy and Bytes For All, the Pakistani organisation, and Ms Kirsty Brimelow QC on behalf of Amnesty, in each case supported by further junior counsel and solicitors. The Respondents, variously named as The Secretary of State for Foreign and Commonwealth Affairs and for the Home Department and various other bodies, have all been represented by Mr James Eadie QC with Mr Ben Hooper and Mr Julian Milford, instructed by the Treasury Solicitor.

3. The Claimants' complaints allege the unlawfulness pursuant to Article 8 (and collaterally Article 10) of the European Convention of Human Rights ("the Convention") of certain assumed activities of the Security Service (also, and colloquially, known as MI5), the Secret Intelligence Service (and similarly also known as MI6) and the Government Communications Headquarters ("GCHQ"), which we shall collectively describe as the Intelligence Services or Respondents. All counsel cooperated to slim down what was a substantial set of bundles of papers and a considerable amount of argument into a five day hearing in which all the necessary and appropriate points on all sides were fully canvassed. We are grateful for the persuasiveness and succinctness of counsels' submissions. We have also been assisted by the contribution, both in writing and orally, of Counsel to the Tribunal, Mr Martin Chamberlain QC and Mr David Manknell.

4. The activities are, as we have put it, <u>assumed</u> for the purpose of the resolution of agreed issues which we shall explain below, for a number of reasons:

   i) The alleged conduct itself is not admitted by the Respondents. It falls to be considered as a result of allegations made by Mr Edward Snowden, a former contractor for the National Security Agency ("NSA") of the United States, by whom a very substantial quantity of documentation has been leaked and much put into the public domain. This has resulted in the Claimants asserting their belief that investigation of the Respondents would show that the Claimants' privacy has been unlawfully invaded. Hence the Tribunal's detailed scrutiny is at this stage carried out upon the basis of assuming the relevant allegations to be derived from Mr Snowden's leaks to be true. The set of assumed facts is set out below, and the arguments of law have proceeded on the basis of those assumed facts, which have enabled the main hearing to take place entirely in public without putting at risk any national security interest. Save for the

existence of two programmes in the United States called Prism and Upstream, which have been publicly admitted in the United States by the NSA, and for confirmation that GCHQ has obtained information from the United States Government that the United States Government obtained via Prism, none of the matters the subject of the assumed facts are admitted by the Respondents (i.e. they fall within the Neither Confirm Nor Deny ("NCND") policy to which we shall refer below), and are only assumed for the purposes of this hearing. Some further evidence has been put in by both Claimants and Respondents by way of background, which has not been subject to cross-examination, and which did not detract from the NCND policy nor the manner in which the hearing has been conducted.

ii) As for the Claimants, they have not needed to prove any of the activities, which are assumed to have occurred, and by virtue of which interference with their privacy has been assumed. This is consistent with the normal practice of this Tribunal, which enables claimants to bring claims without having the kind of arguable case which they would need to pursue a case in the High Court, and also with the jurisprudence of the European Court of Human Rights ("ECtHR"), which permits and encourages such hypothetical cases on the basis that if there has been an unlawful interference a claimant may have been a victim. Thus *locus* is established so as to permit "*general challenges to the relevant legislative regime*" (**Kennedy v United Kingdom** [2011] 52 EHRR 4 at paragraph 119) by those who are "*unable to demonstrate that the impugned measures had actually been applied to them*" (**Weber and Saravia v Germany** [2008] 46 EHRR SE5 at paragraph 78): see also **Liberty v United Kingdom** [2009] 48 EHRR 1 at paragraph 57.

5. The claim before us fell into two parts. The first part was in respect of what has been called the "*Prism issue*", i.e. referring to the NSA programme referred to above, or the "*Intelligence Sharing issue*" because it relates to the supply to the Respondents by the NSA of information, including information by way of communications intercepted either via Prism, or possibly via another programme called the "Upstream programme". The second part has been described as the "*alleged Tempora interception operation*", although there has been no admission or explanation as to what this alleged Tempora programme consists of, and the argument in fact has revolved around the operation by the Respondents of warrants under s.8(4) of the Regulation of Investigatory Powers Act 2000 ("RIPA") ("s.8(4) Warrants"). We prefer to use the description "*s.8(4) issue*" in describing this question, as the lawfulness or otherwise of what the Respondents have done does not depend upon the existence or methodology of "Tempora".

6. It is important to set these complaints into context. The actions of the Respondents, which are not suggested to be unlawful save in the respects alleged by reference to Article 8 of the Convention, to which we refer below, are all taken, or assumed to be taken, in the interests of national security, and at a time when, according to the most recent Annual Report to Parliament of the Intelligence and Security Committee of Parliament ("ISC"), the threat to the United Kingdom from international terrorism is 'Substantial', indicating that an attack is a strong possibility; this has been recently upgraded to 'Severe', meaning that an attack is highly likely. The Claimants accept that Convention jurisprudence recognises the need for states to defend themselves

and to introduce measures in support of national security, and that the concept, familiar within the confines of Article 8, of *accessibility* and *foreseeability*, of laws, rules and arrangements established by democracies in that regard may be approached differently from those situations where national security is not an issue. In particular, the Claimants accept that different forms of intelligence gathering do raise different privacy interests, and the hearing before us has included consideration of where and how to place and evaluate those before us.

7. After the five day public hearing, we held a one day closed hearing to consider certain matters which were, in the considered judgment of the Respondents, too confidential and sensitive for discussion in open court in the interests of preserving national security, and in accordance with our jurisdiction to hold such a closed hearing pursuant to Rule 9 of the Investigatory Powers Tribunal Rules 2000. As will appear, we considered in particular the arrangements, which Mr Eadie QC described during the public hearing as "*below the waterline*", regulating the conduct and practice of the Intelligence Services, in order to consider (i) their adequacy and (ii) whether any of them could and should be publicly disclosed in order to comply with the requirements of Articles 8 and 10 of the Convention as interpreted by the ECtHR, to which we will refer further below.

8. At that hearing, at which the Claimants were not represented, counsel for the Tribunal played a full part. We heard submissions, both oral and in writing, during and subsequent to the open hearing as to the role of counsel to the Tribunal and as to whether a Special Advocate should be appointed to represent the Claimants and be instructed by them. At our invitation, Counsel to the Tribunal made written submissions to us, which contained the following passage by way of distinguishing between the role of Special Advocate and Counsel to the Tribunal:

> "*15.1 A Special Advocate is appointed (normally, but not necessarily, pursuant to statute) to represent the interests of a party at hearings from which that party is excluded. A Special Advocate is required to be partisan. He or she makes such submissions (if any) as he considers will advance the interests of the excluded party. If the Special Advocate reaches the view that it would not advance the interests of the excluded party to make submissions at all (as has happened in a few cases), then the proper course is to decline to make submissions at all, even though this leaves the tribunal without assistance.*
>
> *15.2 Counsel to the Tribunal performs a different function, akin to that of amicus curiae. His or her function is to assist the tribunal in whatever way the tribunal directs. Sometimes (eg in relation to issues on which all parties are represented), the Tribunal will not specify from what perspective submissions are to be made. In these circumstances, counsel will make submissions according to his or her own analysis of the relevant legal or factual issues, seeking to give particular emphasis to points not fully developed by the parties. At other times (in particular where one or more interests are not represented), the Tribunal may invite its counsel to make submissions from a particular perspective (normally the*

> *perspective of the party or parties whose interests are not otherwise represented).*"

9. As the Tribunal had had the benefit of very full legal arguments on assumed facts at the open hearing, we gained a full understanding of the case as fully canvassed between counsel by reference to more than 140 legal authorities, including a substantial number of decisions of the ECtHR. We were and remain satisfied that the Tribunal thus fully appreciated the nature of the Claimants' case, and in any event that it could be and was assisted by the full, perceptive and neutral participation at the closed hearing of counsel to the Tribunal.

10. In their written submissions Counsel to the Tribunal put forward the following conclusions for consideration by the Tribunal:

> "*19.1 The role of counsel to the Tribunal is in principle distinct from that of Special Advocate. The function of the former is to assist the Tribunal by performing such functions as he or she is directed by the Tribunal to perform. The precise roles played by counsel to the Tribunal may therefore vary depending on the circumstances.*
>
> *19.2 However. in the present circumstances, there is a broad measure of agreement between the Claimants and the Respondents that counsel to the Tribunal can best assist the Tribunal by performing the following roles: (i) identifying documents, parts of documents or gists that ought properly to be disclosed;. (ii) making such submissions to the Tribunal in favour of disclosure as are in the interests of the Claimants and open justice; and (iii) ensuring that all the relevant arguments on the facts and the law are put before the Tribunal. In relation to (iii), the Tribunal will expect its counsel to make submissions from the perspective of the Claimants' interests (since the Respondents will be able to make their own submissions). If the Tribunal decides to receive closed oral evidence from one or more of the Respondent's witnesses, it may also direct its counsel to cross-examine them. In practice, the roles performed by counsel to the Tribunal at this stage of the current proceedings will be similar to those performed by a Special Advocate in closed material proceedings.*
>
> *19.3 If, at the closed hearing, the Tribunal concludes that the closed material relied upon by the Respondents could not be properly be made open, there will be no need for any more than one closed hearing: counsel to the Tribunal will be able to make submissions on the closed material. If, on the other hand, it concludes that the closed material relied upon by the Respondents could be disclosed to the parties. it will invite the Respondents to consent to such disclosure. If the Respondents agree, it will afford the parties an opportunity to make open submissions on the disclosed material. If the Respondents decline, it will give directions for* [a further] *open hearing . . .* "

The Tribunal considered and conclude that this was the correct analysis and approach. As will be seen, in the context of a closed hearing there were matters derived from the evidence in the closed hearing which the Respondents were prepared to consent to disclose, and there were no matters which the Tribunal considered should be disclosed which the Respondents declined to disclose. Written submissions by the parties and a further closed and open hearing then followed, and some further matters were disclosed voluntarily by the Respondents. Such open disclosures appear in paragraphs 46 and 47 and 126 below ("the Disclosures").

11. In the judgment which follows, we shall address in full the contentions which were made by the parties at the open hearings, and reach our conclusions on them. Save in respect of the Disclosures, it is only in limited respects, as referred to in paragraphs 54-55 and 138-139 below, that it has been necessary to refer to the closed hearings for the purposes of this judgment.

12. Before we set out the agreed factual assumptions or "*alleged factual premises*" in relation to the issues, we should clarify the position in respect of the Convention and the Agreed Issues listed before us. The questions for us have revolved around Article 8, which reads, under the Heading "*Right to Respect for Private and Family Life*", as follows:

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

Liberty, Privacy and Amnesty International also rely upon Article 10 "*Freedom of Expression*", on the basis that, as campaigning organisations, they are also entitled to the protection of that Article which primarily relates to the freedom of the press. It is common ground that, subject to one possible exception to which we shall return later, no different questions fall to be decided by reference to Article 10 than are raised by Article 8, and we shall therefore leave aside the matter of Article 10, which underlies Agreed Issues (ii), (iii), (vi) and (vii).

13. There were also certain of the Agreed Issues (Issue xii), (xiii) and (xiv) which were described as "*Issues of law relating to procedure*", and which, by agreement, have not fallen for decision at this hearing. They relate in part to the NCND policy, the importance of which is emphasised by the Respondents in the following paragraphs of their Open Response:

> "*5. Secrecy is essential to the necessarily covert work and operational effectiveness of the Intelligence Services, whose primary function is to protect national security. See e.g.* ***Attorney General v. Guardian Newspapers Ltd*** *(No.2)[1990] 1 AC 109, per Lord Griffiths at 269F.*

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

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

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

9. Further, the "neither confirm nor deny" principle would be rendered nugatory, and national security thereby seriously damaged, if every time that sensitive information were disclosed without authority (i.e. "leaked"), or it was alleged that there had been such unauthorised disclosure of such information, the UK Government were then obliged to confirm or deny the veracity of the information in question.

10. It has thus been the policy of successive Governments to adopt a neither confirm nor deny stance in relation to any information derived from any alleged leak regarding the activities or operations of the Intelligence Services insofar as that information has not been separately confirmed by an official statement by the UK Government. That long-standing policy is applied in this Open Response."

Because this hearing has been held on the basis of agreed assumed facts, it has not been necessary to address this policy or its consequences.

THE PRISM ISSUE

14. The *alleged factual premises* agreed for the purposes of the *Prism issue* (Issue (i)) are as follows:

> "*1. The US Government's "Prism" system collects foreign intelligence information from electronic communication service providers under US court supervision. The US Government's "upstream collection" programme obtains internet communications under US court supervision as they transit the internet.*
>
> *2. The Claimants' communications and/or communications data (i) might in principle have been obtained by the US Government via Prism (and/or, on the Claimants' case, pursuant to the "upstream collection" programme) and (ii) might in principle have thereafter been obtained by the Intelligence Services from the US Government. Thereafter, the Claimants' communications and/or communications data might in principle have been retained, used or disclosed by the Intelligence Services (a) pursuant to a specific request from the intelligence services and/or (b) not pursuant to a specific request from the intelligence services.*"

The issue itself is formulated as follows:

> "*In the light of factual premises (1) and (2) above, does the statutory regime as set out in paragraphs 36-76 of the Respondents' Open Response to the Claims brought by Liberty and Privacy satisfy the Art. 8(2) "in accordance with the law" requirement?*"

15. The following matters are also in practice agreed between the parties as part of the agreed assumptions:

i) The NSA has a lawful basis for targeted interception pursuant to s.702 of the Foreign Intelligence Surveillance Act 1978 (as amended) ("*FISA*"), and to Executive Order 12333, pursuant to which Prism and "Upstream" are lawfully sanctioned for "*the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information*". According to the NSA's 'Mission Statement' of 9 August 2013 "*the collection under . . . s.702 is the most significant tool in the NSA collection arsenal for the detection, identification and disruption of terrorist threats to the U.S. and round the world*": and according to the NSA's Director of Civil Liberties and Privacy Office Report of April 18, 2014 "*NSA is subject to rigorous internal compliance and external oversight*". For the purpose of this hearing the information assumed to be supplied to the Respondents by the NSA is assumed to have been lawfully obtained.

ii) The United States is the principal hub of the world's telecommunications system, and a very substantial quantity of the world's communications pass through the United States: thus for example an email sent by a sender in the UK to another email address in the UK may be routed via the United States.

iii) As set out in paragraph 11 of the Respondents' open Response:

> "*11. In order to pursue their statutory objectives, the Intelligence Services need to share intelligence with foreign Governments, including the US Government (with which the Intelligence Services have particularly close ties). Intelligence that foreign governments share with the Intelligence Services (on a strictly confidential basis) represents a significant proportion of the Intelligence Services' total store of intelligence on terrorists, organised criminals and others seeking to harm national security.*"

A British-US Communication Intelligence Agreement of 5 March 1946 which was marked "Top Secret", and remained so until its transfer to the National Archive in 2010, governs the arrangements between the British and United States authorities in relation to the exchange of intelligence information relating to "*foreign*" communications, defined by reference to countries other than the United States, the United Kingdom and the Commonwealth. In his witness statement Mr Charles Farr, the Director-General of the Office for Security and Counter Terrorism ("OSCT") at the Home Office since June 2007, says, after describing the threat from international terrorism, and quoting from the National Crime Agency's recent Strategic Assessment, that *"all of the most serious crime threats are transnational"*:

> "*20. . . It is highly unlikely that any government will be able to obtain all the intelligence it needs through its own activities. It is therefore vital for the UK Government to be able to obtain intelligence from foreign governments both to improve its understanding of the threats that the UK faces, and to gain the knowledge needed to counter those threats. . . .* [He refers to what is said in paragraph 11 of the open Response quoted above, and continues]. *This store of intelligence forms a critical resource for the Government in seeking to take preventative action to counter threats, and save lives.*"

16. The relief sought by the Claimants is summarised by Privacy as follows:

> "*(i) A declaration that the Secretary of State for the Foreign Office and/or the Secretary of State for the Home Office have unlawfully failed to ensure that there is in place a regime which complied with Article 8 and 10 ECHR governing the soliciting, receiving, storing and transmitting by UK authorities of private communications of individuals located in the UK which have been obtained by US authorities.*

> *(ii) A declaration that the soliciting, receipt, storage and transmission of such information by the Security Service, the Secret Intelligence Service and/or GCHQ is unlawful.*
>
> *(iii) An order that the Security Service, the Secret Intelligence Service and/or GCHQ will not solicit, receive, store or transmit such information unless and until such activities are governed by a legal regime which satisfies ECHR Art 8 and 10 and will destroy any material unlawfully obtained.*"

17. It is common ground that RIPA is not applicable to a case where there has not been interception of communications by the Respondents, but receipt of intercepted communications by the Respondents from the NSA derived from Prism or Upstream, which might, by dint of the degree of coverage by US interception, include intercepted product of an email which could have been sent and/or received in the United Kingdom.

18. The Respondents rely on the following statutory framework to permit them to receive and use such information:

i) S.1 of the Security Service Act 1989 ("SSA") provides in relevant part:

> "*(2) The function of [MI5] shall be the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means.*
> *(3) It shall also be the function of [MI5] to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands.*
> *(4) It shall also be the function of [MI5] to act in support of the activities of police forces, the National Crime Agency and other law enforcement agencies in the prevention and detection of serious crime*."

ii) The operations of MI5 are under the control of the Director-General, who is appointed by the Secretary of State (s. 2(1) of SSA). By s. 2(2)(a), it is the duty of the Director-General to ensure:

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

iii) Subject to s. 1(2) of the Intelligence Services Act 1994 ("ISA"), the functions of MI6 are, by s. 1(1):

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

persons."

iv) By s. 1(2) of ISA:

> "*The functions of [MI6] 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; or*
> *(c) in support of the prevention or detection of serious crime."*

v) The operations of MI6 are under the control of the Chief of the Intelligence Service, who is appointed by the Secretary of State (s. 2(1) of ISA). By s. 2(2)(a), it is the duty of the Chief of the Intelligence Service to ensure:

> *". . . that there are arrangements for securing that no information is obtained by [MI6] except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary—*
> *(i) for that purpose;*
> *(ii) in the interests of national security;*
> *(iii) for the purpose of the prevention or detection of serious crime; or*
> *(iv) for the purpose of any criminal proceedings. . ."*

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

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

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

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

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

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

ix) Thus, specific statutory limits are imposed on the information that each of the Intelligence Services can obtain, and on the information that each can disclose. Further, these statutory limits do not simply apply to the obtaining of information from other persons in the United Kingdom or to the disclosing of information to such persons: they apply equally to obtaining information from or disclosing information to persons abroad, including foreign intelligence agencies. In addition, the term "*information*" is a very broad one, and is capable of covering *e.g.* communications and communications data (otherwise referred to as 'metadata' or 'traffic data', to which we refer in paragraph 64(i) below) that a foreign intelligence agency may have obtained and passed to the Intelligence Services.

x) By s. 19(2) of the Counter-Terrorism Act 2008 ("CTA"):

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

xi) By s.19(3) and (4) of CTA it is provided that information obtained by, respectively, MI5 and MI6 for the purposes of any of its functions *"may be disclosed by it – (a) for the purpose of the proper discharge of its functions (b) in the interests of national security (c) for the purpose of the prevention or detection of serious crime, or (d) for the purpose of any criminal proceedings":* and there is a similar provision, but limited to (a) and (d), relating to GCHQ in s.19(5).

19. Mr Eadie emphasises that there are thus significant statutory limits imposed on the information that each of the Intelligence Services can obtain and disclose, which apply both to obtaining and disclosing information in the United Kingdom and to obtaining information from or disclosing it to persons abroad, including foreign intelligence agencies: and he points to the breadth of the definition of the term *"information"*, as referred to in paragraph 18(ix) above. Other relevant parts of the statutory framework upon which Mr Eadie relies are:

i) The Data Protection Act 1998 ("DPA"). Each of the Intelligence Services is a *"data controller"*, and is required by s.4(4) of the DPA to comply with the data protection principles in Part 1 of Schedule 1 to the DPA, subject to exemption by ministerial certificate, and are in any event not exempted from the obligation to comply with the fifth and seventh data protection principles, which provide:

> "*(5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes . . .*
>
> *(7) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*"

ii) A member of the Intelligence Services commits an offence under s.1(1) of the Official Secrets Act 1989 ("OSA") if *"without lawful authority he discloses any information, document or other article relating to security or intelligence which is, or has been, in his possession by virtue of his position as a member of any of those services"*. This disclosure can only be made with lawful authority if it is made in accordance with his official duty by virtue of s.7(1) of the OSA. Thus, Mr Eadie points out that disclosure of information by a member of the Intelligence Services in material breach of the relevant *"arrangements"* made under s.2(2)(a) of SSA or ISA or s.4(2)(a) of ISA would be a criminal offence, and there are other criminal obligations in relation to disclosure under the OSA.

iii) The Respondents are also bound by their obligations under s.6(1) of the Human Rights Act 1998, which, in relation to breach of Articles 8 and 10 of the Convention, is another positive obligation which can be enforced in a court, or in this case, in this Tribunal.

20. Thus the Intelligence Services can obtain information (including communications and communications data) from a foreign intelligence agency falling within their relevant remit, but by reference to *arrangements* for securing that the information is only obtained so far as necessary for one of the specified purposes (as set out in paragraph 18(ii), (v) and (vii) above), which purposes are identical to those specified for the obtaining of a warrant under s.8 of RIPA, and insofar as proportionate for that purpose pursuant to s.6(1) of the HRA.

21. The Claimants' response is their complaint that there is on the face of those statutes (except the DPA) no or no sufficient regulation as to the receipt/handling/retention/destruction of the information so supplied, such as there would be in respect of intercepted information obtained pursuant to a warrant under s.8 of RIPA (whether issued under s.8(1) or s.8(4)), with which we deal below, and that there is thus interference with the privacy of the correspondents whose communications are so accessed, without adequate protection under Article 8(2) ("*in accordance with the law*").

22. The Respondents rely upon significant oversight of the Intelligence Services as protection against arbitrary interference or unlawful use of powers by them. First there is oversight by the ISC, now regulated under the Justice and Security Act 2013 ("the JSA"). This is a Committee of Members of Parliament, from both Houses and cross-party, whose Chairman is Sir Malcolm Rifkind QC, a former Foreign Secretary. The ISC has, and exercises, wide powers, and the Government (including each of the Intelligence Services) must make available to the ISC information that it requests in the exercise of its functions, subject to a power of veto under certificate of the Secretary of State. It has a support staff with the highest level of security clearance, and must make an annual report to Parliament, and such other reports to Parliament as it considers appropriate.

23. On 17 July 2013 the ISC made a *"Statement on GCHQ's Alleged Interception of Communications under the US Prism Program"*. It had carried out an investigation, and it reached conclusions which it set out as follows:

"5. Our investigation has included scrutiny of GCHQ's access to the content of communications, the legal framework which governs that access, and the arrangements GCHQ has with its overseas counterparts for sharing such information. We have received substantive reports from GCHQ, including:

- *a list of counter-terrorist operations for which GCHQ was able to obtain intelligence from the US in any relevant area;*

- *a list of all the individuals who were subject to monitoring via such arrangements who were either believed to be in the UK or were identified as UK nationals;*

- *a list of every 'selector' (such as an email address) for these individuals on which the intelligence was requested;*

- *a list of the warrants and internal authorisations that were in place for each of these individuals being targeted;*

- *a number (as selected by us) of the intelligence reports that were produced as a result of this activity; and*

- *the formal agreements that regulated access to this material.*

We discussed the programme with the NSA and our Congressional counterparts during our recent visit to the United States. We have also taken oral evidence from the Director of GCHQ and questioned him in detail.

- *It has been alleged that GCHQ circumvented UK law by using the NSA's PRISM programme to access the content of private communications. From the evidence we have seen, we have concluded that this is unfounded.*

- *We have reviewed the reports that GCHQ produced on the basis of intelligence sought from the US, and we are satisfied that they conformed with GCHQ's statutory duties. The legal authority for this is contained in the Intelligence Services Act 1994.*

- *Further, in each case where GCHQ sought information from the US, a warrant for interception, signed by a Minister, was already in place, in accordance with the legal safeguards contained in the Regulation of Investigatory Powers Act 2000.*

Next Steps

> *6. Although we have concluded that GCHQ has not circumvented or attempted to circumvent UK law, it is proper to consider further whether the current statutory framework governing access to private communications remains adequate.*
>
> *7. In some areas the legislation is expressed in general terms and more detailed policies and procedures have, rightly, been put in place around this work by GCHQ in order to ensure compliance with their statutory obligations under the Human Rights Act 1998. We are therefore examining the complex interaction between the Intelligence Services Act, the Human Rights Act and the Regulation of Investigatory Powers Act, and the policies and procedures that underpin them, further. We note that the Interception of Communications Commissioner is also considering this issue."*

24. Secondly, the Respondents rely upon the important additional oversight afforded by the Interception of Communications Commissioner ("the Commissioner"), presently Sir Anthony May, formerly a Lord Justice of Appeal and President of the Queen's Bench Division, (although recently temporarily replaced during his indisposition by his predecessor Sir Paul Kennedy, also a former Lord Justice of Appeal and President of the Queen's Bench Division), appointed (for relevant purposes) under s.57(1) of RIPA, independent from Government and the Intelligence Services. He too has a staff to assist him with his functions, which include a constant review of the Intelligence Services, and he is under a duty by s.58(4) to make an annual report to the Prime Minister regarding the carrying out of his functions, which must be laid before Parliament. In his latest report (the 2013 Annual Report laid before Parliament on 8 April 2014), ("the Commissioner's Report") he included a section headed:

> *"8. Do British intelligence agencies receive from US agencies intercept material about British citizens which could not lawfully be acquired by intercept in the UK and vice versa and thereby circumvent domestic oversight regimes?*"

He set out his views (at paragraph 6.8.1-5) by reference to the assumption, which has also been made for the purposes of the case before us (paragraph 15(i) above) that the intercept material in question has been lawfully acquired by the United States Agencies. In the light of his own investigations, as there referred to, he answered his question in the negative. He concluded as follows:

> "*6.8.6 . . . information lawfully obtained by interception abroad is not necessarily available by interception to an interception agency here. In many cases it will not be available. If it is to be lawfully provided from abroad, it is sometimes appropriate for the interception agencies to apply explicitly by analogy the RIPA 2000 Part I principles of necessity and proportionality to its receipt here even though RIPA 2000 Part I does not strictly apply, because the interception did not take place in the UK by*

> *an UK agency. This is responsibly done in a number of appropriate circumstances by various of the agencies, and I am asked to review the consequent arrangements, although this may not be within my statutory remit."*

25. All parties before us accept, and indeed assert, that, by reference to the jurisprudence of the ECtHR, the interference under Article 8 is not to be judged on exactly the same basis in relation to the receipt by the Respondents of product which has already been intercepted by another party as it is when the Respondents are responsible for such interception. The Claimants submit that the Respondents fail by reference to any test. The Respondents submit that receipt by them of information which may (or may not) be derived from intercept simply forms part of lawful *"Intelligence Sharing"*, as discussed above, and that sufficient safeguards are in place.

26. Mr Farr describes this as follows in his witness statement:

> "*27*. [The descriptions he gives of sharing of intelligence with foreign states] *do not just apply to intelligence obtained through interception. These paragraphs apply to all forms of intelligence, including intelligence (i) derived from covert human intelligence sources (as they would be termed under RIPA), (ii) derived from or constituting records of audio and/or visual surveillance and (iii) obtained or derived from covert property searches.*
>
> *28. I am advised that a potential issue in these proceedings is whether the sharing of intelligence in the form of (or that is derived from) communications and communications data between the UK and foreign governments should in some sense be separately regulated.*
>
> *29. From the point of view of the privacy interests of those individuals who are subject to investigative measures, I do not consider that a workable distinction can be drawn between such intelligence and the other three forms of intelligence referred to in paragraph 27 above. In particular, I do not consider that intelligence in the form of (or that is derived from) communications and communications data is in some general sense more personal or private than those other forms of intelligence. For instance, if an eavesdropping device is covertly installed in a target's home it may record conversations between family members that are more intimate and personal than those that might be recorded if the target's telephone were to be intercepted (and this example becomes even clearer if, for instance, the telephone in question is only used by the target to contact his criminal associates). To give a further example, a covert human intelligence source may be able to provide information about a target as a result of his or her friendship (or more intimate relationship) with the target*

> *that is more private than information that could be obtained from, for instance, intercepting the target's emails.*
>
> *30. Nor can some general distinction be drawn between intelligence from interception and the other forms of covert intelligence identified in paragraph 27 above in terms of how likely it is that the individual targets in question will in practice be able to predict or foresee the possibility of the relevant investigative measures being taken against them. All forms of covert intelligence-gathering necessarily seek to benefit from a lack of awareness on the part of the target in order to maximise the chance of obtaining valuable intelligence. Interception is, in this regard, no different from, for instance, covert surveillance or the use of covert human intelligence sources.*"

27. Mr Eadie submits that it would be inappropriate and unnecessary to differentiate between the different kinds of information which might be supplied e.g. to foil a bomb plot in London, and impracticable to try to draw a distinction between information derived from intercept and not so derived or to seek explanations or make enquiries from NSA or any other agency as to whether information supplied did or did not derive from Prism or any other system of interception.

28. Mr Squires, for Privacy, who carried the burden of the argument on this issue on the part of all the Claimants, responded by making clear that the Claimants are not contending that the submissions he is making in this case apply to any information not obtained by intercept by the NSA. It appeared to us from his submissions that information from the NSA would fall into three categories:

    i) material which on its face derives from intercept, provided unsolicited;

    ii) communications which the Respondents have requested the NSA to intercept, or to make available to them as intercept, because they are themselves unable to do so ('solicited intercept');

    iii) all other information or communications obtained from the NSA by way of shared information, as discussed by Mr Farr.

29. So far as the first category is concerned, Mr Ryder QC pointed by way of analogy to s.15(8) of RIPA, which provides:

> "*In this section "copy", in relation to intercepted material or related communications data, means any of the following (whether or not in documentary form) –*
>
> *(a) any copy, extract or summary of the material or data which identifies itself as the product of an interception."*

The Claimants are not addressing any information which does not '*identify itself as the product of an interception*', and he refers to this subsection as indicating that this is a feasible differentiation, recognised as such (for other purposes) in RIPA.

30. As for the second category, there was some discussion of the **Padfield** principle (**Padfield v Ministry of Agriculture, Fisheries and Food** [1968] AC 997), namely that a public body is required to exercise its discretionary powers to promote (and not to circumvent) the policy and objects of the legislation which created those powers. There was also discussion, emanating from a question from the Tribunal, of whether there was a role for a concept of 'agency'. The Respondents plead in paragraph 58 of their Response as follows:

> *"In particular, not least given the safeguards and oversight mechanisms that Parliament saw fit to impose in the case of interception pursuant to a RIPA interception warrant . . . and in the light of the well established Padfield principle, it is accepted that it would as a matter of domestic public law be unlawful for any of the Intelligence Services to deliberately circumvent those safeguards and mechanisms (and attempt to avoid the need to apply for an interception warrant under RIPA) by asking a foreign intelligence agency to intercept certain specified communications and disclose them. That is not to say that there will not be circumstances where there are legitimate reasons to ask a foreign intelligence agency to intercept particular communications, for example, where it is not technically feasible for the Intelligence Services themselves to undertake the interception in question."*

The Claimants do not suggest that such a request to the NSA for solicited intercept would fall foul of the **Padfield** principle, or (in answer to the point raised by the Tribunal) would render the NSA an agent for the Respondents. However they submit that, if that occurs, then the Respondents will know that what is subsequently produced is the product of intercept.

31. As to these two categories, we summarised Mr Squires' submissions in the course of argument as follows (***Transcript 3/148***):

> "*Whether it is solicited, or whether it is not solicited, dealing with the product of intercept is, at some level or other, an interference with Article 8 which needs some legal backing, and there ought to be, at however high a level, a published procedure in relation to it.*"

32. As to the third category, the Claimants make no submissions, but suggest that the exercise of differentiating out the first two categories should not be difficult, and certainly does not require making investigation, whether of the NSA or otherwise, as to whether information supplied by the NSA does result from intercept. Effectively for the purposes of this hearing the Claimants are accepting that this third category of information, and the Respondents' dealings with it, would not need justification by reference to Article 8.

33. The Respondents accept that the obtaining of intercept material within the first two categories from NSA via Prism triggers an interference with Article 8. However Mr Eadie's submission is that there is no authority in Strasbourg to date to suggest or to support the proposition that the "**Weber** requirements" would apply to the

obtaining, handling, use, disclosure or destruction of foreign intelligence material of such kind. This is a reference to the decision of the ECtHR referred to in paragraph 4(ii) above, where the Court, in a case dealing with the recording of telecommunications in the course of 'strategic monitoring' (not greatly different to interception pursuant to a s.8(4) warrant), summarised the principles underlying Article 8(2), not for the first time, at paragraph 84, as follows:

> "*The Court reiterates that the expression "in accordance with the law" within the meaning of Article 8(2) requires, firstly, that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must, moreover be able to foresee its consequences for him, and compatible with the rule of law.*"

The Court then proceeded to set out in relation to an interception case the following propositions, which have become known as the **Weber** requirements: we have numbered these from 1-6 for convenience.

> "95. *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.*"

34. There is no material disagreement between the parties that this is not a **Weber** case (as set out in paragraph 25 above), in particular because, in the assumed scenario under consideration, there is no interception by the Respondents which would, but for the protection of RIPA (if complied with), be unlawful. Mr Eadie refers to **Uzun v Germany** [2011] 53 EHRR 24, which was a case relating to surveillance using GPS, where the ECtHR expressly said (at para 66) that the **Weber** requirements were not applicable because:

> "*While the Court is not barred from gaining inspiration from these principles, it finds that these rather strict standards, set up and applied in the specific context of surveillance of telecommunications . . . are not applicable as such to cases such as the present one, concerning surveillance via GPS of movements in public places, and thus a measure which must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations . . . It will therefore apply the more general principles on adequate protection against arbitrary interference with Article 8 rights as summarised above.*"

Mr Eadie submitted (as referred to in paragraph 25 above) that this is simply a species of intelligence gathering, not to be equated with the position where the UK itself intercepts. Mr Ryder contended that this ignored the fact that the product of the intercept would then be stored, used and analysed in the same way as intercepted material obtained by the Respondent's themselves – although of course that would also apply to the information within the Claimants' third category referred to in paragraph 28(iii) above.

35. Both the Respondents and the Claimants accept that Strasbourg jurisprudence places special emphasis upon interception. Essentially Mr Squires' submission was that there are *"different levels of "prescribed by law*", and that, as he put it, "*we don't necessarily say exactly the same [level], but one [has] to have something at least approaching the "prescribed by law" standards, set out in* ***Weber*** *etc, when it is communications intercepted by the US and then accessed here, received here, analysed here."*

36. We agree that the Prism Issue engages Article 8 and that even at a 'lower level' than **Weber** there will need to be a compliance with requirements by the Respondents, particularly in relation to storage, sharing and retention/destruction. We have set out the statutory framework which imposes obligations upon the Respondents in relation to its obtaining information from the NSA, whether derived from intercept or otherwise, but more is required by the jurisprudence of the ECtHR, albeit at a 'lesser level', as the Claimants put it.

37. The relevant principles appear to us to be that in order for interference with Article 8 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.

A clear reiteration of these principles is contained in the judgment of the Court in **Bykov v Russia** 4378/02 21 January 2009:

> "*76. The Court reiterates that the phrase "in accordance with the law" not only requires compliance with domestic law but also relates to the quality of that law, requiring it to be compatible with the rule of law. In the context of covert surveillance by public authorities, in this instance the police, domestic law must provide protection against arbitrary interference with an individual's right under Article 8. Moreover, the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which public authorities are entitled to resort to such covert measures . . .*

> *78. . . . In particular, in order to comply with the requirement of the "quality of the law", a law which confers discretion must indicate the scope of that discretion, although the detailed procedures and conditions to be observed do not necessarily have to be incorporated in rules of substantive law. The degree of precision required of the "law" in this connection will depend upon the particular subject-matter. Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive – or to a judge – to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.*"

38. It is quite plain, as we have said at paragraph 6 above, that in the field of national security much less is required to be put in the public domain, and the degree of foreseeability must be reduced, because otherwise the whole purpose of the steps taken to protect national security would be at risk. The views of the Court to that effect in paragraphs 67 and 68 of **Malone** are encapsulated by the Court in **Leander v Sweden** [1987] 9 EHRR 433 at paragraph 51:

> "*However, the requirement of foreseeability in the special context of secret controls of staff in sectors affecting national security cannot be the same as in many other fields. Thus, it cannot mean that an individual should be enabled to foresee precisely what checks will be made in his regard by the Swedish special police service in its efforts to protect national security. Nevertheless, in a system applicable to citizens generally, as under the Personnel Control Ordinance, the law has to be sufficiently clear in its terms to give them an adequate indication as to the circumstances in which and the conditions on which the public authorities are empowered to resort to this kind of secret and potentially dangerous interference with private life.*
>
> *In assessing whether the criterion of foreseeability is satisfied, account may be taken also of instructions or administrative practices which do not have the status of substantive law, in so far as those concerned are made sufficiently aware of their contents.*
>
> *In addition, where the implementation of the law consists of secret measures, not open to scrutiny by the individuals concerned or by the public at large, the law itself, as opposed to the accompanying administrative practice, must indicate the scope of any discretion conferred on the competent authority with sufficient clarity, having regard to the legitimate aim of*

> *the measure in question, to give the individual adequate protection against arbitrary interference.*"

39. We consequently bear carefully in mind the requirement to give adequate protection against arbitrary interference on the one hand, but on the other hand that foreseeability does not require all the rules which govern or exclude that arbitrariness to be disclosed, particularly in the field of national security. We thus approach this Prism Issue, in which it is, as we have set out, largely common ground that the **Weber** requirements do not need to be enforced in all their rigour, in relation to a case where the interception has already been carried out by others.

40. In **Esbester v UK** [1994] 18 EHRR CD 72, the Commission, after reference to the passages in **Malone** and **Leander** set out or referred to above, addressed the complaints that guidelines governing supervision of the use of information obtained by the Security Services were unpublished. It continued (at CD 74):

> "*The Commission notes that the exercise of the Security Service's functions* [is] *subject to express limitations and to the supervision of a tribunal and commissioner appointed pursuant to the 1989 Act. The guidelines referred to in section 2(3) of the Act relate only to the administrative implementation of preceding provisions, which expressly limit the use of information by the Service to that necessary to fulfil its functions.*
>
> . . .
>
> *In light of the above, the Commission considers that in the present case the law is formulated with sufficient precision to enable the applicant to anticipate the application of vetting procedures and to the likely nature of the involvement of the Security Service and police Special Branches with regard to the collection, recording and release of information relating to himself.*"

41. We consider that what is required is a sufficient signposting of the rules or *arrangements* insofar as they are not disclosed. We find the Claimants' asserted distinction between the first and second categories and the third category referred to in paragraph 28 above a very difficult one, certainly in terms of the asserted contrasting consequences. We do not find that **Weber** – or 'nearly-**Weber**' – should apply to two of the categories, though not applying to the third. We are satisfied that in the field of intelligence sharing it is not to be expected that rules need to be contained in statute (**Weber**) or even in a code (as was required by virtue of the Court's conclusion in **Liberty v UK**. It is in our judgment sufficient that:

i) Appropriate rules or *arrangements* exist and are publicly known and confirmed to exist, with their content sufficiently signposted, such as to give an *adequate indication* of it (as per **Malone**: see paragraph 37(ii) above).

ii) They are subject to proper oversight.

42. As to their existence, *arrangements* are provided for in the statutory framework to which we have referred in paragraph 18 (ii), (v) and (viii) above. Mr Farr in his witness statement explains as follows:

> "*51. The Intelligence Services take their legal duties under the regime very seriously. The statutory framework is underpinned by detailed internal guidance (including the "arrangements" to which reference is made in section 2 of the Security Service Act 1989 and sections 2 and 4 of the Intelligence Services Act 1994), and by a culture of compliance.*
>
> *52. This culture of compliance is reinforced by the provision of mandatory training to staff within the Intelligence Services regarding the legal and policy framework within which they operate. The training includes clear instructions on the need for strict adherence to the law and to internal guidance.*
>
> . . .
>
> *55. The full details of the arrangements between the Intelligence Services and the UK's foreign intelligence partners for the sharing of intelligence, and the internal guidance of the Intelligence Services for the handling and use of intelligence obtained as a result, are (and have always been) kept confidential. I am satisfied that they cannot safely be published without undermining the interests of national security and the prevention and detection of serious crime. There are four main reasons for this.*"

Mr Eadie on instructions stated in open hearing that such *arrangements* also included provision for destruction. Mr Farr also referred in paragraph 74 of his witness statement to what the ISC had said in paragraph 7 of its Statement, set out in paragraph 23 above, as to GCHQ having put in place policies and procedures to underpin the statutory provisions.

43. In paragraphs 56 to 61 of his witness statement Mr Farr explained why in his belief "*the full details of the arrangement between the Intelligence Services and the UK's Foreign Intelligence Partners for the sharing of intelligence, and the internal guidance of the Intelligence Services for the handling and use of intelligence obtained as a result are (and have always been) kept confidential . . . and cannot safely be published without undermining the interest of national security and the prevention and detection of serious crime*". He gives four detailed reasons, to which we refer.

44. These rules or *arrangements* (in respect of any or all of the Claimants' three 'categories') were thus not made known in their detail to the public, and to that extent are not *accessible*, and, unlike the Code published under RIPA, to which we shall turn, not even a summary of what they contain was disclosed. However the significant fact is that they are subject to oversight and investigation, namely by the ISC and the Commissioner, as appears in paragraphs 23 and 24 above.

45. They are now in the process of challenge before this Tribunal. As accepted in **Kennedy** at paragraph 167, and as pointed out in **Telegraaf Media Nederland v the Netherlands** [2012] 34 BHRC 193 at paragraph 98, this Tribunal, albeit that it has a different role from the Commissioner, who has power to make roving inspections, has a distinct role to play in oversight by way of investigating complaints made to it, and has its own rules to facilitate that investigation. These are founded upon the obligation of the Respondents to provide all relevant material to the Tribunal pursuant to s.68(6) of RIPA. The Tribunal has the power to operate its own procedures pursuant to the Rules (the Investigatory Powers Tribunal Rules 2000) which have been made under s.69(6) of RIPA, which have regard, in particular, to:

> "*(a) the need to secure that matters which are the subject of proceedings, complaints or references brought before or made to the Tribunal are properly heard and considered; and*
>
> *(b) the need to secure that information is not disclosed to an extent, or in a manner, that is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of the United Kingdom or the continued discharge of the functions of any of the intelligence services."*

Rules 6 and 9 permitted and facilitated the following of the procedure set out in paragraph 10 above (particularly as set out in paragraph 19.3 there cited).

46. The Tribunal has in our judgment very distinct advantages over both the Commissioner and the ISC, some of which are set out in paragraphs 70 to 76 of the Respondents' Response. In particular:

i) It can hold this hearing and have the benefit of inter partes argument at which forceful legal submissions can be made on behalf of Claimants who seek to criticise the system. This is and was not available to the ISC or to the Commissioner. Ms Brimelow for Amnesty highlighted a number of matters which she submits were either missed or not dealt with by the ISC: all of those matters have now been addressed before us in depth.

ii) It can hold a public hearing on assumed facts, as it has done in this case, i.e. facts which are asserted by the Claimants, and would otherwise be the subject of NCND, without the Claimants needing to present an arguable case that they are the subject of interference (see paragraph 4(ii) above).

iii) It has access to all secret information, and can adjourn into closed hearing in order to assess whether the *arrangements* (a) do indeed exist as asserted by Mr Farr, (b) are adequate to do the job of giving the individual "*adequate protection against arbitrary interference*".

iv) It has, and takes, the opportunity, with the benefit of full argument, to probe fully whether matters disclosed to it in closed hearing, pursuant to the Respondents' obligation to do so pursuant to s.68(6) of RIPA, can and should be disclosed in open and thereby publicised.

47. We have been greatly assisted by the substantial submissions in the open hearing, and in the closed hearings by sight of and understanding what Mr Eadie called the "*arrangements below the waterline*" and their explanation, and submissions by the Respondents and by Counsel to the Tribunal. As a result of the process described in paragraph 10 above, the following Disclosure was made by the Respondents relevant to the Prism Issue. It was made by reference to the evidence given in the closed hearing which they were prepared to disclose, subject to the express caveat that references to "the Intelligence Services" in the Disclosure were references to whichever of the Intelligence Services carried out the relevant activities described in it, in the context of the factual premises set out in paragraph 14 above:

> "*1. A request may only be made by the Intelligence Services to the government of a country or territory outside the United Kingdom for unanalysed intercepted communications (and associated communications data), otherwise than in accordance with an international mutual legal assistance agreement, if either:*
>
> *a. a relevant interception warrant under the Regulation of Investigatory Powers Act 2000 ("RIPA") has already been issued by the Secretary of State, the assistance of the foreign government is necessary to obtain the communications at issue because they cannot be obtained under the relevant RIPA interception warrant and it is necessary and proportionate for the Intelligence Services to obtain those communications; or*
>
> *b. making the request for the communications at issue in the absence of a relevant RIPA interception warrant does not amount to a deliberate circumvention of RIPA or otherwise contravene the principle established in Padfield v. Minister of Agriculture, Fisheries and Food [1968] AC 997 (for example, because it is not technically feasible to obtain the communications via RIPA interception), and it is necessary and proportionate for the Intelligence Services to obtain those communications. In these circumstances, the question whether the request should be made would be considered and decided upon by the Secretary of State personally.*
>
> *For these purposes a "relevant RIPA interception warrant" means either (i) a s8(1) warrant in relation to the target at issue; (ii) a s8(4) warrant and an accompanying certificate which includes one or more "descriptions of intercepted material" (within the meaning of s8(4)(b) of RIPA) covering the target's communications, together with an appropriate s16(3) modification (for individuals known to be within the British Islands); or (iii) a s8(4) warrant and*

accompanying certificate which includes one or more "descriptions of intercepted material" covering the target's communications (for other individuals). The reference to a "warrant for interception, signed by a Minister" being "already in place" in the ISC's Statement of 17 July 2013 should be understood in these terms. (Given sub-paragraph (b), and as previously submitted in open, a RIPA interception warrant is not as a matter of law required in all cases in which unanalysed intercepted communications might be sought from a foreign government.)

2. *Where the Intelligence Services receive intercepted communications content or communications data from the government of a country or territory outside the United Kingdom, irrespective whether it is / they are solicited or unsolicited, whether the content is analysed or unanalysed, or whether or not the communications data are associated with the content of communications, the communications content and data are, pursuant to internal "arrangements", subject to the same internal rules and safeguards as the same categories of content or data, when they are obtained directly by the Intelligence Services as a result of interception under RIPA.*"

We considered that this Disclosure could be made open, and it was so made with the consent of the Respondents.

48. In addition, after the further open hearing, the Respondents made the following further Disclosure of evidence given in the closed hearings:

(1) "*The US Government has publicly acknowledged that the Prism system and Upstream programme, undertaken in accordance with Section 702 of the Foreign Intelligence Surveillance Act, permit the acquisition of communications to, from, or about specific tasked selectors associated with non-US persons who are reasonably believed to be located outside the United States in order to acquire foreign intelligence information. To the extent that the Intelligence Services are permitted by the US Government to make requests for material obtained under the Prism system (and/or on the Claimants' case, pursuant to the Upstream programme), those requests may only be made for unanalysed intercepted communications (and associated communications data) acquired in this way.*"

(2) As to the request referred to in paragraph 1(b) of the Disclosure above (a "1(b) Request"),

> *"Any such request would only be made in exceptional circumstances, and has not occurred as at the date of this statement.*"

49. As described in paragraph 10 above, the Claimants made submissions as to the Disclosure, both in writing and at the further open hearing, which, insofar as relevant to this Prism Issue, are as follows:

    (i) They relied upon and repeated their arguments that the Tribunal is not entitled to look *below the waterline* to examine the *arrangements* and safeguards, even if the Tribunal is satisfied that there is adequate indication of them *above the waterline* and even for the purpose of assessing their adequacy.

    (ii) They submitted that the Disclosure which was produced after the first closed hearing and then amended in the light of the Claimants' written submissions and the further closed and open hearings, was unsatisfactory in that it did not disclose its sources nor of what it was a gist or summary.

    (iii) The description of circumstances in which such a request could be made where a s.8(4) warrant was in existence was unclear.

    (iv) They complain of the limitation of the Disclosure by reference to paragraph 48(1) to Prism and Upstream, but it is plain that this case, and this Issue, only relate to Prism and Upstream.

50. They also made understandable complaint about the limitation of paragraph 1 of the Disclosure to unanalysed intercept and associated communications data. This is now clarified and met by the further Disclosure of evidence given in closed set out in paragraph 48 above. As for the balance of the Claimants' submissions:

    (i) We shall return further to this later in the judgment, but we conclude that the Tribunal is entitled to look *below the waterline* in order to be satisfied (a) that there are adequate safeguards (b) that what is described *above the waterline* is accurate and gives a sufficiently clear *signpost* to what is *below the waterline* without disclosing detail of it.

    (ii) We do not accept that the holding of a closed hearing, as we have carried it out, is unfair. It accords with the statutory procedure, and facilitates the process referred to in paragraphs 45 and 46 above. This enables a combination of open and closed hearings which both gives the fullest and most transparent opportunity for hearing full arguments inter partes on hypothetical or actual facts, with as much as possible heard in public, and preserves the public interest and national security.

    (iii) The Disclosure has been a running document, being amended by additions or clarifications on 2 occasions (ignoring one which was necessitated by an unfortunate typographical error which was entirely the fault of the Tribunal Secretariat) and again as set out in paragraph 47 above, taking account of the submissions and criticisms of the Claimants and the observations of the Tribunal in closed hearing. We are satisfied that the Disclosures cast a clear

and accurate summary or résumé of that part of the evidence given in the closed hearing which ought to be disclosed: and that the balance of the evidence and submissions given in closed hearing was too sensitive for disclosure without risk to national security or to the NCND principle.

(iv) We are satisfied that the description of the circumstances in which, when a request is made, there is an existing warrant is clear. Although the reader of this judgment will be enabled to understand the position better when, in relation to the s.8(4) issue, fuller exposition is given below, it is clear that the preconditions are either the existence of a s.8(1) warrant or the existence of a s.8(4) warrant within whose ambit the proposed target's communications fall, together, if the individual is known to be within the British Islands, with a s.16(3) modification.

51. In relation to paragraph 1 of the Disclosure, this subjects any requests pursuant to Prism and/or Upstream in respect of intercept or communications data to the RIPA regime, save only for the wholly exceptional scenario referred to as a 1(b) request. A 1(b) request has in fact never occurred, as the ISC has recognised as set out at paragraph 5 of its Statement, (cited in paragraph 23 above), and as now confirmed by the Respondents, as set out in paragraph 48(2) above.

52. In relation to paragraph 2 of the Disclosure, by which the same obligations and safeguards are applied to the receipt of any intercept or communications data pursuant to Prism and/or Upstream as apply when they are obtained directly by the Intelligence Services as a result of interception under RIPA:

(i) We must address below, with regard to the s.8(4) Issue, the nature and adequacy of those obligations and safeguards resulting from and relating to interception under RIPA, and, subject to (ii) below, the same considerations will apply.

(ii) As Mr Squires accepted, the clarification given within paragraph 1 of the Disclosure, that there will only be a request under Prism and/or Upstream, by reference to the existence of a s.8(4) warrant, which relates to an individual known to be within the British Islands, if a s.16(3) modification is in place, means that the RIPA safeguards under ss.15 and 16 (dealt with in detail below) in fact apply: except as he pointed out, in respect of a 1(b) Request so far as s.16 safeguards are concerned.

53. The one matter of concern is this. Although it is the case that any request for, or receipt of, intercept or communications data pursuant to Prism and/or Upstream is ordinarily subject to the same safeguards as in a case where intercept or communication data are obtained directly by the Respondents, <u>if</u> there were a 1(b) request, albeit that such request must go to the Secretary of State, and that any material so obtained must be dealt with pursuant to RIPA, there is the possibility that the s.16 protection might not apply. As already indicated, no 1(b) request has in fact ever occurred, and there has thus been no problem hitherto. We are however satisfied that there ought to be introduced a procedure whereby any such request, if it be made, when referred to the Secretary of State, must address the issue of s.16(3).

54. Subject to this, and to the caveat in paragraph 52(i) above, we are satisfied that the concerns as to the categories in paragraphs 28(i) and (ii) above, as to which we were addressed, are resolved. Nothing that we saw or heard in the closed hearings cast any doubt upon what is stated by the ISC, as set out in paragraph 23 above. As for paragraph 6.8.6 of the Commissioner's Report (set out in paragraph 24 above), this is now corroborated by what has been disclosed, in circumstances to which we shall refer in paragraph 130 below, in a document disclosed by the Respondents in other proceedings before this Tribunal (Belhadj IPT/13/132-9H), relied upon by the Claimants in these proceedings, at paragraph 4: "*GCHQ treats all operational data as if it were obtained under RIPA*". There are rules and procedures, the nature and effect of which have been sufficiently disclosed, which result in the same requirements being applied to both those two categories, and indeed to all intercept, solicited or unsolicited, obtained pursuant to Prism and/or Upstream, as apply to intercept obtained under RIPA by the Intelligence Services themselves.

55. After careful consideration, the Tribunal reaches the following conclusions:

(i) Having considered the *arrangements below the waterline*, as described in this judgment, we are satisfied that there are adequate arrangements in place for the purpose of ensuring compliance with the statutory framework and with Articles 8 and 10 of the Convention, so far as the receipt of intercept from Prism and/or Upstream is concerned.

(ii) This is of course of itself not sufficient, because the *arrangements* must be sufficiently accessible to the public. We are satisfied that they are sufficiently signposted by virtue of the statutory framework to which we have referred and the Statements of the ISC and the Commissioner quoted above, and as now, after the two closed hearings that we have held, publicly disclosed by the Respondents and recorded in this judgment.

(iii) These *arrangements* are subject to oversight.

(iv) The *scope of the discretion conferred* on the Respondents to receive and handle intercepted material and communications data and (subject to the s.8(4) issues referred to below) *the manner of its exercise*, are accordingly (and consistent with **Bykov** - see paragraph 37 above) accessible *with sufficient clarity to give the individual adequate protection against arbitrary interference*.

We refer in paragraphs 153-155 below to the consequences of these conclusions.

56. We should deal with a submission by Ms Brimelow for Amnesty International, although not made or adopted by the other Claimants, made by reference to Article 8, and to Article 17 of the International Covenant on Civil and Political Rights, which provides that:

> "*No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence.*"

and that

> "*Everyone has the right to the protection of the law against such interference*."

57. Amnesty's case is that the United Kingdom thereby owes a positive obligation to prevent or forestall the United States from intercepting such communications; this would extend to not acquiescing in such course by receiving the product. There are numerous difficulties about such an argument. The first is that such alleged positive duty would need to be enforceable against the U.K. by this Claimant (Amnesty International). Then it would seem very unlikely that such a contention would fall within the ambit of the issue being decided at this hearing, as set out in paragraph 14 above.

58. As the Respondents point out, Amnesty does not explain how the United Kingdom could prevent the United States from obtaining (lawfully on the assumptions made for the purposes of this hearing) communications, from United States communication providers under s.702 of FISA, to protect its own national security, nor why the Respondents should be expected, if such is alleged, to undermine the attempts of the United States to protect its own national security, by informing the subjects of US surveillance that their personal data had been obtained, stored or searched by US Officials. The authorities referred to by Ms Brimelow all involve a state's connivance in the acts of third parties such as to engage its own responsibility under the Convention, such as connivance in acts performed by foreign officials on its own territory (**El-Masri v Former Yugoslav Republic of Macedonia** [2013] 57 EHRR 25). There is no authority which imposes any obligation on the part of contracting states to secure that non-contracting states, acting within their own jurisdiction, respect the rights and freedoms guaranteed by the Convention, even if the failure of such non-contracting states to do so may have adverse effects on persons within the jurisdiction of contracting states; nor to pursue a complaint by one of its citizens of breach of his or her rights by another state within the jurisdiction of that state (**Bertrand Russell Peace Foundation v United Kingdom** [1978] 14 DR 117 and the other Commission cases recited with agreement in **(R)Al-Rawi v Foreign Secretary** [2008] QB 289 at paragraphs 96 to 99). The Respondents also refer to **M v Italy** [2013] 57 EHRR 29 at paragraph 127, where the ECtHR said that:

> "*127 . . . the Convention organs have repeatedly stated that the Convention does not contain a right which requires a High Contracting Party to exercise diplomatic protection, or espouse an applicant's complaints under international law, or otherwise to intervene with the authorities of another state on his or her behalf.*"

59. Ms Brimelow drew our attention to the Report dated 30 June 2014 of the Office of the United Nations High Commission of Human Rights, in which the UN Commissioner referred to the failure by states to take effective measures to protect individuals within their jurisdiction against illegal surveillance practices by other states, in breach of their own human rights obligations. However, not only does the UN Commissioner not identify what those human rights obligations are, but in this case there is no suggestion other than that the surveillance practices assumed to have taken place under s.702 of FISA and Executive Order 12333 were not illegal.

60. We did not call upon the Respondents to respond to this additional submission, and we do not accept it, for the reasons we have set out above.

THE S.8(4) ISSUE

61. We must begin by setting out a little of the statutory structure contained in RIPA. By s.1(1), interception of any communication in the course of its transmission by means of a public telecommunication system is unlawful unless, relevantly to this case, it takes place as provided for by s.1(5)(b) of the Act in accordance with a warrant under s.5 ("an interception warrant"). By s.2(2) a person intercepts a communication in the course of its transmission by means of a telecommunication system if (materially) he so modifies or interferes with the system or its operation, or so monitors transmissions made by means of the system as to make "*some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication*". By s.2(7) the times while a communication is being transmitted by means of a telecommunication system "*shall be taken to include any time when the system by means of which the communication is being, or has been, transmitted is used for storing it in a manner that enables the intended recipient to collect it or otherwise to have access to it*".

62. It is common ground that interception can simply comprise the obtaining and recording of a communication (as it is being transmitted), so as to make it available subsequently to be read, looked at or listened to by a person: no one in fact needs actually to have read, looked at or listened to the communication for interception to occur.

63. S.5 of the Act provides in material part as follows:

> "***5 Interception with a warrant.***
>
> *(1) Subject to the following provisions of this Chapter, the Secretary of State may issue a warrant authorising or requiring the person to whom it is addressed, by any such conduct as may be described in the warrant, to secure any one or more of the following—*
>
> > *(a) the interception in the course of their transmission by means of a postal service or telecommunication system of the communications described in the warrant;*
> >
> > . . .
> >
> > . . .
> >
> > *(d) the disclosure, in such manner as may be so described, of intercepted material obtained by any interception authorised or required by the warrant, and of related communications data.*
>
> *(2) The Secretary of State shall not issue an interception warrant unless he believes—*

> *(a) that the warrant is necessary on grounds falling within subsection (3); and*
>
> *(b) that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.*
>
> *(3) Subject to the following provisions of this section, a warrant is necessary on grounds falling within this subsection if it is necessary—*
>
> *(a) in the interests of national security;*
>
> *(b) for the purpose of preventing or detecting serious crime;* [or]
>
> *(c) for the purpose of safeguarding the economic well-being of the United Kingdom;*
>
> *. . .*
>
> *(4) The matters to be taken into account in considering whether the requirements of subsection (2) are satisfied in the case of any warrant shall include whether the information which it is thought necessary to obtain under the warrant could reasonably be obtained by other means.*
>
> *(5) A warrant shall not be considered necessary on the ground falling within subsection (3)(c) unless the information which it is thought necessary to obtain is information relating to the acts or intentions of persons outside the British Islands.*
>
> *(6) The conduct authorised by an interception warrant shall be taken to include—*
>
> *(a) all such conduct (including the interception of communications not identified by the warrant) as it is necessary to undertake in order to do what is expressly authorised or required by the warrant;*
>
> *(b) conduct for obtaining related communications data; and*
>
> *(c) conduct by any person which is conduct in pursuance of a requirement imposed by or on behalf of the person to whom the warrant is addressed to be provided with assistance with giving effect to the warrant.*"

64. There are limited persons who can apply for an interception warrant, as specified in s.6, who include (materially for our purpose), the Director General of MI5, the Chief of MI6 and the Director of GCHQ. Save in exceptional circumstances, an interception warrant cannot be issued except under the hand of the Secretary of

State, who will be the Home Secretary for the purposes of MI5, and the Foreign Secretary for the purposes of MI6 and GCHQ.

65. There are two kinds of interception warrants, a s.8(1) warrant, which can be described as a 'targeted warrant', with which these complaints and this judgment do not deal, and a s.8(4) warrant, which can be described as an 'untargeted' warrant or 'strategic' warrant (by reference to the similar monitoring considered in **Weber**) or, because of the provision in sub-section 8(4)(b) below, a 'certificated' warrant. S.8 reads as follows:

> "***8 Contents of warrants***.
>
> *(1) An interception warrant must name or describe either—*
>
> *(a) one person as the interception subject; or*
>
> *(b) a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place.*
>
> *(2) The provisions of an interception warrant describing communications the interception of which is authorised or required by the warrant must comprise one or more schedules setting out the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications that may be or are to be intercepted.*
>
> *(3) Any factor or combination of factors set out in accordance with subsection (2) must be one that identifies communications which are likely to be or to include—*
>
> *(a) communications from, or intended for, the person named or described in the warrant in accordance with subsection (1); or*
>
> *(b) communications originating on, or intended for transmission to, the premises so named or described.*
>
> *(4) Subsections (1) and (2) shall not apply to an interception warrant if—*
>
> *(a) the description of communications to which the warrant relates confines the conduct authorised or required by the warrant to conduct falling within subsection (5); and*
>
> *(b) at the time of the issue of the warrant, a certificate applicable to the warrant has been issued by the Secretary of State certifying—*
>
> *(i) the descriptions of intercepted material the examination of which he considers necessary; and*

> *(ii) that he considers the examination of material of those descriptions necessary as mentioned in section 5(3)(a), (b) or (c).*
>
> *(5) Conduct falls within this subsection if it consists in—*
>
> *(a) the interception of external communications in the course of their transmission by means of a telecommunication system; and*
>
> *(b) any conduct authorised in relation to any such interception by section 5(6).*
>
> *(6) A certificate for the purposes of subsection (4) shall not be issued except under the hand of the Secretary of State.*"

66. S.8(5) is of some significance in this hearing. As provided in s.8(5)(a), the interception of *'external'* communications, to which we will return, is expressly authorised; but by virtue of s.8(5)(b) so also is conduct falling within s.5(6) (set out in paragraph 63 above). Thus, apart from the express reference in s.5(6)(b) to "*obtaining related communications data*", there is also in s.5(6)(a) clear authorisation to intercept communications "*not identified by the warrant*", i.e. communications other than *external communications,* thus including *internal communications*, where it is necessary to do so "*in order to do what is expressly authorised or required by the warrant*".

67. S.20 is the interpretation section for the purposes of Chapter 1 of RIPA, which is the relevant Chapter:

i) For the meaning of *communications data* cross-reference is made to s.21(4), which gives the following definition:

> *"(a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;*
>
> *(b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person—*
>
> *(i) of any postal service or telecommunications service; or*
>
> *(ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system.*"

As set out in Paragraph 18(ix) above, such communications data are colloquially called 'metadata'.

ii) It is *related communications data* if it:

> "*a) is obtained by, or in connection with, the interception; and*
>
> *(b) relates to the communication or to the sender or recipient, or intended recipient, of the communication;*"

iii) "*Intercepted material*", "*in relation to an interception warrant means the contents of any communications intercepted by an interception to which the warrant relates*". It is common ground that this definition does not include "*related communications data*", separately defined as set out above.

iv) "*External communication*" means a communication sent or received outside the British Islands.

68. All parties refer to a passage in **Hansard**, when RIPA was debated in Parliament. Lord Bassam of Brighton, the relevant Minister, in a speech which led to the withdrawal of a proposed amendment, which had been proposed because Lord Phillips of Sudbury had contended that "*it will be extraordinarily difficult, if not impossible, to capture simply external communications*", said as follows:

> "*It is just not possible to ensure that only external communications are intercepted. That is because modern communications are often routed in ways that are not all intuitively obvious. Noble Lords who have contributed to the debate understand that. An internal communication say, a message from London to Birmingham—may be handled on its journey by Internet service providers in, perhaps, two different countries outside the United Kingdom. We understand that. The communication might therefore be found on a link between those two foreign countries. Such a link should clearly be treated as external, yet it would contain at least this one internal communication. There is no way of filtering that out without intercepting the whole link, including the internal communication.*
>
> *Even after interception, it may not be practicably possible to guarantee to filter out all internal messages. Messages may well be split into separate parts which are sent by different routes. Only some of these will contain the originator and the intended final recipient. Without this information it will not be possible to distinguish internal messages from external. In some cases it may not be possible even if this information is available. For example, a message between two foreign registered mobile phones, if both happened to be roaming in the UK, would be an internal communication, but there would be nothing in the message to indicate that.*
>
> *It is still the intention that Clause 8(4) warrants should be aimed at external communications. Clause 8(5) limits such a warrant to authorising the interception of external communications together with whatever other conduct is necessary to achieve that external interception. Whenever*

> *such a warrant is signed, the Secretary of State must be convinced that the conduct it will authorise as a whole is proportionate—my favourite word—to the objects to be achieved. His decision to sign will be overseen by the Interception of Communications Commissioner.*"

69. In the Interception of Communications Code of Practice ("the Code") issued pursuant to s.71 of RIPA, to which we will return, the definition of *External Communications* was encapsulated in paragraph 5.1, under "*Chapter 5; Interception Warrants (s.8(4))*", as follows:

> "*5.1 This section applies to the interception of external communications by means of a warrant complying with section 8(4) of the Act. External communications are defined by the Act to be those which are sent or received outside the British Islands. They include those which are both sent and received outside the British Islands, whether or not they pass through the British Islands in course of their transit. They do not include communications both sent and received in the British Islands, even if they pass outside the British Islands en route. Responsibility for the issuing of such interception warrants rests with the Secretary of State.*"

70. S.8(4) is of course central to the issues in this part of the case. The Respondents describe the s.8(4) regime in paragraph 66 of their skeleton as one which in principle "*permits a substantial volume of communications to be intercepted, and then requires the application of a selection process to identify a smaller volume of intercepted material that can actually be examined by persons, with a prohibition on the remainder being so examined . . . To this extent, it differs from the regime that applies under s. 8(1) of RIPA, under which interception warrants target a specified person or single set of premises.*"

71. The Tribunal agrees with the statement of the Commissioner in paragraph 6.5.38 of his Report that:

> "*The section 8(4) structure does not permit random trawling of communications. This would be unlawful. It only permits a search for communications referable to individuals the examination of whose communications are certified as necessary for a statutory purpose.*"

72. Although Amnesty in its skeleton argument hyperbolically describes the Respondents' purpose as "*to obtain data wholesale from every living human being with a working internet connection*", that is not the case as put orally by the Claimants, and we are entirely clear that the Respondents are not seeking, nor asserting that the system entitles them to seek, to carry out what has been described as "*mass*" or "*bulk*" surveillance. Mr Ryder made clear that he is not alleging indiscriminate trawling, but rather "*discriminate (in the sense that it is within very broad selectors) but vast*". The Respondents describe their case in paragraphs 70 to 71 of their skeleton, that the only way to intercept *external communications* being sent to, for example, an individual in Syria whose address they do not have is to:

> "70. . . *intercept a substantially greater volume of communications (including, potentially, a volume of internal communications), and then apply a selection stage to identify the communications in question. In other words, it is common ground that the only practical way to find and reconstruct most external communication "needles" is to look through the communications "haystack".*
>
> *71. . . Unless the Claimants wish to submit that the Intelligence Services should not be able to obtain the external communications that are needed for the purposes of national security, etc., they must accept some form of interception regime that permits substantially more communications to be intercepted (including, potentially, internal communications) than are actually being sought.*"

73. Mr Ryder in his closing submissions made it absolutely clear that the Claimants did not intend in any way to limit, hinder or obstruct the important work that the Intelligence Services do. Their submissions, he made clear, were guided at putting what the Services do within a framework and asking the Tribunal to do no more than what Parliament wanted the Tribunal to do, namely to indicate to Government when something is not in accordance with the law, in order to ensure that Government action was done in the most effective way and in accordance with proper legal principle.

74. Under the heading "*Restrictions on use of Intercepted Material etc*" there are the following two sections of RIPA, which in material part are as follows:

> "*15 (1) Subject to subsection (6), it shall be the duty of the Secretary of State to ensure, in relation to all interception warrants, that such arrangements are in force as he considers necessary for securing—*
>
> *(a) that the requirements of subsections (2) and (3) are satisfied in relation to the intercepted material and any related communications data; and*
>
> *(b) in the case of warrants in relation to which there are section 8(4) certificates, that the requirements of section 16 are also satisfied.*
>
> *(2) The requirements of this subsection are satisfied in relation to the intercepted material and any related communications data if each of the following—*
>
> *(a) the number of persons to whom any of the material or data is disclosed or otherwise made available,*
>
> *(b) the extent to which any of the material or data is disclosed or otherwise made available,*

(c) the extent to which any of the material or data is copied, and

(d) the number of copies that are made,

is limited to the minimum that is necessary for the authorised purposes.

(3) The requirements of this subsection are satisfied in relation to the intercepted material and any related communications data if each copy made of any of the material or data (if not destroyed earlier) is destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes.

(4) For the purposes of this section something is necessary for the authorised purposes if, and only if—

(a) it continues to be, or is likely to become, necessary as mentioned in section 5(3);

. . .

(5) The arrangements for the time being in force under this section for securing that the requirements of subsection (2) are satisfied in relation to the intercepted material or any related communications data must include such arrangements as the Secretary of State considers necessary for securing that every copy of the material or data that is made is stored, for so long as it is retained, in a secure manner.

(6) Arrangements in relation to interception warrants which are made for the purposes of subsection (1)—

(a) shall not be required to secure that the requirements of subsections (2) and (3) are satisfied in so far as they relate to any of the intercepted material or related communications data, or any copy of any such material or data, possession of which has been surrendered to any authorities of a country or territory outside the United Kingdom; but

(b) shall be required to secure, in the case of every such warrant, that possession of the intercepted material and data and of copies of the material or data is surrendered to authorities of a country or territory outside the United Kingdom only if the requirements of subsection (7) are satisfied.

(7) The requirements of this subsection are satisfied in the case of a warrant if it appears to the Secretary of State—

> *(a) that requirements corresponding to those of subsections (2) and (3) will apply, to such extent (if any) as the Secretary of State thinks fit, in relation to any of the intercepted material or related communications data possession of which, or of any copy of which, is surrendered to the authorities in question; and*
>
> *(b) that restrictions are in force which would prevent, to such extent (if any) as the Secretary of State thinks fit, the doing of anything in, for the purposes of or in connection with any proceedings outside the United Kingdom which would result in such a disclosure as, by virtue of section 17, could not be made in the United Kingdom.*"

We have already referred to s.15(8) in paragraph 29 above.

> "*16. (1) For the purposes of section 15 the requirements of this section, in the case of a warrant in relation to which there is a section 8(4) certificate, are that the intercepted material is read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant to the extent only that it—*
>
> *(a) has been certified as material the examination of which is necessary as mentioned in section 5(3)(a), (b) or (c); and*
>
> *(b) falls within subsection (2).*
>
> *(2) Subject to subsections (3) and (4), intercepted material falls within this subsection so far only as it is selected to be read, looked at or listened to otherwise than according to a factor which—*
>
> *(a) is referable to an individual who is known to be for the time being in the British Islands; and*
>
> *(b) has as its purpose, or one of its purposes, the identification of material contained in communications sent by him, or intended for him.*
>
> *(3) Intercepted material falls within subsection (2), notwithstanding that it is selected by reference to any such factor as is mentioned in paragraph (a) and (b) of that subsection, if—*
>
> *(a) it is certified by the Secretary of State for the purposes of section 8(4) that the examination of material selected according to factors referable to the individual in question is necessary as mentioned in subsection 5(3)(a), (b) or (c); and*

> *(b) the material relates only to communications sent during a period specified in the certificate that is no longer than the permitted maximum .*
>
> *. . .*"

75. The Code, to which we referred in paragraph 69 above, is the subject of affirmative resolution of both Houses of Parliament. It contains a number of important provisions, of which we have already set out paragraph 5.1 in that paragraph. In Chapter 2, "*General rules on interception with a warrant*" there is specific guidance under paragraphs 2.4 and 2.5 with regard to necessity and proportionality in relation to the issue of warrants, and there are provisions in paragraphs 2.11 to 2.13 in relation to the duration of the interception warrants. Chapter 3 provides for safeguards against collateral intrusion and in respect of information which is confidential, is subject to legal privilege or involves confidential journalistic material. Chapter 4 relates to s.8(1) warrants, while Chapter 5 deals with s.8(4) warrants. Apart from paragraph 5.1, there is an important provision relating to an application for such a warrant, which contains the following:

> "*5.2 An application for a warrant is made to the Secretary of State. Interception warrants, when issued, are addressed to the person who submitted the application. This person may then serve a copy upon any person who may be able to provide assistance in giving effect to that warrant. Each application, a copy of which must be retained by the applicant, should contain the following information:*
>
> - *Background to the operation in question.*
> - *Description of the communications to be intercepted, details of the communications service provider(s) and an assessment of the feasibility of the operation where this is relevant.*
> - *Description of the conduct to be authorised, which must be restricted to the interception of external communications, or to conduct necessary in order to intercept those external communications, where appropriate.*
> - *The certificate that will regulate examination of intercepted material.*
> - *An explanation of why the interception is considered to be necessary for one or more of the section 5(3) purposes.*
> - *A consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct.*
> - *A consideration of any unusual degree of collateral intrusion, and why that intrusion is justified in the circumstances. In particular, where the communications in question might affect religious, medical or journalistic confidentiality or legal privilege, this must be specified in the application.*

- *Where an application is urgent, supporting justification should be provided.*

- *An assurance that intercepted material will be read, looked at or listened to only so far as it is certified, and it meets the conditions of sections 16(2)-16(6) of the Act.*

- *An assurance that all material intercepted will be handled in accordance with the safeguards required by sections 15 and 16 of the Act.*"

There are then provisions placing obligations on the Secretary of State in relation to the authorisation of such a warrant, and giving further guidance as to its necessity and proportionality (paragraphs 5.3 to 5.6). Paragraph 5.12 provides, in respect of renewal of such a warrant, that:

> "*The Secretary of State may renew a warrant at any point before its expiry date. Applications for renewals are made to the Secretary of State and contain an update of the matters outlined in paragraph 5.2 above. In particular, the applicant must give an assessment of the value of interception to the operation to date and explain why he considers that interception continues to be necessary for one or more of the purposes in section 5(3).*"

Detailed records are required to be kept by paragraph 5.17.

76. Chapter 6 of the Code is headed "*Safeguards*". There is detailed reference to ss.15 and 16, to dissemination of intercepted material, to copying, storage and, in paragraph 6.8, destruction:

> "*6.8 Intercepted material, and all copies, extracts and summaries which can be identified as the product of an interception, must be securely destroyed as soon as it is no longer needed for any of the authorised purposes. If such material is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid under section 15(3) of the Act.*"

Paragraph 6.9 deals with personnel security.

77. As appears from what we have set out above, there are numerous references to the duty of the Secretary of State to ensure that *arrangements are in force* in relation to dealings with the intercepted material and any related communications data: viz sub-sections 15(1), (5), (6): and there are some similar references in the Code (e.g. paragraph 5.17). Mr Farr, in his witness statement, similarly to his evidence with regard to the Prism Issue, says as follows as to these *arrangements*:

> "*100. Section 15 of RIPA imposes a duty on the Secretary of State to ensure, in relation to section 8(4) warrants, that such arrangements are in force as he considers necessary for*

securing that the requirements of sections 15(2)-(3) and 16 are satisfied. Chapter 6 of the current Code expands on the nature of the required safeguards, as does the revised draft Code to which I refer in paragraph 161 below (which was published for consultation and remains in the public domain). Beyond these public statements, the full details of the sections 15 and 16 arrangements are (and have always been) kept confidential. I have reviewed the safeguards that have been put in place for the purposes of sections 15 and 16 and I am satisfied that they cannot safely be put into the public domain without undermining the effectiveness of interception methods. This would be contrary to the interests of national security and prejudicial to the prevention and detection of serious crime. Interception techniques form a critical resource for the Government in countering terrorism and serious crime. To maintain the effectiveness of the techniques of interception that are adopted, the Government must take steps to ensure appropriate levels of secrecy not only as regards the fact of interception but also as regards the detailed manner in which it is performed. This applies to what I am able to say about the nature of the s. 8(4) regime and the safeguards that attach to it.

101. Although the full details of the sections 15 and 16 arrangements cannot be made public, they are not simply an internal Government matter. Rather, they are made available to the Commissioner (see paragraph 6.1 of the Code) who is required (by section 57(2)(d)(i) of RIPA) to keep them under review. Further, to facilitate oversight by the Commissioner (i) each intercepting agency is required to keep a record of the arrangements in question (see paragraph 5.17 of the Code) and (ii) any breach of the arrangements must be reported to the Commissioner (paragraph 6.1 of the Code)."

78. The *alleged factual premises* agreed for the purposes of the s.8(4) Issue at this hearing are as follows:

"3. *The Claimants' communications might in principle have been intercepted in the United Kingdom under the s. 8(4) regime (as defined in the Original Open Response) and at least some of those intercepted communications might in principle have been "read, looked at or listened to" by a person or persons under that regime.*

4. The Claimants allege:

(a) the Intelligence Services operate a programme, described as Tempora, under which fibre optic cables are intercepted. This involves making available the contents of all the communications and communications data being transmitted through the fibre optic cables;

(b) the intercepted communications and communications data may be retained for an indefinite period and automatically searched through the use of a large number of search terms, including search terms supplied by the United States National Security Agency.

(c) The intercepted communications and communications data may then be further retained, analysed and shared with other public authorities."

79. Leaving aside the questions relating to Article 10, as discussed in paragraph 12 above, the Agreed Issues themselves are formulated as follows:.

"*Issue (iv)*
In light of the factual premises at paragraphs (3) and (4) above, does the statutory regime as set out in paragraphs 102-178 of the Respondents' Open Response to the Claims brought by Liberty and Privacy satisfy the Art. 8(2) "in accordance with the law" requirement?

Issue (v)

Given the Claimants' allegations at factual premise (4), is the definition of "external communications" within s.20 Regulation of Investigatory Powers Act 2000 sufficiently precise to be "in accordance with the law" for the purposes of Art.8(2)?

Issue (ix)

Does the absence of a requirement that any s. 8(4) warrants issued in respect of the alleged Tempora programme target specific individuals or premises give rise to a breach of the "necessity" and "in accordance with the law" requirements in Art. 8(2) and/or (if the answer to Issue (vi) is "yes") Art. 10(2)?

Issue (x)

Are the "necessity" and "in accordance with the law" requirements in Art. 8(2) . . . breached because interception under the s. 8(4) regime issued in respect of the alleged Tempora programme may in principle involve (i) the interception (and subsequent recording) of communications and communications data without there being any reason to suspect that the communications of the individuals in question are relevant to national security, serious crime and/or the economic well-being of the United Kingdom, and (ii) the intercepted communications and communications data so obtained being processed to determine whether (pursuant to s.

> *16 and the certificate in question) it may be read, looked at or listened to by one or more persons?*
>
> *Issue (xi)*
>
> *Does the alleged Tempora programme and/or the s. 8(4) regime give rise to unlawful discrimination contrary to (i) Art. 14 of the ECHR (as read with Art. 8 and/or Art. 10), . . .*"

We have foreshortened the wording of this Issue, because it became common ground that there was only need to consider the Convention in this regard.

80. Although these issues were agreed as forming the basis for the hearing, it was inevitable that some of them should elide and overlap, and it seems to us that the following Four Questions encapsulate the arguments:

(1) Is the difficulty of determining the difference between *external* and *internal* communications, whether as a theoretical or practical matter, such as to cause the s.8(4) regime not to be *in accordance with law* contrary to Article 8(2)?

(2) Insofar as s.16 of RIPA is required as a safeguard in order to render the interference with Article 8 *in accordance with law*, is it a sufficient one?

(3) Is the regime, whether with or without s.16, sufficiently compliant with the **Weber** requirements, insofar as such is necessary in order to be *in accordance with law*?

(4) Is s.16(2) indirectly discriminatory contrary to Article 14 of the Convention, and, if so, can it be justified? It should be explained that, led by Mr Jaffey, the Claimants developed this more limited argument in the course of the hearing, effectively not pursuing the original pleaded claim by all Claimants that s.8(4) and (5) were so discriminatory.

The relief sought is effectively for a declaration that the Respondents acted unlawfully in violation of the Claimants' rights under Articles 8 and 14 ECtHR.

81. Before we turn to consider these questions, it is important to set out four matters of juristic background.

82. By a judgment of 9 December 2004 this Tribunal, Mummery LJ President, Burton J (then Vice-President), made a ruling in relation to the s.8(4) regime in a case which has been called the **British Irish Rights Watch** case, in which the complainants were represented by Liberty. This Tribunal concluded that the s.8(4) regime was in accordance with law. It is immediately necessary to say that of the Four Questions, set out above, now before this Tribunal, the first, second and fourth questions were not addressed, because they were not raised, and the third question was not addressed in terms of **Weber**, which had not yet reached the ECtHR.

83. Nevertheless, it is important to refer to the Tribunal's conclusions, and we quote certain passages from the judgment:

"9. *The s8(4) warrant is accordingly also described as a "certificated warrant". It can and may result, provided that the requirements of s8(4) and (5) are satisfied, in the interception of all communications between the United Kingdom and an identified city or country.*

. . .

11. It is apparent that the interference with the privacy of communications is likely to be greater by virtue of a s8(4) warrant than as a result of what Counsel called a "targeted" s8(1) warrant; although there may still be a mass of material obtained pursuant to a s8(1) warrant, dependent upon the activities of the individual, or at the premises, the subject of the warrant, and the number of calls made. In relation to both regimes, there are restrictions upon the use of intercepted material. S15 in particular applies to both a s8(1) and a s8(4) warrant. By s15(1) the Secretary of State must ensure in relation to all interception warrants that such arrangements are in force as he considers necessary for securing, by reference to s15(2), that there is the minimum necessary disclosure and copying of such material, and by reference to s15(3) the soonest possible destruction. No challenge is any longer made by the Complainants to the processes relating to disclosure retention or destruction of material obtained under a s8(1) or a s8(4) warrant. There are extra safeguards provided by s16 of RIPA in the case of s.8(4), or certificated, warrants.

. . .

14. As to the safeguards in ss15 and 16 of RIPA, in his witness statement served on behalf of the Respondents, the Director General of the Organised Crime, Drugs and International Group of the Home Office explains as follows:

> *'26. The internal agency manuals that set out the section 15 and section 16 safeguards, contain comprehensive instructions and refer in detail to specific techniques and processes. This level of detail is required precisely in order to ensure that the section 15 and section 16 safeguards, and the section 8(4) requirements, are properly understood by staff and are fully effective in practice. For the reasons given in the above paragraph [his description of the growing threat of terrorism, and the use by terrorist groups of modern technology, requiring to be countered by interception techniques and appropriate levels of secrecy to protect those techniques] the Government is unable to disclose the full detail of the arrangements for s8(4) warrants that are in place under sections 15 and 16 of [RIPA]. Disclosure of the specific arrangements, the*

> *Government assesses, and I believe, would be contrary to the interests of national security. In particular, it would enable individuals to adapt their conduct so as to undermine the operational effectiveness of any interception efforts which it might be thought necessary to apply to them. It is axiomatic that such instructions would be a very great utility to, for instance, members of the intelligence agencies of countries that are hostile to British interests.*
>
> *27. In the light of the above, what I set out in this statement is the fullest account of the safeguards and operating procedures that the Government is able to provide without undermining national security. The Government has experience of the loss of intelligence available to it and the loss of effectiveness of its intelligence gathering machinery, consequent upon revealing details of the methodologies available to it*'"

84. In paragraph 15 of the judgment it was recited that two complaints, which have been repeated before us, though not in any way in the forefront of the Claimants' arguments, were put before the Tribunal in that case, namely that the search terms were not specified in the Secretary of State's certificates and that they were selected without reference to the judiciary or ministers.

85. Another complaint made before us, which again has not been in the forefront of argument, is referred to in paragraphs 19ff of the judgment, namely the untargeted nature of a s8(4) warrant; this is rejected in paragraphs 19 to 22 of the judgment.

86. In paragraphs 29 to 31 of the judgment, the Tribunal addresses issues of foreseeability, and reference was made to paragraph 67 of the judgment in **Malone**, to which we have referred in paragraph 30 above. The judgment continued as follows:

> "*30. The Respondents' Counsel placed considerable reliance upon the decision of the Commission in* ***Christie v United Kingdom*** *[1993] 78-ADR 119. This decision took express account of, and referred to,* ***Kruslin and Huvig*** *(at 132). It was considering the very legislation now before us (save that it related to the predecessor statute, the Interception of Communications Act 1985, the terms of s2(2) of which were materially identical to s5(3) of RIPA). It was not a question of a judicial order for evidence leading to its admissibility in court. The issue related to authorised interception of telexes received from trade unions in Eastern Europe, which had been considered necessary under s2(2) (now s5(3)). Accessibility and foreseeability were addressed, and there was express reference not only to the* ***Sunday Times*** *judgment but also to paragraph 67 of the* ***Malone*** *judgment. The Commission concluded at 133ff as follows:"*

> *"The Government contend that the terms of the relevant legislative provisions sufficiently indicate the type of activity likely to be susceptible to interception of communications, and that safeguards are imposed that regulate the retention and use of information obtained from interceptions.*
>
> *The Commission notes that the case law of the Commission and Court establishes that the requirement of foreseeability in the special context of sectors affecting national security cannot be the same as in many other fields. In the* ***Leander*** *case [[1987] 9 EHRR 433] the Court stated:*
>
> > *"Thus, it cannot mean that an individual should be enabled to foresee precisely what checks will be made in his regard by the Swedish special police service in its efforts to protect national security. Nevertheless, in a system applicable to citizens generally ... the law has to be sufficiently clear in its terms to give them an adequate indication as to the circumstances in which and the conditions on which the public authorities are empowered to resort to this kind of secret and potentially dangerous interference with private life ... "*
>
> *The Commission recalls that it has considered the compatibility with the requirements of foreseeability of the partial definition of "interests of national security" ... in two previous cases,* ***Esbester v United Kingdom*** *[[1994]18 EHRR CD 72] ... and* ***Hewitt and Harman v United Kingdom*** *[Commission decision 1.9.93] ... It considered that the principles referred to above did not necessarily require a comprehensive definition of the notion of "the interests of national security", noting that many laws, which by their subject matter require to be flexible, are inevitably couched in terms which are to a greater or lesser extent vague and whose interpretation and application are questions of practice. It held that, given the express limitations on the exercise of the Security Service's functions and the supervision of a Tribunal and Commissioner, the law was formulated with sufficient precision ...*
>
> *While, as the applicant points out, the provisions of the 1985 ... [Act] are not subject to the influence of the adversarial input which forms part of the judicial process of interpretation, the Commission does not consider that the concept of foreseeability requires that questions of interpretation and practice must be decided in a judicial forum. It is compatible with the requirements of foreseeability that terms which are on their face general and unlimited are explained by administrative or executive statements and instructions, since it is the provision of sufficiently precise guidance to enable individuals to regulate their conduct, rather than the source of*

*that guidance, which is of relevance (cf … **Silver v UK** [1983] 5 EHRR 347). ...*

In light of the above, the Commission considers that the scope and manner of exercise of the powers to intercept communications and make use of the information obtained are indicated with a requisite degree of certainty to satisfy the minimum requirements referred to above.

The Commission thus concludes that any interference in the present case was "in accordance with the law".

31. The Complainants' Counsel submits that Christie and the two previous decisions referred to can be distinguished, since, although the issue addressed related to the identical statutory provision, the precise point now being taken was not addressed, namely one directed towards the absence of selection criteria. As will be seen however, it is the Respondents' submission that s5(3) supplies the answer to the Complainants' new submission also, such that, if that be right, the submission is both not new and answered by Christie.

*32. The nub of the Complainants' contention is that this is a case which falls within **Silver**, because there is no answer provided by the statute, and no other guidelines, published or available, which supply an answer to the requirement of accessibility or foreseeability:*

32.1 Although the Complainants' expert referred to a case presented to the Constitutional Court in the Federal Republic of Germany, [this must be a reference to **Weber**, which was not yet before the ECtHR] *in which there was reference made to a list of search terms which could or might be used as a filtering system prior to accessing material (although, as the Respondents' Counsel points out, he does not himself appear actually to say that the German search terms were ever published, as opposed to an account being given to the German Constitutional Court), the Complainants' Counsel does not suggest that, in order to comply with the in accordance with law doctrine there would have to be publication in the United Kingdom of a list of search terms. Such a course would in our judgment be both risky and pointless; risky because it would or might, contrary to the principle enunciated in paragraph 67 of **Malone,** enable those intending to participate in secret communications to avoid the use of words which would be known to appear in the search list; and pointless both for that reason and because any accessing of information intercepted pursuant to a s8(4) warrant would be bound to be fact specific, and what was being looked for would depend upon the subject matter of the warrant.*

32.2 At the end of the day the Complainants' Counsel's submission is a simple one. He is in no position, he submits, to guess at what should be said, but he simply submits that something more should be said, by way of

indication as to selection criteria than is presently stated, and that the selection should not be left simply to the discretion of officials.

33. The Respondents' response is unequivocal. They refer to paragraph 22 of the statement mentioned above in paragraph 14:

" ... This process under section 8(4) permits selection and examination of the selected material only to the extent that to do so would be necessary in the interests of national security, to prevent or detect serious crime or to safeguard the economic well-being of the United Kingdom. In this regard and generally, section 8(4) is to be read in conjunction with section 15 of RIPA, which in subsection (1) (b) specifically makes section 8(4) warrants subject to arrangements for ensuring that the requirements of section 16 of RIPA are satisfied (namely "that intercepted material is read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant to the extent only that it has been certified as material the examination of which is necessary as mentioned in section 5(3)(a), (b) or (c))". It is the duty of the Secretary of State to ensure that such arrangements are in force that he considers necessary for securing that the requirements of s16 are satisfied."

34. The selection criteria in relation to accessing a large quantity of as yet unexamined material obtained pursuant to a s8(4) warrant (as indeed in relation to material obtained in relation to a s8(1) warrant) are those set out in s5(3). The Complainants' Counsel complains that there is no "publicly stated material indicating that a relevant person i s satisfied that the [accessing] of a particular individual's telephone call i s proportionate". But the Respondents submit that there is indeed such publicly stated material, namely the provisions of s6(l) of the Human Rights Act which requires a public authority to act compatibly with Convention rights, and thus, it is submitted, imposes a duty to act proportionately in applying to the material the s5(3) criteria.

35. To that duty there is added the existence of seven safeguards listed by the Respondents' Counsel, namely (I) the criminal prohibition on unlawful interception (2) the involvement of the Secretary of State (3) the guiding role of the Joint Intelligence Committee ("JIC") (4) the Code of Practice (5) the oversight by the Interception of Communication Commissioner (whose powers are set out in Part IV of the Act) (6) the availability of proceedings before this Tribunal and (7) the oversight by the Intelligence and Security Committee, an all-party body of nine Parliamentarians created by the Intelligence Services Act 1994, whose operation is described in the Respondents' evidence. The existence of the Commissioner

and the Tribunal alone expressly weighed with the Commission in its decision in ***Christie****.*

36. It is plain that, although in fact the existence of all these safeguards is publicly known, it is not part of the requirements for accessibility or foreseeability that the precise details of those safeguards should be published. The Complainants' Counsel has pointed out that it appears from the Respondents' evidence that there are in existence additional operating procedures, as would be expected given the requirements that there be the extra safeguards required by s 16 of the Act, and the obligation of the Secretary of State to ensure their existence under sI5(1)(b). It is not suggested by the Complainants that the nature of those operating procedures be disclosed, but that their existence, i.e. something along the lines of what is in the Respondents' evidence, should itself be disclosed in the Code of Practice.

37. We are unpersuaded by this. First, such a statement in the Code of Practice, namely as to the existence of such procedures, would in fact take the matter no further than it already stands by virtue of the words of the statute. But in any event, the existence of such procedures is only one of the substantial number of safeguards which are known to exist. Accessibility and foreseeability are satisfied by the knowledge of the criteria and the knowledge of the existence of those multiple safeguards.

38. It is in those circumstances that the Respondents submit, by reference to the criteria in s5(3), as exercised with proportionality and the existence of the multiple safeguards, that both the question and the answer are the same as in ***Christie****. We agree. It is clear from the* ***Sunday Times*** *case at para 49 that foreseeability is only expected to a degree that is reasonable in the circumstances, and the circumstances here are those of national security, as discussed in* ***Klass*** *and* ***Leander****. This is not a* ***Silver*** *case where the legislation itself was inadequate and the guidelines were unpublished. In this case the legislation is adequate and the guidelines are clear. Foreseeability does not require that a person who telephones abroad knows that his conversation is going to be intercepted because of the existence of a valid s8(4) warrant. The "why me?" test is as inapt in this case as it would have been found to be by the Court of Appeal in its recent decision in* ***R ex parte Gillan and Another v Commissioner of Police for the Metropolis*** *[2004] 3 WLR 1144, at paragraph 50 of the judgment of the Court given by Lord Woolf LCJ, in relation to the subject of a valid stop and search order.*"

87. We see no reason to doubt these conclusions, albeit not binding upon us, always subject to what we have said in paragraph 82 above, in relation to the matters not then argued, and in particular the absence of **Weber**:

i) The Claimants point out that the decision in **Gillan**, to which the Tribunal referred in paragraph 38 of its judgment, has been subsequently effectively overruled by the ECtHR decision in **Gillan v United Kingdom** [2010] 50 EHRR 45. However, apart from the inappropriateness of the question "*why me*?", which does not appear to us to have been essential to the Tribunal's conclusions, the conclusory passage in paragraphs 77 to 79 of the ECtHR's judgment in that case does not appear to us to flaw the Tribunal's conclusion, nor to lead to a conclusion different from that reached by the Tribunal, namely the Court's requirement in paragraph 77 that:

> "*For domestic law to meet these requirements it must afford a measure of legal protection against arbitrary interferences by public authorities with the rights safeguarded by the Convention . . . it would be contrary to the rule of law . . .for a legal discretion granted to the executive to be expressed in terms of an unfettered power*",
>
> such as the Court found there to be in **Gillan**, and the Tribunal did not find in the **British Irish Rights Watch** case.

ii) The Claimants also point out that in **Liberty v UK**, at paragraph 63, the ECtHR stated that its "*approach to the foreseeability requirement in this field has . . . evolved since the Commission considered the United Kingdom's surveillance scheme in its decision in . . .* ***Christie***". But **Christie** and **Esbester** (see paragraph 40 above), to which the Tribunal also referred, were both cited without disapproval in **Kennedy**. We see no reason, particularly as the Tribunal expressly referred to and relied upon **Malone** and **Leander**, to differ from its conclusion, by reference to foreseeability. Further we see no reason, bearing in mind the Tribunal's findings in that case, to conclude that, in whatever respect the ECtHR was of the view in **Liberty v UK** that the Court's jurisprudence had *evolved* since **Christie**, the Tribunal's conclusions as to accessibility and foreseeability in that case should be regarded as in any way flawed.

88. In **Liberty v UK** the ECtHR in fact came to consider the same factual complaint as the Tribunal was addressing in **British Irish Rights Watch** in 2004, in its judgment of July 1 2008; but in the event the Court considered the proceedings by reference to an earlier application, made by reference to the predecessor Act of the RIPA, namely the Interception of Communications Act 1985 ("IOCA"). Not only was the Court addressing the earlier statutory regime, but it was also, for the same reason, addressing a regime which did not have the Code under s.71 of RIPA referred to in paragraphs 69 and 75-76 above, which had not been brought into force under the old Act.

89. The somewhat peculiar circumstances were thus that the Court was considering the case without the benefit of the Code, that the Respondent Government was having to justify the statutory measures without, and antedating, the Code; the finding was, perhaps not surprisingly, that, without the Code, the interference with the applicant's

rights under Article 8 was not therefore *in accordance with the law*. In paragraph 65 of the **Liberty v UK** judgment the Court pointed out that IOCA conferred a wide discretion, and in paragraph 66 that the *arrangements*, which the Government described as applying to the processes of selection for examination, dissemination and storage of intercepted material, *were not contained in legislation or otherwise made available to the public*. The Court concluded:

> "*68 . . . In the United Kingdom, extensive extracts from the Code of Practice issued under s.71 of the 2000 Act are now in the public domain, which suggests that it is possible for the state to make public certain details about the operation of a scheme of external surveillance without compromising national security.*"

90. This was thus a decision in relation to the s.8(4) warrant, but made on the basis set out above, which clearly sets out, at the very least, a strong inference that with the Code the situation would have been different. On the other hand, once again, of the Four Questions set out before us, the first, second and fourth were not before them, although the third plainly was, since **Weber** was considered.

91. The ECtHR did consider RIPA in **Kennedy**. This was an application by Mr Kennedy to the Court arising out of the dismissal by this Tribunal of a complaint by him relating to a s.8(1) warrant. Although the Court plainly did not therefore consider s.8(4) in any detail, it did consider those parts of the Statute and of the Code which apply to both warrants, and the statutory scheme, including oversight by the Commissioner and this Tribunal. It concluded as follows in paragraph 169:

> "*In the circumstances, the Court considers that the domestic law on interception of internal communications together with the clarifications brought by the publication of the Code indicate with sufficient clarity the procedures for the authorisation and processing of interception warrants as well as the processing, communicating and destruction of intercept material collected. The Court further observes that there is no evidence of any significant shortcomings in the application and operation of the surveillance regime. On the contrary, the various reports of the Commissioner have highlighted the diligence with which the authorities implement RIPA and correct any technical or human errors which accidentally occur. Having regard to the safeguards against abuse in the procedures as well as the more general safeguards offered by the supervision of the Commissioner and the review of the IPT, the impugned surveillance measures, insofar as they may have been applied to the applicant in the circumstances outlined in the present case, are justified under Article 8(2).*"

Again, of the Four Questions before us, the first, second and fourth were not asked of the Court: the third plainly was, albeit in the context of a s.8(1) warrant.

92. Before turning to consider the questions before us, we first further address the Commissioner's Report. Based upon the investigations he carried out, he reached conclusions as to the operation of s.8(1) and s.8(4) and the warrants thereunder, and the Respondents' retention, storage and destruction policies and procedures, including whether there is an indiscriminate or excessive retention of intercept (particularly in paragraphs 3.55-56 and 6.5 and 6.6), and (in paragraphs 6.6.8-9) he expresses his own caveats. Leaving aside his factual findings, his Report illustrates the scope and depth of his oversight duties and activities. It also discloses, by its very publication, considerable information into the public domain so far as compatible with the needs of national security. The role of the Commissioner, and his clearly independent and fully implemented powers of oversight and supervision, were addressed in detail with approval by the ECtHR (notwithstanding what was said in paragraph 67 of **Liberty**) in **Kennedy**, at paragraphs 57 to 74, 166 and 168. We make clear, however, that we reach our own conclusions, not least in the circumstances set out in paragraphs 45 and 46 above.

93. We turn now to the first question which we have set out in paragraph 80 above, relating to *external/internal* communications. As is clear from RIPA, s.8(1), the targeted warrant is to be directed to one person or to a single set of premises: presumably that is likely to be in the UK, but it does not need to be. The s.8(4) warrant is not so targeted and not so limited, but can extend to substantial quantities of communications, not just as this Tribunal discussed in the **British Irish Rights Watch** case, but contained in 'bearers' carrying communications to many countries. By s.8(5), set out above, the communications that are permitted to be intercepted are (a) *external* communications and (b) by virtue of s.5(6) and s.8(5)(b) all *related communications* data and any other communications (i.e. *internal communications*) which are necessarily intercepted in order to do what is authorised by the warrant. As to this, the inevitable intermingling of *external* and *internal* communications was apparent in Lord Bassam's statement in Parliament (paragraph 68 above) and is addressed in paragraph 5.1 of the Code (paragraph 69 above).

94. The following is common ground between the parties, as Mr Ryder, who bore the brunt of these submissions, made clear:

i) It is impossible to differentiate at the 'interception' stage between *external* and *internal* communications, which will all be carried within the same 'bearer'.

ii) It is impossible to know at the time of interception, i.e. in the course of transmission, what is *external* and what is *internal*, and such has always been the case:

a) The definition of *interception* in s.2(2) of RIPA refers (as set out above) to transmission "*to a person other than the sender or intended* [our underlining] *recipient of the communication*" i.e. it is (or may be) intercepted before receipt.

b) Again as set out above, s.2(7) provides that transmission of a communication is to include the time when the communication has arrived but is being stored pending collection by the intended recipient – e.g. stored on an email server.

iii) It is inevitable that, when a telephone call is made from a mobile phone or IPhone, or an email is sent to an email address, it will not necessarily be known whether it will be received in the United Kingdom or in the course of travel or at a foreign destination. It is accepted that once and if received abroad by the intended recipient it will be an *external* communication, even if the sender did not know, when he or she made the call or sent the email, that that was to be the case.

95. It is also common ground that the interception under a s.8(4) warrant (what the Respondents call "Stage one") occurs before any question of selection for examination (what the Respondents call "Stage two") arises under s.16. As Mr Ryder put it, the relevance of the *internal/external* distinction has no relation to the s.16 examination, when a communication may be accessed and read. The identification of communication links for interception is, as he described it, a 'generic' exercise, not an exercise which is done specifically case by case and communication by communication.

96. This is the context of the Claimants' case, namely that there has been a sea-change in technology since 2000 which means that, by virtue of the blurring of the distinction between *external* and *internal* communications, s.8(4) is no longer, as the ugly phrase has it, based upon a misquotation of the Sale of Goods Act, 'fit for purpose'. The background upon which the Claimants rely is that there are (as is obviously the case) many more emails and other similar communications since 2000 (and certainly less landline communications), and that, in addition, there are highly developed and greatly used new forms of communication through Facebook, Twitter and Google, in its various facets. They submit that, given that the servers, particularly for Facebook and Google, are likely to be in the United States, there is likely to be substantially more *external* communication than there was in 2000, particularly so by virtue of what he submits to be an incorrect interpretation of what is an *external* communication adopted by Mr Farr and disputed by Mr Eric King, the Deputy Director of Privacy, who has also filed a witness statement.

97. It is necessary to indicate the ambit of this dispute:

i) There is no dispute that emails sent to an email address will still be likely to be in transmission when intercepted (see above). There is also no dispute that if an email is sent to more than one addressee, and one of the addressees is abroad, then there is an *external* communication to that addressee, even if not to the others. It is also not disputed, in accordance with Lord Bassam's statement and the Code, that if an email is sent via a server which is abroad, such as Hotmail, that that is not an *external* communication if the addressee receives it in the UK, irrespective of the fact that it has been transmitted to, and stored, until called down, on a US server.

ii) It is also not disputed that if Google is used as a search engine to navigate the internet in order to find a web page or addressee abroad, for example such as Wikipedia, then, if e.g. Wikipedia is abroad, that is *external*.

iii) It is also not in dispute that a Facebook message which is posted to a US server and picked up by a recipient abroad is an *external* communication.

iv) The disputes between Mr Farr (paragraphs 132 to 141) and Mr King (paragraphs 32 to 55) revolve primarily around (i) other uses of Google, where Mr Farr considers that a message is sent to Google or a Google entity/platform in the United States, and a message is then sent back (ii) other uses of Facebook – e.g. placing a message on the US Facebook page or (iii) Twitter. In each of these cases Mr King considers that (absent the common ground referred to above) the communications are or remain *internal*. It was apparent that much of the dispute related to the difference between what is interpreted as a "*communication*" within s.81 of RIPA, which includes the definition, at (c), that communication includes "*signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus.*"

98. It is clear to us that this dispute, although it is one that plainly cannot be resolved by us on disputed witness statements, is, in the context, of very limited ambit:

i) Of the respects in which it is common ground that *external* and *internal* communications are either intermingled or impossible to differentiate at the interception stage (set out in paragraphs 94 to 95 above), all were present, foreseeable and foreseen at the time of the passage of RIPA by Parliament in 2000.

ii) There is in any event no dispute about the communications which will be contained on the same bearers, namely incoming communications into the United Kingdom from abroad. They are likely to be substantial, and will qualify as *external* communications, thus diminishing yet further the proportionality of consideration of the intermingling of the outgoing communications.

iii) Although the changes in technology are substantial, they do not seem to us, given the common ground to which we have referred, to constitute any material addition to the quantity (or proportion) of communications which either could or could not be differentiated as being *internal* or *external* at the time of interception.

99. Mr Eadie submits, if necessary, that he can rely upon the concept of the "*always speaking statute*", referred to by Lord Bingham of Cornhill in **R (Quintavalle) v The Health Secretary** [2003] 2 AC 687, and addressed in that and the subsequent **Quintavalle** case in [2005] 2 AC 561, so far as concerns the meaning of the word *external*.

100. It appears to us that there is no need to adopt that concept in order to be satisfied that "*external communications*" for the purposes of s.8(4) and s.8(5) of RIPA still mean the same and have the same effect. Even if, as is suggested, more (outgoing) communications are *external*, or there is some genuine dispute, capable of being resolved if necessary, as to its meaning in relation to some or many of such communications, insofar as the Claimants complain of the sweep up of telecommunications cables, that has always been the case. The same total quantity of *internal* and *external* communications is likely to have continued to be intercepted, and permitted in the event of an appropriate s.8(4) warrant, complying inter alia with the concepts of necessity and proportionality, and properly authorised

by the Secretary of State, as provided by s.8(5) and s.5(6) and the Code. There is no radical change, notwithstanding the dispute about some parts of the communications. We are not satisfied that any provision in RIPA has become itself ambiguous. If Mr Farr's interpretation is incorrect, then at worst it has, as Mr Jaffey himself submitted, "*accelerated the process of more things in the world on a true analysis being external than internal*", but at the 'generic' stage of interception.

101. In our judgment, there are only two consequences of this 'acceleration', given that, as is clear, and set out above, the distinction only arises at "Stage one", when there is no examination:

i) All communications, whether they be *external* or *internal*, intercepted by s.8(4) warrant come to be considered for examination by reference to s.16 of RIPA, to which we turn below. It is that section which does what Mr Ryder called in argument the "*heavy lifting*".

ii) The only impact, in our judgment, that could arise would be if Mr Farr's interpretation were incorrect, and it were the case that a warrant under s.8(4) had been granted by express reference to it, and thus on an arguably false basis. However, given that such warrants and such interception would be likely to be applied for on a "*generic basis*", and a bearer sought to be intercepted would be bound to include, for the reasons that we have given, a substantial quantity of communications which would be on any basis either *external* or at any rate inchoate *external* communications in the sense discussed above, it would seem to us not to follow that any such warrant would be so flawed. Plainly if a warrant, for example a warrant issued impacting upon these Claimants (if in due course it later becomes apparent, in subsequent closed consideration or otherwise, that there has been such a warrant) were applied for or granted on the basis of express reliance upon such an arguably flawed basis, then it would be at that stage that the question would arise, and would need to be resolved.

102. We resolve the First Question in favour of the Respondents. No difference of view as to the precise definition of *external* communications renders the s.8(4) regime contrary to Article 8(2).

103. The Second Question relates to s.16. There is no doubt that s.16 is to be regarded as a safeguard for some of those whose communications have been intercepted under a s.8(4) warrant, either by reference to *external* communications or to those *internal* communications collaterally included under the warrant, so far as the effect of s.16(2) is concerned. By that subsection (in general terms), communications so intercepted could not be accessed (read, looked at or listened to) by reference to an individual known to be in the UK in relation to communications sent by him or to him. The sideline to the Statute refers to s.16 as an "*extra safeguard in the case of certificated warrants*", and the Commissioner has described it as a safeguard in paragraph 6.5.54 of his Report. We have referred to Mr Ryder's reference to s.16 doing the "*heavy lifting*", and we do not accept that it is simply, as Mr Eadie put it in reply submissions, "*procedural*". We shall return later to the context in which he so submitted.

104. There are two respects in which the Claimants submit that s.16 fails as a safeguard. The first was addressed by Mr Ryder by reference to the terms of s.16(2). He submits that the two provisos there contained in relation to access to *intercepted material* are insufficient. As to (a), that material will not be accessed according to a factor which is *referable to* an individual who is *known* to be in the UK, he submits that this is inadequate. *Referable to* is not wide enough or not sufficiently clear; and *known to be,* as opposed to *suspected to be,* is too low a hurdle.

105. We do not accept either of these submissions. *Referable to* is in our judgment a wide term, and generally accepted to be so as a matter of statutory construction, and would prohibit the use of terms which were connected with, or could lead to the identity of, the individual by the use of names, nicknames, addresses, descriptions or other similar methods. If it was more specific, it would become unworkable. To impose an obligation upon the Respondents not to read the communication if the presence of the individual in the UK is simply *suspected* would impose far too high an obligation, particularly in the course of extended examination of substantial numbers of communications. The ability to use the *communications data/metadata* (to which we return below) would render it a manageable task to ascertain whether the individual could be said to be *known* to be in the UK. As for the concomitant subparagraph (b), we do not consider that this is too limited a restriction: the aim is to prevent access to communications sent by or sent to an individual who is in the United Kingdom.

106. We turn to the second criticism of s.16, which was the subject of a two-pronged attack by Mr Ryder and Mr Jaffey. Mr Ryder pointed out that s.16 does not exclude examination of the *related communications data*, permitted by s.5(6)(b) and s.8(5) to be included with the communications under a s.8(4) warrant, because the words *intercepted material*, as defined in s.20 (set out above), refers to "*the contents of any communications intercepted by an interception to which the warrant relates*", and thus not to *communications data* (separately there defined).

107. Mr Jaffey further points out that, once the *communications data* could be examined, such examination was not limited to the purpose for which the warrant had been given, but could be carried out for any purpose falling within s.5(3)(a)(b) or (c) – national security, preventing or detecting serious crime, safeguarding the economic wellbeing of the UK. This is therefore a much less satisfactory safeguard than if it extended to the exclusion of examination of contents and *related communication data*.

108. Communications data under RIPA are explained in Privacy's Reply (paragraph 21) as including the following:

> "*Data associated with emails:*
>
> - *Sender's name, email, and IP address*
> - *Recipient's name and email address*
> - *Date, time, and time zone in which email is sent and received*
>
> *Data associated with mobile phones:*

- *Phone number of every caller*
- *Serial numbers of phones involved*
- *Time of call*
- *Duration of call*
- *Cell site location*

Data associated with web browsers:

- *Activity including pages the user visits and when visited*
- *User IP address, internet service provider, device hardware details, operating system, and browser version.* "

109. Mr King and Mr Brown, Associate Professor at the Oxford Internet Institute, who also made a witness statement on behalf of Privacy, have explained how useful metadata can be in supplying information about the location and correspondents of the sender, derived from the header of an email, including its timing, particularly in aggregation with other such data. The Claimants point to the fact that communications data have been the subject of protection under Article 8 in **Copland v UK** [2007] 45 EHRR 37 and, by analogy with EU law (and the Charter of Fundamental Rights of the European Union), to be derived from **Digital Rights Ireland v Minister for Communications and Others** [2014] ECLI:EU:C:2014:238.

110. The Claimants submit that, without the same protection for communications data as is extended to contents, such data can be used for what they call 'Big Data', namely the building up of a database, whose retention can then be justified by reference to s.15(3) and (4), on the basis that it was or was likely to become necessary for one of the permitted purposes. The Claimants submit that Mr Eadie was trying to play down the safeguard as merely '*procedural*' so as to avoid confessing the weakness which the ability to access metadata, related to communications which could not themselves be accessed, revealed in his defence of the system.

111. The Respondents counter as follows. First, although they may be driven to accept that Convention jurisprudence allows that there can be interference with Article 8 by reference to the storing of metadata, nevertheless there is no authority for the kind of drastic proposition of exclusion of access to metadata for which the Claimants are contending. In **Digital Rights**, the European Court made it clear, in paragraphs 59 to 60 of its judgment, that its invalidating of the Directive which required storage (for any period) of metadata by the communications networks was on the ground of an absence of "*any relationship between the data whose retention is provided for and a threat to public security"* and "*any objective criterion by which to determine limits of the access of the competent national authorities to the data*". That is plainly not so here, where the s.8(4) warrant will have been granted. Mr Eadie submitted that, notwithstanding the evidence of Mr King and Mr Brown, interference with communications data is plainly less intrusive than access to the contents of the communications, and less informative. In that context, he submitted

that although in **Malone**, at paragraph 84, the Court decided that access to metering information amounted to an interference with an Article 8 right, it plainly concluded that it was to be "*distinguished from interception of communications*", by virtue, he says, of its lesser degree of intrusion. He referred also to the passage in **Uzun,** which we have quoted in paragraph 34 above, as supporting the same conclusion.

112. As for the justification for any interference with Article 8, Mr Eadie submitted as follows:

i) S.16(2) is clearly in *accordance with law*. He set out the reasons for the exemption of communications data, namely that the metadata enabled compliance with the difficult task imposed by s.16(2) with regards to contents. He submitted as follows in paragraph 121.5 of his skeleton argument:

> "*(a) In order for s. 16 to work as a safeguard in relation to individuals who are within the British Islands, but whose communications might be intercepted as part of the s8(4) Regime, the Intelligence Services need information to be able to assess whether any potential target is "for the time being in the British Islands" (for the purposes of s. 16(2)(a)). Communications data is a significant resource in this regard.*
>
> *(b) In other words, an important reason why the Intelligence Services need access to related communications data under the s.8(4) Regime is precisely so as to ensure that the s. 16 safeguard works properly and, insofar as possible, factors are not used at the selection that are - albeit not to the knowledge of the Intelligence Services - "referable to an individual who is ... for the time being in the British Islands".*"

This was, he submitted, plainly the express, and sensible, purpose of Parliament.

ii) The structure of s.16 is quite clear, and amounts to the safeguard intended in respect of the operation of the s.8(4) warrant discussed above. The existence of the exemption for communications data is nothing new, and had been intended.

iii) Communications data are fully protected by the safeguards of s.15(2) handling and (3) destruction, etc. The protection for communications data is thereby established, and such protection is only less than for contents, by virtue of s.16(2), in relation to some communications. If this could be said to be something less than full **Weber** requirements, then, if, contrary to his submissions, **Weber** applies to communications data at all, a lesser protection is permitted, so far as communications data is concerned, and in any event the exemption was fully justified, as above.

113. Mr Ryder did not challenge the suggestion that being able to look at communications data in order to determine whether someone is in the UK could be of use, but his submission was twofold. First that that could be achieved by making an exception to provide for the use of metadata for that purpose. That seems to us to be an impossibly complicated or convoluted course. His second argument was as set out above, namely that metadata so obtained could be used (and used as described by Mr Jaffey) to build up a database – what we described in the course of his submissions as a '*just in case*' database, which could still comply with s.15(3) and (4) of RIPA.

114. We conclude that although the **Weber** requirements do extend to protection in respect of communications data, for the reasons set out by the Respondents there is such protection or safeguard by reference to s.15, and, insofar as there is, in the particular circumstances governed by s.16, greater protection in certain respects for communications than for communications data, that difference is justified and proportionate by virtue of the use of that communications data for the purpose of identifying the individuals whose intercepted material is to be protected by reference to s.16(2)(a). That answers the Second Question. With regard to the retention of communications data in a database, we return to this matter below.

115. We turn to consider whether the system, leaving aside s.16, is a sufficient compliance with **Weber** and *in accordance with law*. In our recitation of the relevant paragraph, 95, of **Weber** (in paragraph 33 above) we inserted numbers, and have found it convenient to refer to the six **Weber** requirements as **Weber** 1, **Weber** 2, etc. We are content to follow, and agree with, the observation of the ECtHR in paragraph 160 of its judgment in **Kennedy** that **Weber** 1 and **Weber** 2 overlap, and we shall therefore consider them together.

116. So far as a s.8(4) warrant is concerned, the following seems to be clear:

i) The reference to "*national security*" is a sufficient description: see **Esbester** at CD 74 and **Kennedy** at paragraph 159, where the ECtHR stated:

> "*. . .The applicant criticises the terms "national security" and "serious crime" as being insufficiently clear. The Court disagrees. It observes that the term "national security" is frequently employed in both national and international legislation and constitutes one of the legitimate aims to which Article 8(2) itself refers. The Court has previously emphasised that the requirement of "foreseeability" of the law does not go so far as to compel States to enact legal provisions listing in detail all conduct that may prompt a decision to deport an individual on "national security" grounds. By the nature of things, threats to national security may vary in character and may be unanticipated or difficult to define in advance.*"

ii) The absence of targeting at 'Stage one' is acceptable and inevitable. This was so in the **Weber** case itself (by reference to the 'strategic monitoring' being there addressed). In **Liberty v UK** the Court criticised the "*virtually unfettered*" nature of the legal discretion granted to the executive for the physical capture of *external* communications (paragraph 64), but would

appear, rather as in **Weber** itself, to have concluded that the defect was the failure to set out with sufficient clarity the scope or manner of such exercise (paragraph 69), and in particular the absence of the Code, which by then had been published (paragraph 68).

iii) The Code was plainly acceptable so far as the s.8(1) warrant is concerned, when it was fully considered by the Court in **Kennedy**. Insofar as the Code was referred to in **Liberty v UK** (at paragraph 68), no specific complaints were made or problems identified.

iv) We heard considerable argument by Mr Ryder as to the appropriateness of paragraph 5.2 of the Code. Of course it may be that in a given case the particulars supplied in an application for a warrant would be found to have been insufficient, although we note the Commissioner's duties as to the supervision and inspection of such warrants. We find that on its face paragraph 5.2 is impressive, and that the provisions of paragraph 5.2, particularly together with those of paragraphs 2.4 and 2.5 and 5.3, 5.4, 5.5 and 5.6 referred to in paragraph 56 above, dealing with necessity and proportionality, are satisfactory.

v) There is in our judgment no call for search words to be included in an application for a warrant or in the warrant itself. It seems to us that this would unnecessarily undermine and limit the operation of the warrant and be in any event entirely unrealistic. It does not appear to us to be in any way demanded by the **Weber** requirements. So far as the facts of **Weber** are concerned, it appears that some form of notification of search words was required under the German domestic law. But the facts of **Weber** are of course not prescriptive, and, particularly as the outcome was that the Court found that the application i n **Weber** was "*manifestly unfounded*", it does not impose on any other legislature the requirement either to have some system of search words, (or indeed to adopt another matter which formed part of the facts of **Weber**, namely a provision for some form of notification to the target(s) that there is or has been a warrant – a proposition that was not argued before us, and in our judgment rightly so). We agree with the conclusion of this Tribunal in **British Irish Rights Watch** that such a course would be both risky and pointless.

vi) There is also in our judgment no basis for objection by virtue of the absence for judicial pre-authorisation of a warrant. The United Kingdom system is for the approval by the highest level of government, namely by the Secretary of State. The absence of such judicial authorisation in **Liberty v UK** was not a matter of criticism, and the Court in **Kennedy** concluded (at paragraph 167) that, whereas "*it has previously indicated that in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge*", it was satisfied, not only by virtue of the existence of the Commissioner (then, as now, a distinguished retired Judge), which it had examined at length (as referred to in paragraph 92 above), but also by virtue of the fact that "*the Court highlights the extensive jurisdiction of the IPT to examine any complaint of unlawful interception*". This approval of the absence of judicial pre-authorisation was further addressed by the Court in **Telegraaf Media** at paragraph 98.

vii) We have seen nothing to cause us to take a different view from that of the Tribunal in **British Irish Rights Watch**, particularly as to the matters set out in (ii), (v) and (vi) above, which the Tribunal then specifically addressed.

117. We turn to the consideration of the balance of the **Weber** requirements, namely (3) duration of the interception (4) examination, usage, and storage (5) disclosure and (6) destruction. Such requirements, or safeguards, are addressed (with the exception of s.16, to which we have referred) in s.15, which relates both to the contents and to communications data. These provisions are supported by the following:

i) The Code. The Code (save for its earlier absence) was not a subject of specific criticism in **Liberty v UK**, and, relevantly, because s.15 applies to both s.8(1) and s.8(4) warrants, was approved in **Kennedy**.

ii) The *arrangements*. These are provided for in sub-sections 15(1), (5) and (6). There are also the *arrangements* referred to in paragraph 42 above by reference to ISA, SSA and CTA, and DPA; and the Code itself makes reference to the *arrangements* in force with relation to s.15(2) and s.15(3) and specifically with regard to s.16, all of which must be recorded in the records referred to in paragraph 5.17 of the Code.

118. So far as such *arrangements* are concerned, they are, in Mr Eadie's description, "*below the waterline*", and it is true to say that in paragraph 95 of **Weber**, in setting out the **Weber** requirements, the ECtHR referred to the fact that it "*has developed the following minimum safeguards that should be set out in statute law*". However:

(a) The ECtHR in paragraph 68 of **Malone** stated that "*the detailed procedures and conditions to be observed do not necessarily have to be incorporated in rules of substantive law*", which must "*indicate the scope of* [the] *discretion conferred upon the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference*". This is repeated in **Bykov**, in the passage cited at paragraph 37 above.

(b) It is clear that actual statute is not required – hence the approval of the Code in **Kennedy** (and its anticipated approval in **Liberty v UK)**. The Code itself, as set out above, refers to the underlying *arrangements*. Whether or not the Court in **Liberty v UK** considered the Code in detail, and thus noticed the reference in it to the *arrangements*, the way the Court dealt with the Code was by noting (in paragraph 68) that "*it is possible for a state to make public certain details about the operation of the scheme of external surveillance without compromising national security*". The Court in **Kennedy**, in specifically approving the availability of reference to the Code, approved (at paragraph 156) its earlier judgment in **Silver,** reference to which had formed part of the conclusion of this Tribunal in **British Irish Rights Watch**.

119. It is plain that what underlies the **Weber** requirements is that which the Court firmly articulates in **Weber** itself at paragraph 106, namely:

> "*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).*"

This is reiterated in paragraph 77 of the Court's judgment in **Association for European Integration and Human Rights v Bulgaria** App No. 62540/00 28 June 2007.

120. In that context it is made clear by the Court in **S v UK** [2009] 48 EHRR 1169 at paragraph 96 that: "*The level of precision required of domestic legislation – which cannot in any case provide for every eventuality – depends to a considerable degree on the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed*". We have already considered and set out in paragraphs 38 and 40 above the relevant passages of the Court's judgment in **Leander** and the Commission's in **Esbester**. We have no doubt that we are entitled to look at the rules, requirements and arrangements, both those expressly set out in statute or in the Code and those set out in more detail in *arrangements below the waterline*, but which are sufficiently signalled in publicly available documents to ensure both that any abuse is avoided and a sufficient degree of accessibility and foreseeability is secured.

121. This is in our judgment not only consistent with the decisions of the ECtHR to which we have referred, but, although, as is clear from paragraph 67 of **Liberty v UK**, oversight (by the Commissioner) was not enough of itself, it is coupled with the approval by the Court of the oversight arrangements in place in respect of RIPA. In addition to this Tribunal, there is also the ISC, to which the Court in **Kennedy**

did not expressly refer, and which, notwithstanding Ms Brimelow's critique is, we are satisfied, robustly independent, and now additionally fortified by the provisions of the JSA which were, according to their Report, referred to in paragraph 6 above, broadly in line with the changes which they themselves had previously recommended to the Government. As for the Commissioner, of particular relevance is his duty under s.57(1)(d) of RIPA to keep under review the adequacy of the arrangements by virtue of which the duty imposed on the Secretary of State by s.15 are sought to be discharged, and, by reference to s.58(3), his duty if it at any time appears to him "*that any arrangements by reference to which the duties imposed by s. . . 15 . . have* [been] *sought to be discharged are proved inadequate in relation to any matter with which the Commissioner is concerned*, *to make a report to the Prime Minister with respect to those arrangements.*"

122. We remain of the same view as this Tribunal in **British Irish Rights Watch** (at paragraphs 36 and 37) that it is not necessary that the precise details of all the safeguards should be published, or contained in legislation, delegated or otherwise.

123. Against that background, we consider **Weber** 3, 4, 5 and 6. We have set out the relevant sections of RIPA in paragraphs 63-67 and 74 above, and set out and referred to the relevant parts of Chapters 5 and 6 of the Code in paragraphs 69 and 75 above. The Court considered and approved these provisions at paragraphs 161 and 163 to 165 of its judgment in **Kennedy**, as follows:

> "*161. In respect of the duration of any telephone tapping, the Act clearly stipulates, first, the period after which an interception warrant will expire and, second, the conditions under which a warrant can be renewed. Although a warrant can be renewed indefinitely, the Secretary of State himself must authorise any renewal and, upon such authorisation, must again satisfy himself that the warrant remains necessary on the grounds stipulated in section 5(3). In the context of national security and serious crime, the Court observes that the scale of the criminal activities involved is such that their planning often takes some time. Subsequent investigations may also be of some duration, in light of the general complexity of such cases and the numbers of individuals involved. The Court is therefore of the view that the overall duration of any interception measures will depend on the complexity and duration of the investigation in question and, provided that adequate safeguards exist, it is not unreasonable to leave this matter for the discretion of the relevant domestic authorities. The Code explains that the person seeking the renewal must make an application to the Secretary of State providing an update and assessing the value of the interception operation to date. He must specifically address why he considers that the warrant remains necessary on section 5(3) grounds. Further, under section 9(3) RIPA, the Secretary of State is obliged to cancel a warrant where he is satisfied that the warrant is no longer necessary on section 5(3) grounds. There is also provision in the Act for specific factors in the schedule to the warrant to be*

deleted where the Secretary of State considers that they are no longer relevant for identifying communications from or to the interception subject. The Code advises that the duty on the Secretary of State to cancel warrants which are no longer necessary means, in practice, that intercepting agencies must keep their warrants under continuous review (see paragraph 55 above). The Court concludes that the provisions on duration, renewal and cancellation are sufficiently clear.

. . .

163. As to the general safeguards which apply to the processing and communication of intercept material, the Court observes that section 15 RIPA imposes a duty on the Secretary of State to ensure that arrangements are in place to secure any data obtained from interception and contains specific provisions on communication of intercept material. Further details of the arrangements are provided by the Code. In particular, the Code strictly limits the number of persons to whom intercept material can be disclosed, imposing a requirement for the appropriate level of security clearance as well as a requirement to communicate data only where there is a "need to know". It further clarifies that only so much of the intercept material as the individual needs to know is to be disclosed and that where a summary of the material would suffice, then only a summary should be disclosed. The Code requires intercept material, as well as copies and summaries of such material, to be handled and stored securely to minimise the risk of threat or loss. In particular, it must be inaccessible to those without the necessary security clearance. A strict procedure for security vetting is in place. In the circumstances, the Court is satisfied that the provisions on processing and communication of intercept material provide adequate safeguards for the protection of data obtained.

164. As far as the destruction of intercept material is concerned, section 15(3) RIPA requires that the intercept material and any related communications data, as well as any copies made of the material or data, must be destroyed as soon as there are no longer any grounds for retaining them as necessary on section 5(3) grounds. The Code stipulates that intercept material must be reviewed at appropriate intervals to confirm that the justification for its retention remains valid.

165. The Code also requires intercepting agencies to keep detailed records of interception warrants for which they have applied an obligation which the Court considers is particularly important in the context of the powers and duties of the Commissioner and the IPT."

We have not cited paragraph 162, because that did not relate to the conclusions of the Court which are common to both s.8(1) and s.8(4) warrants.

124. There is no call for us to reconsider those conclusions. We need to deal only with any matters which have been freshly contended before us. Amendments to the Code have been proposed and published. Mr Farr refers to their origin as follows:

> "*161. In March 2010, the Home Office published on its website a revised draft of the Code . . . the draft was subject to a targeted consultation, lasting 3 months. The aim, in response to the* ***Liberty v UK*** *judgment was to make public, to the extent possible, further information as to how material gathered under s.8(4) warrant comes to be examined following interception. The proposed changes were mainly to chapters 5 and 6. Some minor corrections and updates were also made.*"

In the event, the amended Code was never brought into force. The Claimants, while recognising that there were thus some proposed changes, do not assert that those changes would resolve their complaints against the existing Code. We have considered the amendments, and although they may constitute improvements in methodology and supervision, which we encourage, we do not consider that the additions call into question the adequacy of the existing Code.

125. In the light of our careful consideration of the decisions of the ECtHR and our conclusions in paragraphs 117–124 above, we conclude that, as was the case with the Prism Issue, we need to be satisfied that 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, that they are sufficiently accessible, bearing in mind the requirements of national security, and that they are subject to oversight.

126. The Respondents have agreed at and after the closed hearings, in the circumstances described in paragraph 10 above, also to make the following further Disclosures, by way of a summary of the evidence in Closed (the numbering continues from that in paragraph 47):

3. *Those of the Intelligence Services that receive unanalysed intercepted material and related communications data from interception under a s.8(4) warrant have internal "arrangements" that require a record to be created, explaining why access to the unanalysed intercepted material is required, before an authorised person is able to access such material pursuant to s.16 of RIPA.*

4. *The internal "arrangements" of those of the Intelligence Services that receive unanalysed intercepted material and related communications data from interception under a s.8(4) warrant specify (or require to be determined, on a system-by-system basis) maximum retention periods for different categories of such data which reflect the nature and intrusiveness of the particular data at issue. The periods so specified (or determined) are normally no longer than 2 years, and in certain cases are significantly shorter (intelligence reports that draw on such data are treated as a separate category, and are retained for longer). Data may only be retained for longer than the applicable maximum retention period where prior authorisation has been obtained from a senior*

official within the particular Intelligence Service at issue on the basis that continued retention of the particular data at issue has been assessed to be necessary and proportionate (if the continued retention of any such data is thereafter assessed no longer to meet the tests of necessity and proportionality, such data are deleted). As far as possible, all retention periods are implemented by a process of automated deletion which is triggered once the applicable maximum retention period has been reached for the data at issue. The maximum retention periods are overseen by, and agreed with the Commissioner. As regards related communications data in particular, Sir Anthony May made a recommendation to those of the Intelligence Services that receive unanalysed intercepted material and related communications data from interception under a s8(4) warrant, and the interim Commissioner (Sir Paul Kennedy) has recently expressed himself to be content with the implementation of that recommendation.

5. *The Intelligence Services' internal "arrangements" under SSA, ISA and ss.15-16 of RIPA are periodically reviewed to ensure that they remain up-to-date and effective. Further, the Intelligence Services are henceforth content to consider, during the course of such periodic reviews, whether more of those internal arrangements might safely and usefully be put into the public domain (for example, by way of inclusion in a relevant statutory Code of Practice).*

127. The Claimants made the following submissions in response to these further Disclosures, in addition both to those set out in paragraphs 49-50 above and to repeating and adopting those they made during the open hearing.

128. First they submitted that the further information supplied was not adequate, being contained neither in statute nor in the Code pursuant to s.71 of RIPA. Their submission was that if the *arrangements* described were not contained in statutory form or in a code required to be laid before Parliament then it could be changed and was thus changeable at an '*executive whim*', by which they referred to the possibility of change in administrative policy, somewhat pejoratively, given the inevitable constraints inherent in any such changes. The *arrangements* were therefore not suitable to be taken into account in consideration of whether they were *according to law* or *prescribed by law*. They referred to **Malone** at paragraphs 67, 68 and 76 and **Liberty** at paragraphs 60-61 and 68.

129. We are satisfied that this proposition is not to be derived from those authorities, taken together with the other authorities to which we have referred in detail in paragraphs 37-38, 85-88, 118-119 and 121-124 above. 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 (see in particular paragraph 118(a) above). This is particularly so where:

(i) The Code, which was the subject of consideration by the ECtHR, latterly in **Kennedy**, itself refers to a number of *arrangements* not contained in the Code, and even in **Liberty** (at paragraph 68) the ECtHR required the disclosure of only "*certain details*".

(ii) There is the system of oversight, which the ECtHR has approved, which ensures that such *arrangements* are kept under constant review.

130. The Claimants further pointed out, and relied upon the fact, that in **Belhadj**, referred to in paragraph 54 above, in which issue is joined between the Respondents and those claimants (who include, among others, Amnesty) as to the adequacy and lawfulness of the Respondents' treatment of intercepted material which may be subject to legal and professional privilege, in reply to a lengthy Request for Information served by the claimants, the Respondents supplied a document (referred to in paragraph 54 above) amounting to a redacted extract from the GCHQ Compliance Guide. This contained a gisted passage summarising GCHQs "*overall policy*" as to "*retention limits*". The Claimants submit that they should have been entitled to see such a document in this case, and suggest that if it did not offend against national security to supply such document in **Belhadj** then it would not do so in this case.

131. The **Belhadj** case is very different. It has not yet reached a hearing, but it is still at the interlocutory stage, and is limited in its scope, as discussed. Apart from a query as to terminology, by which we are not persuaded, it is not suggested by the Claimants that the gist of the GCHQ policy (save that it also includes a provision for retention of certain material to comply with legal requirements) shows anything materially different from, inconsistent with or additional to the gist that has been supplied of the closed evidence in this case. What has happened in the present case is that there has been a closed hearing, at which pursuant to s.68(6) of RIPA the Respondents were obliged to and did provide the relevant documents. Within the limits of the same concerns about national security, a summary has then been provided by the Respondents of the evidence given and documents produced at the closed hearing, and disclosed to the Claimants. That summary of the evidence is consistent with the summary provided in **Belhadj**. We do not see either that there has been inconsistency or that the Claimants have been prejudiced or treated materially differently from the claimants in **Belhadj**.

132. Two further submissions were made with regard to the Disclosure:

(i) Whereas in paragraph 3.56 of the Commissioner's Report, one of the paragraphs referred to in paragraph 92 above, the Commissioner stated that he had yet to satisfy himself fully that some of the retention periods were justified, paragraph 4 of the Disclosure states that he has now made a recommendation (said to have been implemented). This is not evidence which could have been given in any detail in open, and is sufficiently summarised by that paragraph in the Disclosure.

(ii) Privacy relies on paragraph 5 of the Disclosure as indicating that there is more that could be disclosed. It states that there may be yet further review, resulting in additional disclosure of matters which may in the future be concluded not to be prejudicial to national security. Plainly, with the assistance of the Commissioner, the position as to what can and cannot safely be disclosed without prejudicing national security will be kept under review. That is a welcome approach. It does not mean that there are any more details which can at present be disclosed without such risk.

133. At the second open hearing on 31 October, the fact of the disclosure of documents in the **Belhadj** case was the subject of discussion and submission, but the Claimants had not had the opportunity of studying them in full. The Tribunal agreed that they could put in short further submissions in writing after doing so, in respect of any matters which arose out of the **Belhadj** documents once they had fully perused them. The primary purpose of doing so was in case there were found to be anything in those documents which appeared to be inconsistent with the content of the Disclosures. We have addressed that in paragraphs 130-131 above. However Liberty in particular put in lengthy further written submissions which were not limited to that point:

(i) Mr Ryder made an argument that the **Belhadj** documents should not have been produced (in part) by way of gisting, but by way of service of the full document redacted, showing the deletions. Quite apart from the fact that the Tribunal could not see how this arose for consideration in the present case, the Tribunal (differently constituted) has given a reasoned judgment on this very point in **Belhadj** on 18 November 2014 ([2014] UKIPTrib 13_132-9H_2), to which reference can be made, and which this Tribunal sees no purpose in reconsidering.

(ii) A request for disclosure, at this very late stage, of further documents from the Respondents is now made, by reference to the fact that the Respondents disclosed (in redacted or gisted form) some extracts of the GCHQ compliance procedures in the **Belhadj** case, relating specifically to legal professional privilege ("LPP"), and it is suggested that similar documents could now be disclosed by the Respondents in this case (although of course, as set out in paragraph 130 above, on a basis far wider than a scope which is limited to LPP). In this case there has been disclosure to the Tribunal by the Respondents pursuant to s.68(6) of RIPA, as referred to in paragraph 46(iv) above, and there has been a closed hearing at which the documents in respect of which the Respondents claim protection on national security grounds have been considered by the Tribunal. The Tribunal in this case is tasked to judge the adequacy of the *arrangements*, both *above and below the waterline*, and to judge *accessibility*, by reference to the extent to which the *scope of the discretion* of the Respondents is revealed or the nature of the *arrangements* is adequately signposted. Particularly at this late stage of the proceedings, after the close of the hearings, further disclosure to the Claimants is unnecessary. If there is inadequate signposting *above the waterline* of the *arrangements below the waterline*, then the Respondents will fail. This is not a case which depends, particularly at this late stage, upon the need for any further disclosure to the Claimants.

134. Mr Ryder also sought to introduce in those written submissions a much wider argument. He submitted that in the light of the late stage in the proceedings (not until the date of the Respondents' skeleton on 3 July 2014) at which the Respondents admitted that the ambit of Article 10 could apply to the investigatory activities of NGOs, it was likely that there was no or no adequate provision for dealing with confidential information obtained by intercept in that context ("*NGO confidence*"). Accordingly in his written submissions dated 17 November 2014 he asked the Tribunal to direct the Respondents to disclose the original documents

(subject to redaction as appropriate) containing their policies and procedures for the handling of such confidential material derived from intercept in relevant circumstances.

135. It is important to set this very belated request into the context of these proceedings:

(i) It is right that the Claimants pleaded from the outset that Article 10 applied to investigatory NGOs as to journalists, and that in the Respondents' pleadings this was denied.

(ii) Amnesty in its claim specifically alleged in relation to LPP, but not in relation to *NGO confidence*, a case (in particular at paragraph 58(g) of its grounds) that there was likely to be no or no adequate (or in any event no *accessible*) legal framework for the protection of LPP in relation to intercepted documents.

(iii) That case was, by an agreed direction of 14 February 2014, hived off to be dealt with in the **Belhadj** case, to which Amnesty was joined as an additional claimant.

(iv) There was no similar case made in respect of *NGO confidence*. The issues in relation to Article 10, as agreed in the 14 February direction were, as discussed in paragraph 12 above, simply mirror images of the same issues under Article 8 and raised (save as set out in paragraphs 149 to 151 below) no further or separate issue.

(v) The arguments raised on Article 10 were led at the hearing by Liberty, according to the skeleton arguments served by the Claimants, and Liberty's skeleton addressed Article 10 succinctly:

(a) In relation to the Prism Issue (iii):

> "*54. For the same reasons the Claimants submitted that the statutory regime does not satisfy the Article 8(2) "in accordance with the law" requirement, it does <u>not</u> satisfy the Article 10(2) "prescribed by law" requirement*".

(b) Similarly (mutatis mutandis) in relation to the s.8(4) issues (vi) and (vii), at paragraphs 102-103 of the skeleton.

(vi) This is exactly how Article 10 was addressed by the Claimants at the hearing, as set out in paragraphs 149-152 below, save for the addition of the argument there addressed, in relation to prior judicial authorisation.

136. Quite apart from the fact that Liberty's new argument (set out in 20 paragraphs at the close of its 17 November 2014 submissions) is not, in the Tribunal's judgment, within the ambit of the additional written submissions anticipated or permitted at the 31 October hearing, those submissions could have been made at any time even prior to the Respondents' skeleton of 3 July 2014, and in tandem with Amnesty's similar submissions in relation to LPP, which were hived off into separate proceedings. It is, in the judgment of the Tribunal, far too late for any such case to be made now, not to speak of one which is said to require further disclosure and would certainly

require considerable further argument, to be incorporated within the ambit of these proceedings and at this stage.

137. It is plain that there are very substantial published procedures in s.15 and the Code, described above. The Respondents are in our judgment justified in their concern that disclosure of further particulars of those procedures would reveal and disclose sensitive and specific details with regard to methods of obtaining and dealing with information, and reveal the precise capacity and capabilities of the Respondents, and we are satisfied that no more needs to be disclosed.

138. We were concerned in the closed hearings to be satisfied in particular as to the existence of *arrangements* relating to the duration of retention and destruction of information the product of intercept or obtained under Prism. The concerns of the Claimants are that a database can be built up of communications data (including communications data not excluded by s.16(2), as discussed above) so as to justify a continuing databank, continuously renewed by reference to the continued necessity for it for one of the s.5(3) purposes, not necessarily being the statutory purpose for which the communications data was originally intercepted.

139. We are satisfied as a result of what we saw and heard at the closed hearings, and the further Disclosure set out above, that this is not the case and that there are adequate *arrangements*, in respect of duration of retention and destruction, to control and regulate the retention of such material. Such retention, storage and destruction policies and procedures are also regularly supervised by the Commissioner, as he makes clear in his Report.

140. We are satisfied, subject to what we say in paragraphs 153 and 154 below, that the s.8(4) regime is sufficiently compliant with the **Weber** requirements and in any event is *in accordance with law,* and that paragraph 164 of the ECtHR judgment in **Kennedy** (cited in paragraph 123 above) endorses this conclusion. As set out in paragraph 55(ii) in relation to the Prism Issue, we are satisfied that the s.8(4) *arrangements* are sufficiently signposted, in the statute, in the Code, in the Commissioner's Reports, and as now recorded in this judgment.

DISCRIMINATION

141. The discrimination claim arises out of Article 14 of the Convention (read with Article 8): a parallel claim by reference to the Charter of Fundamental Rights of the EU did not need to be separately pursued. Article 14 reads as follows:

> "*The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status.*"

The claim is made by reference to differential treatment on the grounds of national origin.

142. The case was originally put by the Claimants in the pleadings and submissions by reference to the alleged difference between s.8(1) as relating to *internal* and s8(4) to

external communications. This however was not pursued orally, and Mr Jaffey, supported by Ms Brimelow, made the case by reference to s.16(2) of RIPA.

143. It is not suggested that there is direct discrimination on nationality grounds. The case is put by reference to indirect discrimination, by reference to location, and thus indirectly to national origin. Communications intercepted under a s.8(4) warrant cannot be read if sent by or to a person located in the UK, by reference to the s.16(2) procedure discussed at some length above. The exclusion, as discussed above, is limited to using (in respect of contents) relevant search words to discover communications, whether *external* or *internal* sent to or received by someone in the UK, and is described, as set out in paragraph 103 above, as a *safeguard*.

144. The complaint is that favour is thus shown to those who are located in the UK, so far as the reading of their communications is concerned. If they are in the UK, they are more likely to be of UK nationality, and there is thus indirect discrimination upon grounds of national origin. Direct discrimination on such grounds requires "*very weighty*" justification (**Gaygusuz v Austria** [1996] 23 EHRR 365). This is however indirect discrimination, and simply requires a rational justification.

145. The background is of course, as discussed above, that a s.8(1) warrant is a targeted warrant, and insofar as directed within the UK it avoids the criticism of being a general warrant (as Mr Jaffey explained by reference to a fascinating exegesis of English law, back to John Wilkes). The need to avoid a 'general warrant' requires the authorities here to target those they can by more specific methods of surveillance within the jurisdiction, short of a s.8 warrant. A s.8(4) warrant is primarily aimed at *external* communications, and not primarily at those located here; although the exemption under s.16(2) can be ousted by means of a certificate under s.16(3).

146. Mr Jaffey's submission is that there is thus a detrimental treatment of those who are not located here, not justifiable on that ground. The Respondents submit that the system is to deal with an unintended method of surveillance of those in the UK, as opposed to normal methods which are not available against those abroad.

147. The Respondents accept that there is an arguable distinction based upon location, and thus, by reference to the Claimants' arguments, on a ground by reference to national origin. They submit however that there is no doubt that there is a rational justification for such distinction, as follows:

i) Protection is needed for those against whom otherwise a s.8(4) warrant could be used to avoid the need for other 'domestic' remedies of surveillance, not available against those abroad. Hence the exceptional nature of a s.16(3) certificate.

ii) Given that the purpose of accessing *external* communications is primarily to obtain information relating to those abroad, the consequence of eliminating the distinction would be the need to obtain a s.16(3) certificate in almost every case rather than by way of an exception, and normally without the information available in respect of those in the UK. The Respondents rely on what they submit to be obvious, namely that it is harder to investigate terrorism and crime abroad, and difficult if not impossible to provide a case for a certificate

under s.16(3) in every case, rather than the exceptional. The numbers of those involved if s.16(3) certificates were extended to those abroad would inevitably be very substantial (we were provided with figures in closed hearing) and this would radically undermine the efficacy of the s.8(4) regime. In any event in relation to a potential target abroad there might not be any or any sufficient information for a s.16(3) certificate.

148. As to the Fourth Question, we are persuaded by the Respondents, for the reasons they put forward, that any indirect discrimination is sufficiently justified. It is quite plain to us that the imposition of a requirement for a s.16(3) certificate in every case would radically undermine the efficacy of the s.8(4) regime, given the pre-eminent role of that regime in the identification of threats to UK national security from abroad.

Article 10

149. We return finally to the balance of the argument in relation to Article 10 (referred to in paragraph 12 above). Article 10 reads as follows:

> "(1) *Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.*
>
> *(2) The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or the rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.*"

It was accepted at the hearing that there is no separate argument in relation to Article 10(2), over and above that arising out of Article 8(2), save that there may be a special argument relating to Article 10 with respect to the need for judicial pre-authorisation of a warrant if such were not necessary, as indeed we have found, in respect of Article 8. Reference was made by Mr Ryder to **Sanoma Uitgevers BV v The Netherlands** [2011] EMLR 4, in which the ECtHR concluded that prior judicial authorisation was required before the state may seize and retain journalistic material. Since it is common ground for the purposes of this case (see paragraph 12 above) that the Claimants may be entitled to the benefit of any protection under Article 10 otherwise available to journalists, it was submitted that the consequences of **Sanoma** should follow.

material. Since it is common ground for the purposes of this case (see paragraph 12 above) that the Claimants may be entitled to the benefit of any protection under Article 10 otherwise available to journalists, it was submitted that the consequences of **Sanoma** should follow.

150. The Respondents do not accept that this applies to any context in which Article 10 is engaged, and in particular point to **Telegraaf Media** at paragraphs 96-97, in which the ECtHR made clear that such a case would be limited to where there was targeted surveillance of journalists with a view to obtaining knowledge of their sources. The Respondents further refer to the words of Laws LJ in **Miranda v the Secretary of State for the Home Department** [2014] 1 WLR 3140, whereby he rejected the suggested absolute rule of prior judicial scrutiny for cases involving State interference with journalistic freedom.

151. We are in any event entirely persuaded that this, which is not of course a case of targeted surveillance of journalists, or indeed of NGOs, is not such an appropriate case, particularly where we have decided in paragraph 116(vi) above, that the present system is adequate in accordance with Convention jurisprudence without prior judicial authorisation. In the context of the untargeted monitoring by s.8(4) warrant, it is clearly impossible to anticipate a judicial pre-authorisation prior to the warrant limited to what might turn out to impact upon Article 10. The only situation in which it might arise would be in the event that in the course of examination of the contents, some question of journalistic confidence might arise. There is, however, express provision in the Code (at paragraph 3.11), to which we have already referred, in relation to treatment of such material.

152. The answer to the Article 10 issues is therefore the same as in respect of the Article 8 issues.

CONSEQUENCES

153. We have therefore reached the necessary conclusions as to the Four Questions set out in paragraph 80 above: No as to the First, Yes as to the Second and Third and No as to the Fourth. However, with regard to the First and Third Questions, our answers are given with the benefit of the Disclosures by the Respondents given in paragraphs 47-48 and 126 above.

154. It is apparent that the Disclosures are in each case such that their effect is to reveal the existence of a safeguard rendering it less, rather than more, likely that there will be objectionable interference with privacy or arbitrary conduct by the Respondents. We do not in any event consider that the disclosure (by reliance upon [illegible] Disclosure) of the additional recording obligation, while welcome, makes any material difference. But it is obvious that the disclosure as to the procedures relating to the obtaining and treatment of intercept pursuant to Prism is of significance. We shall invite submissions from the parties as to the consequence in respect of whether there has been breach of Article 8 prior hereto, only by virtue of the Disclosures.

155. The Tribunal is satisfied that no further disclosure is required to be made as to the detail of the Respondents' practices and procedures in order to render them sufficiently *accessible*. However we in any event consider it of importance that

there should be as much transparency as is consistent with the protection of national security, and welcome the Respondents' statement recorded at paragraph 5 of the Disclosure: we encourage the Respondents to continue to see whether more disclosures can be made even in areas where we have reached no such conclusion.

A SUMMARY

156. In the course of this judgment we have made detailed reference to the various statutory and other safeguards and oversights which govern the receipt of intercepted material in the United Kingdom. Save in one possible (and to date hypothetical) respect, (see paragraph 53 above), we have ruled that the current regime, both in relation to Prism and Upstream and to s.8(4), when conducted in accordance with the requirements which we have considered, is lawful and human rights compliant; but having regard to the submissions we have received, which amount to a comprehensive critique of the interception regime, we think it right in the public interest to describe the essence of what the law provides by way of human rights protection.

157. The legislation in force and the safeguards to which we have referred are intended to recognise the importance of, and the need to maintain, an acceptable balance between (a) the interests of the State to acquire information for the vital purposes of national security and the protection of its citizens from terrorism and other serious crime, and (b) the vital interests of all citizens to know that the law makes effective provision to safeguard their rights to privacy and freedom of expression, together with appropriate and effective limits upon what the State does with that information.

158. Technology in the surveillance field appears to be advancing at break-neck speed. This has given rise to submissions that the UK legislation has failed to keep abreast of the consequences of these advances, and is ill fitted to do so; and that in any event Parliament has failed to provide safeguards adequate to meet these developments. All this inevitably creates considerable tension between the competing interests, and the 'Snowden revelations' in particular have led to the impression voiced in some quarters that the law in some way permits the Intelligence Services *carte blanche* to do what they will. We are satisfied that this is not the case.

159. We can be satisfied that, as addressed and disclosed in this judgment, in this sensitive field of national security, in relation to the areas addressed in this case, the law gives individuals an adequate indication as to the circumstances in which and the conditions upon which the Intelligence Services are entitled to resort to interception, or to make use of intercept.

160. We wish to emphasise that whatever the circumstances of the receipt by the Intelligence Services of intercepted material, the following matters of law are of paramount importance:

    (i) In relation to any material intercepted abroad it would always be unlawful for the Intelligence Services to use the absence of a warrant as a device deliberately to circumvent the requirements of UK law by procuring another State to do what they could not lawfully do themselves.

(ii) The indiscriminate trawling for information by interception, whether mass or bulk or otherwise, would be unlawful, as would be the seeking, obtaining or retention of material which is unnecessary or disproportionate. In this context, even if, pursuant to a s.8(4) warrant enabling the interception of substantial quantities of communications, large quantities are lawfully intercepted, material can only be then accessed lawfully if it is necessary in the interests of national security, for the purpose of preventing or detecting serious crime or for the purpose of safeguarding the economic well being of the United Kingdom ("the statutory purposes"); and it is only proportionate if it is proportionate to what is sought to be achieved by lawful conduct.

(iii) Once it has been accessed by the Intelligence Services, either by specific targeting or selection, intercepted material, including communications data, may only be retained for as long as is necessary for the statutory purposes; thereafter it must be destroyed.

(iv) In respect of all intercepted information which they receive and retain by any of these means the Intelligence Services are accountable. The receipt, handling and destruction of material must be carefully managed, monitored and recorded, and all this information must be freely available for inspection by the relevant authorised oversight bodies, who must be given full and ongoing cooperation in their work.

CONCLUSION

161. This has been a valuable exercise, in which, with the benefit of full and penetrating advocacy on all sides, the Tribunal has been enabled to carry out a review of the systems in relation to both Prism and/or Upstream and the s.8(4) warrant. We have been able (as we state in paragraph 156) to satisfy ourselves that as of today there is no contravention of Articles 8 or 10 by reference to those systems. As set out in paragraphs 153 and 154 above, we have left open for further argument the question as to whether prior hereto there has been such breach. We shall also proceed, guided by the submissions we have heard and the conclusions we have reached, to consider in closed whether there has been in fact any unlawful interception or treatment of the Claimants' communications.

Mr Justice Burton (President)

Mr Robert Seabrook QC

Mrs Justice Carr

The Hon Christopher Gardner QC

His Honour Geoffrey Rivlin QC