Application No. 58170/13

IN THE EUROPEAN COURT OF HUMAN RIGHTS
GRAND CHAMBER

BETWEEN:

BIG BROTHER WATCH and ors

Applicants

-and-
THE UNITED KINGDOM

Respondent

-and-
13 INTERVENING PARTIES

Intervenors

Application No. 24960/15

IN THE EUROPEAN COURT OF HUMAN RIGHTS
GRAND CHAMBER

BETWEEN:

10 HUMAN RIGHTS ORGANISATIONS

Applicants

-and-
THE UNITED KINGDOM

Respondent

-and-
2 INTERVENING PARTIES

Intervenors

Application No. 62322/14

IN THE EUROPEAN COURT OF HUMAN RIGHTS
GRAND CHAMBER

BETWEEN:

(1) BUREAU OF INVESTIGATIVE JOURNALISM
(2) ALICE ROSS

Applicants

-and-
THE UNITED KINGDOM

Respondent

-and-
5 INTERVENING PARTIES

Intervenors

THE UNITED KINGDOM'S OBSERVATIONS ON THE GRAND CHAMBER'S QUESTIONS TO THE PARTIES

These Submissions set out a summary of the Government's case; address certain particularly material facts; and finally, answer the questions set out in the Court's letter of 7 March 2019 in turn. They do not summarise the domestic law and practice, which is fully set out in the First Section's Judgment at §§56-201. They use the terms and acronyms contained in the Glossary to the Submissions (attached at the end of these Submissions for ease of access). Those are the same terms and acronyms used in the Government's earlier observations in these cases. The Government has also inserted (in bold) document references to the Agreed Core Bundle of Annexes used by the First Section, which is before the Grand Chamber. References to the Core Bundle are in the form "CB/x", where "x" is the tab number.

I INTRODUCTION AND SUMMARY

1. These cases are ones of the utmost importance to the UK. They are also of paramount importance to Council of Europe States who benefit from intelligence sharing arrangements with the UK or have similar legislative provisions governing the lawful interception and surveillance of communications. The information and intelligence obtained under the Intelligence Sharing and the s.8(4) Regimes are critical to the protection of the UK from national security threats - including the threats of terrorism, serious and organised crime, and hostile state activity. That is all the more so today, given the sophistication of terrorists and criminals in communicating over the internet in ways that seek to avoid detection, whether that be through the use of encryption, the adoption of bespoke communications systems, or simply the volume of internet traffic in which they can now hide their communications. The internet is now used widely both to recruit terrorists, and to direct terrorist attacks, as well as by cyber criminals. It is also used by hostile states to coordinate activity against the UK. Imposing additional fetters on interception or intelligence sharing of the kind sought by these Applicants would damage Member States' ability to safeguard national security and combat serious crime, at exactly the point when advances in communications technology have increased the threat from terrorists and criminals using the internet.

2. The seriousness of that threat, and its potential to have devastating consequences including the loss of innocent life, are underscored by recent events across the UK and Europe, including the attack on Westminster Bridge on 22 March 2017, the Manchester Arena bombing of 22 May 2017, the attack on London Bridge on 3 June 2017, the attacks in Barcelona on 17 August 2017, and recent terrorist attacks in Copenhagen and Paris. Since March 2017, the UK authorities have thwarted a further 14 Islamist-inspired and 4 extreme right-wing terror plots.

3. Under the Convention scheme, it is properly for States to judge what systems are necessary to protect the general community from such threats. Of course, those systems are subject to the Court's scrutiny, because Convention rights are in play, and the systems must provide appropriate protection against abuse and arbitrariness by the State. However, it is vital that, in assessing the detail of protection required, care is taken not to undermine the effectiveness of systems for obtaining life-saving intelligence that cannot be gathered in any other way. That is why the Court has consistently and rightly afforded States a broad margin of appreciation in this field; and has approached the concept of lawfulness realistically and with that concern clearly in mind.

4. In the UK, the legal regime governing the activities at issue has changed[1] as a result of the recent coming into force of the Investigatory Powers Act 2016. The 2016 Act provides an updated framework for the use of a range of investigatory powers to obtain communications and information about communications, supported by extensive statutory protections against unjustified interference with individuals' rights, including under Articles 8 and 10 ECHR. Nevertheless, the UK already had at the material time a detailed set of controls and safeguards in place governing the activities under challenge.

5. The Intelligence Sharing Regime and the s.8(4) Regime were contained in a combination of primary legislation, published Codes and internal arrangements (which for good operational reasons could not be made public). The bedrock of these Regimes was the Convention concepts of necessity and proportionality. These fundamental principles governed all aspects of information and intelligence from obtaining it in the first place, to examining it, to handling, storing and disclosing it, and finally to its retention and deletion. The safeguards built into the Regimes included a comprehensive and effective system of oversight by Parliamentary Committee (the ISC), a specially appointed Commissioner (a former Lord Justice of Appeal), and a specialist Tribunal, the Investigatory Powers Tribunal, chaired by a senior judge ("IPT"). The ISC, the Commissioner, and the IPT in the Liberty Proceedings[2], have all examined the s.8(4) Regime and Intelligence Sharing Regime in detail. So too has the independent person appointed to keep terrorism laws under review, Lord (David) Anderson QC. His reports (the Anderson Report, **CB/48**, and the Bulk Powers Review, **CB/50**) contain particularly useful material in the context of the present issues, as does the 2013 Annual Report of the Commissioner (**CB/35**).

6. Those oversight bodies have *all* unanimously confirmed – contrary to the position asserted by the Applicants - that the UK does not engage in "*mass surveillance*"; that the s.8(4) Regime does not permit generalised access to communications; that the selection of communications for examination is tightly and carefully controlled; and that the communications selected for examination under the Regime are those of the highest intelligence value (i.e. those of suspected criminals or national security targets). As a result of the Liberty Proceedings, it has also now been publicly confirmed in the factual premises relevant to these applications (and is embodied in the Intelligence Sharing Regime) that the Intelligence Services will only ever seek intercepted communications from other States either where they concern a target who is already the subject of a warrant, or when the Secretary of State has personally considered and approved the request (no such request having been made to date). It has also been publicly confirmed in the factual premises relevant to these applications that the Intelligence Services handle intercepted communications received from foreign states with exactly the same safeguards applied to material intercepted by the Intelligence Services themselves[3]; and will not take receipt of material that they know or believe has been acquired contrary to UK law.

---

[1] The 2016 Act does not provide the statutory authority for the Intelligence Sharing Regime, which continues to be governed by the Security Services Act 1989 and Intelligence Services Act 1994, as set out at §§97-103 of the First Section's Judgment. However, the Intelligence Sharing Regime is now subject to the statutory Interception of Communications Code issued under the 2016 Act, rather than the Code issued under RIPA.

[2] I.e. the 5-day hearing of proceedings in the IPT brought in 2013 by Liberty, Privacy, Amnesty International and various other civil liberties organisations, challenging the Intelligence Sharing and s.8(4) Regimes, in the same factual premises as are relevant to the present application. See the glossary. The main judgment is at **CB/14**.

[3] See in particular the content of the Disclosure from the Liberty Proceedings, now embodied in Chapter 12 of the Code.

7. The First Section, following detailed written observations and an oral hearing, has now issued a conspicuously thorough judgment addressing the lawfulness of both Regimes. It has concluded in summary that:

(1) The IPT has shown itself to be an effective oversight mechanism, which plays an *"important and unique role"* in *"both elucidating the operation of [the Regimes], and remedying any breach of the Convention"*: Judgment, §§267-268.

(2) In relation to the **s.8(4) Regime**, it was not appropriate to impose requirements for objective evidence of reasonable suspicion in relation to persons for whom data was sought, or for judicial pre-authorisation of interception warrants:

i. It would be "*wrong automatically to assume that bulk interception constitutes a greater intrusion into the private life of an individual than targeted interception, which by its very nature is more likely to result in the acquisition and examination of a large volume of his or her communications*": §316. Requiring objective evidence of reasonable suspicion in relation to the persons for whom data is sought, and subsequent notification of the data subject, would be inconsistent with the Court's acknowledgment that the operation of a bulk interception regime in principle falls within a State's margin of appreciation: §317.

ii. Judicial pre-authorisation of interception is not necessary for compliance with Article 8, if the existence of independent oversight provides adequate safeguards against abuse: §§318-320.

(3) The grounds upon which a s.8(4) warrant could be issued were sufficiently clear, and domestic law gave citizens an adequate indication of the circumstances in which their communications might be intercepted: §§330-338. While it would be desirable for the criteria governing the selection of bearers for interception to be subject to greater oversight by the Commissioner, this was not in itself fatal to the operation of the s.8(4) Regime: §338.

(4) The duration of warrants under the s.8(4) Regime, the procedure to be followed for storing, accessing, examining and using the intercepted data, the procedure to be followed for communicating data to other parties, and the circumstances in which it must be erased or destroyed were all sufficiently clear to satisfy the foreseeability test under Article 8: §§359-374. The supervision and oversight of bulk interception was also capable of providing adequate and effective guarantees against abuse: §§375-383.

(5) The s.8(4) Regime satisfied the proportionality test. There was no basis to disagree with the conclusions of independent bodies that it was an essential capability, and that no alternative or combination of alternatives would be a sufficient substitute: §§384-386.

(6) However, the safeguards within the system were not sufficiently robust to provide adequate safeguards against abuse in three particular respects.

i. First, the Court concluded that there was an "*absence of robust independent oversight of the selectors and search criteria used to filter intercepted communications prior to possible examination by analysts*": §347.

ii. Secondly, it was only appropriate to exempt related communications data from the safeguards applicable to the searching and examination of content in s.16 RIPA, to the

extent necessary to determine whether an individual was, for the time being, in the British Islands: §§348-357.

iii. Thirdly, it contained no "above the waterline" requirements circumscribing the Intelligence Services' power to search for and examine confidential journalistic material within material obtained under a bulk interception warrant (and as such breached Article 10): §§490-495.

(7) The **Intelligence Sharing Regime** was sufficiently foreseeable, and provided sufficient guarantees against abuse, for the purposes of Article 8 ECHR, applying the 6 "minimum criteria" in *Weber* by analogy: §§420-444. Further, it satisfied the test of necessity: §§445-446.

(8) The complaints of breach of Articles 6 and 14 were manifestly ill-founded: §§501-519.

8. The UK in large part accepts the findings of the First Section. It strongly agrees with the First Section's conclusion that a bulk interception regime is in principle compatible with the ECHR, and with its reasoning to the effect that any meaningful interference with privacy rights under such a regime occurs only when communications are selected for possible examination, or examined. Moreover, in general, it does not seek to gainsay the First Section's findings that in certain limited respects the s.8(4) Regime did not comply with Articles 8 and 10. Indeed, those matters are remedied in the new regime under the Investigatory Powers Act 2016.

9. In summary, the UK submits the proper answers to the Court's questions are as follows:

(1) ***Question 1***: It is accepted that the interception of communications in bulk constitutes a theoretical interference with the Applicants' rights under Article 8(1), because their communications may have been passed over bearers subject to interception. That having been said, any *meaningful* interference with a person's Article 8(1) rights occurs only if their intercepted communications are selected for examination and/or subsequently examined by an analyst. Of the various Applicants, only Amnesty International and the Legal Resources Centre have shown such an interference: see the IPT's judgment of 22 June 2015 at **CB/16**, as corrected by the letter at **CB/18**.

(2) The Government cannot provide specific examples of individual queries or selectors used, without unacceptable damage to national security. However, the Government has set out below in the "Facts" section examples of the types of the selectors that may be used, and further detail of the automated processes used to select material for examination, and of the number and duration of interception permissions issued annually.

(3) The phrase "*selection for examination*" is capable of misleading. As used by the Intelligence Services, it refers to the *automated* process of conducting simple or complex searches of intercepted material, in order to create a list of communications from which an analyst may potentially choose items to inspect (in effect, stage 1). This therefore involves no actual examination or consideration of the communication by an analyst. Stage 2 then involves the choice from the list and subsequent examination of the communication by the analyst. Thus, only communications or communications data that have been examined by an analyst are or can be used to provide intelligence; and only items that have been selected for examination can actually be examined.

(4) ***Question 2***. In answer to questions (a)-(d):

(a) It is appropriate to apply the standards developed in the Court's case law on secret measures of surveillance to bulk interception, for the reasons the First Section gave.

(b) The existence of "below the waterline safeguards", and the independent oversight of those safeguards by the Commissioner, is relevant to the question whether the s.8(4) Regime contains adequate safeguards against abuse, and thus, relevant to the foreseeability test.

(c) The Court's established case law requires effective supervision and review of the impugned activities by an independent body, but rightly does not prescribe the precise form that such supervision should take. In this respect, the combined oversight functions of the ISC, Commissioner and IPT satisfy the requirements of the Convention. The UK accepts (in line with the First Section's judgment) that there should be robust independent oversight of selectors and search criteria. However, this has always been within the Commissioner's powers (the First Section do not appear to have appreciated this). Notwithstanding that, the UK is currently working with the Office of the Investigatory Powers Commissioner to ensure enhanced oversight of selectors and search criteria under the Investigatory Powers Act 2016.

(d) Examining the content of the most sensitive and private communications will always involve a greater degree of intrusion than examining communications data, irrespective whether items of communications data are aggregated to provide a detailed picture of where an individual is located, what websites he visits, or whom he chooses to contact. On that basis, it remains appropriate for the rules governing content to be more exacting than those governing communications data. The UK nevertheless accepts following the Judgment of the First Section that the Secretary of State should be required to certify the necessity of examining communications data obtained under a bulk interception warrant, pursuant to a regime analogous though not identical to the certification regime in place for the content of communications under s.16 RIPA. The UK is intending to amend the new code governing interception of communications under the Investigatory Powers Act 2016 to this effect.

(5) ***Question 3***: There has been no interference with the Applicants' rights under Article 8(1) on account of the operation of the Intelligence Sharing Regime. None of them has shown that their communications or communications data have been intercepted pursuant to Prism and/or Upstream and shared with the UK, or were ever likely to be so.

(6) ***Question 4*****:** To the extent that there has been any interference with the Applicants' rights under Article 8(1), the Intelligence Sharing Regime is in accordance with the law and necessary for the purposes of Article 8. The law is accessible, and gives the individual adequate protection against arbitrary interference. No separate issue arises concerning necessity.

(7) ***Question 5****:*

(a) The UK accepts that there has been an interference with the Applicants' Article 10 rights under the s.8(4) Regime, on the same basis and for the same reasons that there has been an interference with their Article 8 rights. Their Article 10 complaint gives rise to no arguable separate issue from their Article 8 complaint, save in respect of the safeguards applied to confidential journalistic material and communications capable of identifying journalists' sources. The UK accepts that there should be special provision made for the treatment of such material intercepted under a bulk warrant, and has made such provision in the new code under the Investigatory Powers Act 2016.

(b) No separate Article 10 issue arises *at all* in relation to the Intelligence Sharing Regime, for the reasons given by the First Section, viz: (i) the 10 HR Applicants did not exhaust domestic remedies in relation to any complaint about the special protection afforded to

journalists under Article 10 – see §473 of the First Section's judgment; and (ii) the BIJ Applicants have not complained about the Intelligence Sharing Regime: see §476 of the First Section's judgment.

(c) If (contrary to the above) any Article 10 issue arose in relation to the Intelligence Sharing Regime, then by reason of Chapter 12 of the Code, the answer would be exactly the same as for the s.8(4) Regime.

II THE FACTS

The Prism/Upstream Complaints

10. Both the 10 HR and BBW applications concern the Intelligence Services' alleged receipt of material obtained under Prism and Upstream[4]. Prism and Upstream are US surveillance programmes conducted under the authority of s.702 Foreign Intelligence Surveillance Act 1978 ("FISA"). Prism and Upstream are targeted programmes, undertaken with the knowledge of the service provider and under Court-approved procedures, in accordance with extensive privacy protections for non-US nationals. The First Section has repeated a common misunderstanding by asserting that Upstream is a bulk programme, that has "*broad access to global data*": see Judgment, §18. That is wrong[5]. The US Privacy and Civil Liberties Oversight Board ("PCLOB"), an independent, bipartisan agency within the US Government's Executive Branch, has investigated the position in detail and concluded as follows:

"*The [Section 702 program] consists entirely of targeting specific persons about whom an individualised determination has been made. Once the government concludes that a specific non-U.S person located outside the United States is likely to communicate certain types of foreign intelligence information – and that this person uses a particular communications "selector", such as an email address or telephone number – the government acquires only those communications involving that particular selector.*
Every individual decision to target a particular person and acquire the communications associated with that person must be documented and approved by senior analysts within the NSA before targeting…".

11. In the Liberty proceedings, the Government explained the highly restricted circumstances in which relevant Intelligence Services sought intercepted communications (and associated communications data) from a foreign government, amounting to a set of internal rules. The rules were embodied in the IPT's judgment of 5 December 2014 ("the 5 December Judgment", **CB/14**) and following that judgment were incorporated into the Code at Chapter 12, set out in full at §109 of the First Section's judgment. (Identical rules are now embodied in Chapter 9 of the current code of practice governing interception under the Investigatory Powers Act 2016).

[4] GCHQ has obtained information from the US that the US obtained via Prism. The Government neither confirms nor denies that either the Security Service or SIS has obtained information from the US collected via Prism, or that any of the Intelligence Services have obtained information collected under Upstream.

[5] The mischaracterisation of Prism and Upstream as involving "bulk seizure, acquisition and storage" appears to result from a failure to distinguish between two different types of NSA programme: the collection of bulk telephone call records under section 215 of the USA Patriot Act - a programme which PCLOB recommended should cease in 2014, and which has ceased – and collection under FISA. That misunderstanding is widely shared, and has been repeated by various courts or other bodies in Council of Europe States. Nevertheless, it remains a clear misunderstanding.

12. In sum, the effect of Chapter 12 of the Code is to confirm that, in the factual premises relevant to the Liberty proceedings (and therefore to these Applications), the only "raw intercept" requested by the Intelligence Services from any foreign government (including the USA) is either (i) intercepted material concerning targets who are already the subject of an interception warrant under Part I of RIPA, where that material cannot be obtained by the Intelligence Services themselves, and it is necessary and proportionate to obtain it; or (ii) in exceptional circumstances, and where necessary and appropriate, other material not covered by a RIPA interception warrant, provided that the request has been considered and decided upon by the Secretary of State for Foreign and Commonwealth Affairs. So far, no request falling within (ii) has ever been made. The Code also confirmed that exactly the same internal safeguards governing use, disclosure, storage and destruction apply as a matter of substance to such material, as apply to similar material obtained through interception under Part I of RIPA.

13. Further, the Disclosure and Code, as set out above, and the findings of the ISC and Commissioner[6] also confirm that receipt of intelligence material from the US via Prism and Upstream (or indeed, receipt of any intelligence material whatsoever) is not (contrary the Applicants' allegations) used as a means of circumventing domestic constraints on interception, imposed via RIPA. That would be unlawful as a matter of basic domestic public law[7]. In short, the Applicants' factual assertions that the UK Intelligence Services may obtain data from the NSA in breach of domestic controls, or in circumstances where they could not lawfully obtain that data themselves, are simply wrong.

The complaints about the alleged 'Tempora' operation

14. All 3 Applications (BBW, 10 HR and BIJ) complain about the bulk interception of communications pursuant to the alleged 'Tempora' interception operation. The Government intercepts communications in "bulk" – including at the level of communications cables – pursuant to the lawful authority of warrants under s.8(4) RIPA. Such interception is aimed at "*external communications*" (that is, communications sent or received outside the British Islands[8]). The essential characteristics of this form of bulk interception are set out by the First Section at §§11-13. Its features are addressed in more detail by the Commissioner in his Annual Reports of 2013 (**CB/35**) at §§6.5.27-6.6.18 and 2014 (**CB/36**) at §§6.23-6.40; in the ISC Report §§49-77 (**CB/47**); in the Anderson Report at chapter 10 (**CB/48**); and in the Bulk Powers Review in Chapters 2, 5 and 9 and Annex 8 (**CB/50**). All have been able to investigate the interception capabilities of the Intelligence Services in detail, with the full cooperation of the Intelligence

[6] See the ISC's Statement of 17 July 2013 on its investigation into the allegation that GCHQ used Prism as a means of evading UK law (**CB/43**). See also the Commissioner's 2013 Annual Report at §§6.8.1-6.8.6 (**CB/35**) and the question and answer posed at the beginning of that section:
"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?
6.8.1 No. I have investigated the facts relevant to the allegations that have been published…"

[7] Specifically, it would be contrary to the principle of domestic public law set out by the House of Lords in *Padfield v Ministry of Agriculture, Fisheries and Food* [1968] AC 997 for the Intelligence Services deliberately to circumvent safeguards and mechanisms in RIPA by asking a foreign intelligence agency to intercept communications instead. (The position would be different if, for example, it was not technically feasible for the UK to intercept those communications itself, or if such interception could not be carried out within the required timeframe.)

[8] See s.20 RIPA and §6.5 of the Code, as set out in the First Section's Judgment at §69 and page 33.

Services. Each has engaged with, or taken evidence from, many interested parties outside government, including some of the Applicants, for the purposes of drafting their Reports. The Government can confirm the factual accuracy of the Reports' accounts of the Intelligence Services' capabilities.

The rationale for, and utility of, s.8(4) interception

15. There are two fundamental reasons why it is necessary to intercept the contents of bearers for wanted external communications, both of which ultimately derive from the substantial practical difference between the Government's control over and powers to investigate individuals and organisations within the UK, and those that operate outside that jurisdiction[9] (see e.g. the Anderson Report at §10.22, **CB/48**):

    (1) Bulk interception is critical both for the discovery of threats, and for the discovery of targets who may be responsible for threats. When acquiring intelligence on activities overseas, the Intelligence Services do not have the same ability to identify targets or threats that they possess within the UK. For example, small items of intelligence (such as a suspect location) may be used to find links leading to a target overseas; but that can only be done, if the Services have access to a substantial volume of communications through which to search for links.
    (2) Even where the Intelligence Services know the identity of targets, their ability to understand what communications bearers those targets will use is limited, and their ability to access those bearers is not guaranteed. Subjects of interest are very likely to use a variety of different means of communication, and to change those means frequently. Moreover, electronic communications do not traverse the internet by routes that can necessarily be predicted. Communications will not take the geographically shortest route between sender and recipient, but the route that is most efficient, as determined by factors such as the cost of transmission, and the volume of traffic passing over particular parts of the internet at particular times of day. (That does not detract in the slightest from the fact that particular bearers may carry a high proportion of communications of a particular type[10]). So in order to obtain even a small proportion of the communications of known targets overseas, it is necessary for the Services to intercept a selection of bearers, and to scan the contents of all those bearers for the wanted communications.

16. In addition, there are technical reasons why it is necessary to intercept the entire contents of a bearer, in order to extract specific communications. The precise position is complex, and the technical details are sensitive, but the basic position is that communications sent over the internet are broken down into small pieces, known as "packets", which are then transmitted separately, often through different routes, to the recipient, where the message is reassembled. It follows that in order to intercept a given communication that is travelling over the internet (say, an email), any intercepting agency will need to obtain as many of the packets associated with that

[9] See Mr Farr's w/s at §§143-147 for a summary of those differences, **CB/9**.

[10] This is why 10 HR is wrong to assert that the Government's assertion that it chooses bearers on the basis of the possible intelligence value of the traffic they carry is inconsistent with this description of how internet communications travel (see 10 HR Obs in Reply, §41). The route down which a particular email to or from Syria might travel is almost infinitely varied. However, specific bearers may nevertheless carry a high proportion of such emails. It is those upon which GCHQ would wish to focus, in order both to (i) intercept the communications of a particular target; or (ii) discover targets (for example) planning terrorist attacks from Syria.

communication as it can, and reassemble them[11]. Thus, if an intercepting agency needs (for example) to obtain communications sent to an individual (C) in Syria, whilst they are being transmitted over the internet, and has access to a given bearer down which such communications may travel, the intercepting agency will need to intercept all communications that are being transmitted over that bearer – at least for a short time – in order to discover whether any are intended for C. Further, since the packets associated with a given communication may take different routes to reach their common destination, it may be necessary to intercept all communications over more than one bearer to maximise the chance of identifying and obtaining the communications being sent to C. (So again, those bearers would be chosen that had the greatest chance of carrying the packets concerned.) In summary, as Mr Farr stated at §149 (**CB/9**):

"Taking these considerations in the round, it will be apparent that the only practical way in which the Government can ensure that it is able to obtain at least a fraction of the type of communication in which it is interested is to provide for the interception of a large volume of communications, and the subsequent selection of a small fraction of those communications for examination by the application of relevant selectors."

17. The Commissioner, the ISC Report, the Anderson Report and the Bulk Powers Review have all examined in detail the need for bulk interception of communications under s.8(4) RIPA (or equivalent powers) in the interests of the UK's national security. All have concluded there is no doubt that such a capability is valuable, because it meets intelligence needs which cannot be satisfied by any other reasonable means.

18. The Commissioner's Annual Report of 2013 (**CB/35**) asked at §6.4.49 whether there were other reasonable but less intrusive means of obtaining needed external communications, and concluded at §6.5.51:

"I am satisfied that at present there are no other reasonable means that would enable the interception agencies to have access to external communications which the Secretary of State judges it is necessary for them to obtain for a statutory purpose under the section 8(4) procedure. This is a sensitive matter of considerable technical complexity which I have investigated in detail."

Further, the Commissioner, having pointed out that there was a policy question whether the Intelligence Services should continue to be enabled to intercept external communications under s.8(4) RIPA, stated that he thought it "*obvious*" that, subject to sufficient safeguards, they should be: §6.5.56.

19. The ISC Report stated (**CB/47**):

"It is essential that the Agencies can "discover" unknown threats. This is not just about identifying individuals who are responsible for threats, it is about finding those threats in the first place. Targeted techniques only work on "known" threats: bulk techniques (which themselves involve a degree of filtering and targeting) are essential if the Agencies are to discover those threats." (§77(K))

On that basis, the ISC concluded that GCHQ's bulk interception capacity under s.8(4) RIPA was: *"a valuable capacity that should remain available to them",* and was used for *"complex*

[11] This position was very well understood at the time that RIPA was enacted: see the debate in the House of Lords for 12 July 2000, and the remarks of Lord Bassam (the responsible Government Minister), **CB/38**.

problems relating directly to some of the UK's highest priority intelligence requirements": see §§81, 90.

20. The Anderson Report (**CB/48**) commented on the uses of bulk interception at §§7.22-7.27, noting the importance of bulk interception for target discovery; and observing that this did not mean suspicion played no part in the selection of communications channels for interception, or in the design of searches conducted on intercepted material. Lord Anderson QC concluded that bulk access was (inter alia) the only means by which GCHQ could obtain the information it needed to develop effective responses to cyber threats[12]; that case studies left him in *"not the slightest doubt"* of the value of its role for protecting national security[13]; that there no cause for him to recommend that collection in its current form should cease; and that its utility, particularly in fighting terrorism in the years since the London bombings of 2005, was clear to him[14].

21. The Anderson Report contains (at Annex 9) six "case study" examples of intelligence from the bulk interception of communications. The importance of those examples speaks for itself, not least in light of recent events in Paris and Brussels. In summary, they are:

    (1) The triggering of a manhunt for a known terrorist linked to previous attacks on UK citizens, at a time when other intelligence sources had gone cold, and the highlighting of links between the terrorist and extremists in the UK, ultimately enabling the successful disruption of a terrorist network ("Case Study 1").
    (2) The identification in 2010 of an airline worker with links to Al Qaida, who had offered to use his airport access to launch a terrorist attack from the UK, in circumstances where his identification would have been highly unlikely without access to bulk data ("Case Study 2").
    (3) The identification in 2010 of an Al Qaida plot to send out operatives to act as sleeper cells in Europe, and prepare waves of attacks. The operatives were identified by querying bulk data for specific patterns ("Case Study 3").
    (4) The discovery in 2011 of a network of extremists in the UK who had travelled to Pakistan for extremist training, and the discovery that they had made contact with Al Qaida ("Case Study 4").
    (5) Analysis of bulk data to track two men overseas who had used the world wide web to blackmail hundreds of children across the world. GCHQ was able to confirm their names and locations, leading to their arrest and jailing in their home country ("Case Study 5").
    (6) The discovery in 2014 of links between known ISIL extremists in Syria and a previously unidentified individual, preventing a bomb plot in mainland Europe which was materially ready to proceed. Bulk data was the trigger for the investigation ("Case Study 6").

[12] See §7.25 of the Anderson Report

[13] See §7.26 of the Anderson Report

[14] See §14.45 of the Anderson Report. At §14.44, Lord Anderson QC referred to *"contrasting reports"* from the Council of Europe on bulk data collection. He compared the findings and resolution of the Committee on Legal Affairs and Human Rights, which cast doubt on the efficacy of bulk interception, with a report of April 2015 from the European Commission for Democracy through Law. He observed that the notion that bulk interception is ineffective "*is contradicted by the detailed examples I have been shown at GCHQ"*'. He pointed out that aspects of the methodology upon which the Committee's findings were made "*seem debatable*", and failed to take into account "*the potential of safeguards, regulation and oversight*". He commented that the April 2015 report was drafted "*in considerably more moderate (and on the basis of what I have seen realistic) terms*".

22. Quite aside from the direct threats to life set out above, bulk interception is also the only way in which the Intelligence Services can realistically discover cyber threats: a danger which potentially affects almost every person in the UK using a computer. The scale of the issue is one to which Lord Anderson QC referred, when he pointed out that over a 2-week period bulk access had enabled GCHQ to discover 96 separate cyber-attack campaigns. The internet is an intrinsically insecure environment, with billions of computers constantly running millions of complex programmes.

23. Finally, the utility of bulk interception carried out by GCHQ under the s.8(4) Regime was considered in still further detail in the Bulk Powers Review at Chapter 5, on the basis of an intensive review of *"a great deal of closed material concerning the value of bulk interception"* (see §5.2). Lord Anderson QC set out detailed reasons in Chapter 5 why intelligence obtained under the s.8(4) Regime will or may not be obtainable in any other way, and stated in conclusion:

> *"5.53 This Review has given me the opportunity to revisit my earlier conclusion [in the Anderson Report] with the help of Review team members skilled respectively in technology, in complex investigations and in the interrogation of intelligence personnel, and on the basis of considerably more evidence: notably, a variety of well-evidenced case studies, internal documentation and the statistic that almost half of GCHQ's intelligence reporting is based on data obtained under bulk interception warrants.*
>
> *5.54 My opinion can be summarised as follows:*
>
> *(a) the bulk interception power has proven itself to be of vital utility across the range of GCHQ's operational areas, including counter-terrorism in the UK and abroad, cyber-defence, child sexual exploitation, organised crime and the support of military operations.*
>
> *(b) The power has been of value in target discovery but also in target development, the triaging of leads and as a basis for disruptive action. It has played an important part, for example, in the prevention of bomb attacks, the rescue of a hostage and the thwarting of numerous cyber-attacks.*
>
> *(c) While the principal value of the power lies in the collection of secondary data, the collection and analysis of content have also been of very great utility, particularly in assessing the intentions and plans of targets, sometimes in crucial situations.*
>
> *(d) The various suggested alternatives, alone or in combination, may be useful in individual cases but fall short of matching the results that can be achieved using the bulk interception capability. They may also be slower, more expensive, more intrusive or riskier to life."*

24. The Bulk Powers Review emphasised in particular the importance of bulk interception for target discovery, i.e. finding previously unknown threats. See in particular:

    (1) §5.3 of the Bulk Powers Review:

    > "*Bulk interception is essential because the security and intelligence agencies frequently have only small fragments of intelligence or early, unformed, leads about people overseas who pose a threat to the UK. Equally, terrorists, criminals and hostile foreign intelligence services are increasingly sophisticated at evading detection by traditional means. Just as importantly, due to the nature of the global internet, the route a particular communication will travel is hugely unpredictable. Combined, this means that sometimes the data acquired via bulk interception is the only way the security and intelligence agencies can gain insight into particular areas and threats…"* (Emphasis added)

    (2) Annex 7 to the Bulk Powers Review, which sets out GCHQ's "*Statement of Utility of Bulk Capabilities*", supplied to the Review in July 2016, stating inter alia:

"GCHQ would not be able to identify those who wish us harm without bulk powers. Terrorists, child abusers, drug traffickers, weapons smugglers and other serious criminals choose to hide in the darkest places on the internet. GCHQ uses its bulk powers to access the internet at scale so as then to dissect it with surgical precision.

By drawing out fragments of intelligence from each of the bulk powers and fitting them together like a jigsaw, GCHQ is able to find new threats to the UK and our way of life; to track those who seek to do us harm, and to help disrupt them.

- ***Bulk Interception:*** *Interception provides valuable information that allows us to discover new threats. It also provides unique intelligence about the plans and intentions of current targets – through interception of the content of their communications. Communications data obtained through bulk interception is also crucial to GCHQ's ability to protect the UK against cyber-attack from our most savvy adversaries and to track them down in the vast morass of the internet."*

25. Annex 8 to the Bulk Powers Review contains 13 "case studies", illustrating the use of and need for bulk interception, and providing context and a factual underpinning for the conclusions in chapter 5. Four of those case studies were summarised (albeit in slightly less detail) in the Anderson Report. Those are the identification in 2011 of a network of extremists in UK, on the basis of an email address obtained through complex queries of bulk data; the identification and monitoring of a senior Al Qaida leader and his network through interrogation of bulk data, leading to the arrest and conviction of a UK-based terrorist planning to use airport access to launch an attack; the arrest and jailing of men using the world wide web to blackmail children; and the discovery in 2014 of links between known ISIL extremists in Syria and a previously unidentified individual, preventing a bomb plot in mainland Europe. The other nine are summarised below. As with the examples in the Anderson Report, their importance speaks for itself:

(1) In 2015, GCHQ used communications data obtained under bulk interception warrants to search for new phones used by individuals known to be plotting terrorist acts in the UK. Following the identification of a new phone number, GCHQ eventually identified an operational cell, and its analysis revealed that the cell had almost completed the final stages of a terrorist attack. The police were able to disrupt the plot in the final hours before the planned attack. Without access to bulk data, GCHQ would not have been able to complete this work at all. See Case Study A8/1.

(2) Following terrorist attacks in France, GCHQ provided support to MI5 and European partners in identifying targets and prioritising leads. GCHQ triaged around 1,600 international leads (in the form of telephone numbers, email addresses or other identifiers) in the days following the attacks. It was necessary quickly to determine whether there was any further attack planning, and to identify leads that should be prioritised for further investigation. Without bulk data, that triage work would have taken much longer – potentially many months – and would have led to GCHQ obtaining an incomplete picture, providing only limited assurance that further attack planning had been identified or ruled out: Case Study A8/3.

(3) During the UK's Afghanistan campaign, analysis of data obtained through bulk interception enabled GCHQ to locate and monitor an armed group that had taken hostages captive. Within 72 hours of the kidnapping, the hostages were located. They were subsequently rescued. There was no likely alternative method to bulk interception through which the hostage-takers could have been identified and located, or their intentions revealed: Case Study A8/6.

(4) During the UK's Afghanistan campaign, GCHQ used analysis of data obtained under bulk interception warrants to identify mobile devices in the area of Camp Bastion, the main base for UK forces. Analysis flowing from that data revealed that extensive attacks on Camp Bastion were being planned by multiple insurgents. The information led to several such

attacks being disrupted. There was no practical means to obtain the information on a targeted basis. See Case Study A8/7.

(5) GCHQ used bulk interception to identify sophisticated malware placed on a nationally important UK computer network by an overseas-based criminal gang. Further analysis of the bulk data identified the infrastructure used to control the malware. The information obtained by GCHQ eventually led to the arrest of the gang. This is by no means an isolated incident: GCHQ deals with over 200 cyber incidents a month. See Case Study A8/8.

(6) In 2016, a European media company suffered a major, destructive cyber-attack. The analysis of bulk data permitted GCHQ (i) to link this attack to other attacks, and to explain what had happened; and (ii) to identify a possible imminent threat to the UK from the same cyber-attackers. As a result, GCHQ was able to protect government networks, and warn media organisations so that they were able to protect their own networks. GCHQ would have been unable to achieve the same outcome without the use of bulk powers: Case Study A8/9.

(7) Bulk data has given GCHQ significant insight into the nature and scale of online child sexual exploitation activity. In April 2016 alone, GCHQ identified several hundred thousand separate IP addresses worldwide being used to access indecent images of children through the use of bulk data. Further analysis can then lead (for example) to targeting those whose online behaviour suggests they pose the greatest risk of committing physical or sexual assaults against children: see Case Study A8/10.

(8) Between November 2014 and November 2015, GCHQ's analysis of data obtained under bulk interception warrants led to significant disruption of cocaine trafficking, involving the seizure of cocaine with a street value of around £1.1 billion. The traffickers could not have been identified, tracked, and disrupted without the use of bulk interception: Case Study A8/12.

(9) In early 2015, GCHQ's analysis of data obtained under bulk interception warrants was able to identify the multiple communications methods used by the principal members of an organised crime group involved in human trafficking into the UK. The information enabled investigations which eventually resulted in the release of a group of trafficked women, and the individual concerned was subsequently arrested: Case Study A8/13.

26. Much of the aim of interception pursuant to the s.8(4) Regime is not to search for the communications of identified targets. Rather, it is to ascertain, via the application of complex searches, who should be a target in the first place ("target discovery"). It is to identify who are the individuals, groups and organisations outside the UK that pose a threat to the UK, because without such a power the Intelligence Services would be unable to tell who they were. Well over half of the examples referred to in the previous paragraph concern the discovery of previously unknown targets through the use of a bulk interception capability, instead of (or in addition to) the tracking of known targets. See §§28(2), (3), (4), (5), (7), (8), (9) above. See also §5.3 and Annex 7 extracts from the Bulk Powers Review quoted above, and the ISC's Report (**CB/47**) at vii on page 3 ("*Key Findings*"), under the heading "*Why do the Agencies intercept communications?"*

"(b) As a "discovery" or "intelligence-gathering", tool. The Agencies can use targeted interception only after they have discovered that a threat exists. They require separate capabilities to uncover those threats in the first place, so that they can generate leads and obtain the information they need to then target those individuals…"

27. The Executive Summary of the Bulk Powers Review by Lord Anderson QC drew the threads together concerning the utility of bulk powers in the following way:

"*• The Report concludes that there is a proven operational case for three of the bulk powers, and that there is a distinct (though not yet proven) operational case for bulk equipment interference (9.12-9.15).*
• As the case studies show, the bulk powers are used across the range of Agency activity, from cyber-defence, counter-espionage and counterterrorism to child sexual abuse and organised crime (Annexes 8-11).
• The bulk powers play an important part in identifying, understanding and averting threats in Great Britain, Northern Ireland and further afield. Where alternative methods exist, they are often less effective, more dangerous, more resource-intensive, more intrusive, or slower (chapters 5-8)."

28. More generally, the Privacy 2 judgment from the IPT (**CB/21**) considered in some detail both the need for bulk data capabilities, the actual manner of their operation (rather than often ill-informed and inaccurate assertions or assumptions) and the nature of the attendant safeguards (the impact of an imposition of the sort of safeguards considered in eg the CJEU's judgment in *Watson*[15] is considered below). At this stage, the following matters appearing from that judgment are to be noted.

    (1) The IPT recorded that there were two facts which were uncontroversial, and in any event established by the evidence. They were first that "*the use of Bulk Data capabilities is critical to the ability of the SIAs to secure national security*" (or as they put it later at §17: "*The finding of this Tribunal is that these capabilities are essential to the protection of the national security of the United Kingdom*"); and secondly, that "*a fundamental feature of many of the SIAs' techniques of interrogating Bulk Data is that they are non-targeted, i.e. not directed at specific targets*" (§9(i) and (ii)) – that being because, as the ISC put it "*It is essential that the Agencies can "discover" unknown threats. This is not just about identifying individuals who are responsible for threats, it is about finding those threats in the first place. Targeted techniques only work on "known" threats: Bulk techniques (which themselves involve a degree of filtering and targeting) are essential if the Agencies are to discover those threats.*"
    (2) The IPT noted the particular importance of the Anderson report as being "*that it was conducted by a team of independent persons…, with considerable expertise in the use of secret intelligence, and with the necessary security clearance to obtain access to secret documents, in order to analyse a number of actual case studies, to judge the effect and utility of the bulk powers. The reviewers were not only able to review documents, but also to question intelligence officers to ascertain whether the case being made for the use of those powers was justified*" (§11).
    (3) The IPT specifically agreed with the overall conclusion reached by Lord Anderson QC at §6.47, commenting: "*Those findings fully support the evidence given in this case by the Respondents that the use of bulk communications data is of critical value to the intelligence agencies, and is of particular value in identifying potential threats by persons who are not the target of any investigation. These datasets need to be as comprehensive as possible if they are to be effective. The use of these datasets is very different from, for example, their use in an investigation of a criminal offence by police, in which case the police may well have an identified suspect who can be made the subject of a targeted investigation. The Respondents' witnesses speak persuasively of developing fragmentary intelligence, of enriching 'seed' information, of following patterns and anomalies, and of the need for the haystack in order to find the needle"*(§14).
    (4) The IPT took the view that there was "*considerable force"* in the submissions made to them that "*a. The use of bulk acquisition and automated processing produces less intrusion*

[15] Joined Cases *Tele2 Sverige C-203/15* and *Watson & ors C-698/15*, 21 December 2016

than other means of obtaining information. b. The balance between privacy and the protection of public safety is not and should not be equal. Privacy is important and abuse must be avoided by proper safeguards, but protection of the public is preeminent. c. The existence of intrusion as a result of electronic searching must not be overstated, and indeed must be understood to be minimal. d. There is no evidence of inhibition upon, or discouragement of, the lawful use of telephonic communication. Indeed the reverse is the case. e. Requirements or safeguards are necessary but must not, as the Respondents put it, eviscerate or cripple public protection, particularly at a time of high threat" (§50).

How bulk interception under the s.8(4) Regime works

29. It is of fundamental importance to understand how bulk interception under the s.8(4) Regime operates. In particular, it is critical to appreciate that (i) although, for technical reasons, it is necessary to intercept the entire contents of a fibre optic cable (or "bearer") in order to obtain any intercepted communications or communications data from it at all, there is no possibility whatsoever of any communications being viewed by an analyst, unless and until they have been selected for examination – "selection for examination" being an automated process of creating an index by computerised searches; (ii) selection (and any ensuing examination) are very carefully controlled; and (iii) the overwhelming bulk of communications flowing over that bearer can never be so selected, but will (and must) be discarded. Further, no intelligence report can be made of any communications or communications data unless they have been viewed by an analyst.

30. Interception under the s.8(4) Regime has taken place under the authority of fewer than 20 s.8(4) warrants at any one time. The warrants may not last for more than 6 months (and generally last for the full period of 6 months). They may be renewed where necessary and proportionate: see the Code at p.24 of the First Section's Judgment.

Communications

31. Bulk interception of communications under the s.8(4) Regime involves four stages, including examination itself[16]:

    (1) Collection.
    At this stage, GCHQ selects bearers to access on the basis of the likely intelligence value of the communications they carry. GCHQ only processes a fraction of the bearers it has the ability to access. It will select that fraction on the basis of those bearers most likely to be carrying external communications of intelligence value. GCHQ will do this by regular surveys of the contents of bearers to seek to ensure that the most useful bearer is targeted. In practical terms, "accessing" means making a copy of the communications and associated communications data flowing down the bearer.
    (2) Filtering
    GCHQ's processing systems automatically discard in near-real time a significant proportion of the communications and communications data on the targeted bearers, on the basis that it comprises the traffic of a type least likely to be of intelligence value.
    (3) So called 'selection for examination'
    The remaining communications are then subjected to the computerised application of queries inputted by analysts[17], both simple and complex, to draw out communications of intelligence

[16] See in particular Chapter 2 of the Bulk Powers Review at §§2.15-2.20, **CB/50**.

value which may potentially be viewed by an analyst. Queries may be either "simple" (in that they require the application of a single "strong selector", such as a telephone number or email address), or "complex" (in that they combine a number of criteria, which may include weaker selectors, but which in combination aim to reduce the odds of a false positive). Communications which match the relevant selectors are retained for possible examination; all other communications are discarded. This stage does not entail the production of any intelligence; it merely sifts the material which an analyst may be authorised to view.

(4) Examination

An analyst may then examine a particular communication from the list of items created at the "selection for examination" stage, where it is necessary and proportionate to do so. No intelligence report is made of any communication which has not been examined by an analyst.

32. At the "selection for examination" stage, the "strong selector" (i.e. "simple query") process is applied against all the bearers that GCHQ has chosen to access. As observed by the ISC: *"while this process has been described as bulk interception because of the numbers of communications it covers, it is nevertheless targeted since the selectors used relate to individual targets"*. In short, this aims to extract the communications of specified targets, albeit that it is necessary to intercept the entire contents of a bearer for a very short time, to enable this to be done. See the ISC Report, §§61-63.

33. The "complex query" process is applied against a far smaller number of bearers. Those bearers are not chosen at random: GCHQ focuses its resources on those most likely to carry items of intelligence value. The process entails 2 stages: (i) the initial application of a set of processing rules, designed to discard material least likely to be of value; and (ii) the application of complex queries to the material so selected, in order to draw out items which relate to GCHQ's statutory functions and descriptions of material in the Secretary of State's certificate, and the selection of which meets tests of necessity and proportionality. A complex query might involve, for example, searching for material which combined use of a particular language, emanation from a particular geographical region, and use of a specific technology. Other selectors used in complex queries might for example involve the use of a complex digital signature created by a particular machine used in cyber attacks, or the use of a call sign from a particular vessel. Those searches generate an index. Only items contained in the index can potentially be examined by analysts. All other communications must be discarded. See the ISC Report, §§67-73 (**CB/47**), and the Bulk Powers Review at §2.19 (**CB/50**).

34. The selection of communications for examination, whether via "strong selectors" or "complex queries", and any ensuing examination, is very carefully controlled. Automated systems are used (and by §7.14 of the Code[18], must be used) to effect the selection for examination, save where a limited number of specifically authorised staff access intercepted material for the specific purpose of checking whether it falls within the Secretary of State's certificate, or to check whether the selection methodology remains up-to-date and effective.

35. The choice of selectors to effect selection of communications for examination is also itself carefully controlled. Whenever a new selector is added to the system, the analyst adding it needs

[17] "Selection for examination" entails an automated process of computerised searching, but the search terms themselves are selected and input by analysts, rather than (for example) being generated automatically; and are selected only where it is necessary and proportionate to do so. See further paragraphs 34 and 35 below.

[18] See the First Section's judgment, page 33.

to complete a written record, explaining why it is necessary and proportionate to apply the selector for purposes within the Secretary of State's certificate. In the case of a "strong selector", the analyst would need to explain (for example) the justification for seeking the communications of a particular target; how the selector related to the target's methods of communicating; and why selection of the relevant communications would not involve an unacceptable degree of collateral intrusion into privacy. Selectors applied directly to bearers are subject to a rigorous process of automated rules, augmented by human intervention where necessary, to ensure that they meet the appropriate legal and policy requirements. In the case of a new "complex query", (to be used as described in §33 above) the analyst would need to develop selection criteria most likely to identify communications bearing intelligence of value; and would similarly need to explain why the criteria were justified, and why their use would be necessary and proportionate for purposes within the Secretary of State's certificate. Any selector must be as specific as possible, in order to select the minimum material necessary for the intelligence purpose, and to be proportionate. If, through analysis, it is established that selectors are not being used by their intended target, prompt action must be taken to remove them from relevant systems. The use of selectors must be recorded in an approved location that enables them to be audited; creates a searchable record of selectors in use; and enables oversight by the Commissioner.

36. Selectors used for target development or target discovery may remain in use for a maximum of three months before a review is necessary.

37. Any analysts who then examine selected material will be specially authorised to do so, and receive mandatory regular training, including training on the requirements of necessity and proportionality (see Code, §7.15). They will be vetted. Before they examine the material, they must create a record setting out why access to the material is required, consistent with the Secretary of State's certificate and the requirements of RIPA; and why it is proportionate (including considerations of any circumstances likely to give rise to a degree of collateral infringement of privacy). Unless such a record has been created, GCHQ's systems do not permit access to material.

38. Only a fraction of those communications selected for possible examination by either of the processing systems set out above is ever in fact looked at by an analyst.

    (1) In relation to communications obtained via the use of "simple selectors", an automated "triage" process is applied, to determine which will be of most use. This triage process means that the vast majority of the items collected in this way are never looked at by an analyst, even where they are known to relate to specific targets.
    (2) In relation to communications obtained via the application of complex search terms, items are presented to analysts as a series of indexes in tabular form showing the result of searches. To access the full content of any item, the analyst has to decide to open the specific item of interest based on the information in the index, using their judgment and experience. In simple terms, this can be considered as an exercise similar to that conducted when deciding what search results to examine, from a list compiled by a search engine such as Bing or Google. The remainder of the potentially relevant items are never opened or read by analysts.

39. Communications to which the "strong selector" process is applied are discarded immediately, unless they match the strong selector. Communications to which the "complex query" process is applied are retained for a few days, in order to allow the process to be carried out, and are then automatically deleted, unless they have been selected for examination.

40. Communications which have been selected for examination may be retained only where it is necessary and proportionate to do so. The default position is that, the retention period for selected communications is no longer than a few months, after which they are automatically deleted (though of course if the material has been cited in intelligence reporting, the report will be retained). In exceptional circumstances a case may be made to retain selected communications for longer, as provided for in the Code.

Communications data

41. The Court has asked about the factual position regarding communications data. It is important to appreciate that a similar (though not identical) process applies to RCD, intercepted under the s.8(4) Regime, as applies to communications[19].

42. As with communications, communications data is subject to filtering, so that in near real time a very substantial proportion of communications data is instantly discarded.

43. As with communications, communications data will then be subjected by automated means to simple or complex queries, in order to draw out communications data of potential intelligence value. However, this is a more "iterative" process than with regards to communications, and communications data which is not selected by this method is not immediately discarded. The principal reason is that communications data is to a large extent used to discover threats or targets of which the Intelligence Services may previously have been unaware[20]. It requires more analytical work, over a lengthy period, to discover "unknown unknowns". That discovery may very often involve an exercise of piecing together disparate small items of communications data to form a "jigsaw" revealing a threat; and will include the possible examination of items that initially appeared of no intelligence interest. Discarding unselected communications data immediately, or after a few days only, would render that exercise impossible.

44. Nevertheless, before any analyst can examine any communications data <u>at all</u>, they must complete a record explaining why it is necessary and proportionate to do so, in pursuit of the Intelligence Services' statutory functions. So, just as with the content of communications, an auditable record is produced, setting out the justification for examination. These records are available for inspection. And just as with content, no intelligence reporting can be made on the basis of communications data unless and until it has been examined.

45. Communications data intercepted under the s.8(4) Regime may be retained only where it is necessary and proportionate to do so, for a maximum period of several months, unless an exceptional case to retain for longer is made. They are automatically deleted once that period has expired.

General observations on the facts concerning interception under the s.8(4) Regime

46. The factual position set out above is consistent with the conclusion of the Commissioner in his Annual Report for 2013 (**CB/35**) at §6.7.5:

[19] The Court has not asked for comments on the regime for the acquisition of communications data under Part I Chapter II of RIPA; it is important not to conflate the two distinct questions of the regime governing RCD intercepted pursuant to a s.8(4) warrant, and the regime governing communications data acquired under Part I Chapter II.
[20] See in this respect the IPT's Privacy 2 Judgment, cited above.

"I am…personally quite clear that any member of the public who does not associate with potential terrorists or serious criminals or individuals who are involved in actions which could raise national security issues for the UK can be assured that none of the interception agencies which I inspect has the slightest interest in examining their emails, their phone or postal communications or their use of the internet, and they do not do so to any extent which could reasonably be regarded as significant."

47. The factual position also indicates that it is simply wrong for the Applicants to suggest that a selector might be used to *"store and analyse the reading habits of the population",* or *"identify everyone who had read a particular book"*. The selection stage would not permit the use of such a selector; nor could an analyst provide the required justification for examining material on this basis. It might be the case that a complex query selected communications for examination on the basis of accessing known extremist literature, where that was combined (say) with being in a particular location such as northern Iraq; or using a particular software application associated with terrorism. But using such a complex search to identify a target is not only doing exactly what GCHQ's systems are designed for, but is of vital utility to the UK's national security.

48. Interception under a s. 8(4) warrant is directed at "*external communications*" of a description to which the warrant relates: that is, at communications sent or received outside the British Islands (see s.20 RIPA). But the fact that electronic communications may take any route to reach their destination inevitably means that a proportion of communications flowing over a bearer between the UK and another State will consist of "*internal communications*": i.e., communications between persons located in the British Islands.

49. When conducting interception under a s.8(4) warrant, knowledge of the way in which communications are routed over the internet is combined with regular surveys of internet traffic to identify those bearers that are most likely to contain external communications that will meet the descriptions of material certified by the Secretary of State as necessary to intercept. While this approach may lead to the interception of some communications that are not external, s.8(4) operations are conducted in a way that keeps this to the minimum necessary to achieve the objective of intercepting wanted external communications: see Farr §154, **CB/9**. Mr Farr gave various examples of communications which he regarded as "*internal*", and those which he regarded as "*external*" at Farr §§134-138. For example, he indicated that a "Google" search was in effect a communication between the person conducting the search, and Google's index of web pages, hosted on its servers; and that because those servers were in general based in the US, such a search might well be an external communication. The Applicants have criticised those examples as "*expansive*" and/or "*arbitrary*". That criticism is misplaced; but more importantly, the Applicants have neglected to mention Mr Farr's observation that the question whether a particular communication is internal or external is entirely distinct from (and irrelevant to) the question whether it can lawfully be selected for examination: see Farr §§139-141, 157-158.

Other factual matters

50. The First Section's judgment includes much detailed factual material on issues important to this case, and on which the UK relies but does not repeat here, including most particularly:

    (1) The powers and effectiveness of the oversight mechanisms of the ISC, Commissioner and IPT. See, in particular, Judgment at §§123-143 (IPT); §§148-159 (ISC); and §§144-147 (Commissioner).
    (2) The nature of the detailed reviews of the Intelligence Sharing Regime and the s.8(4) Regime carried out by the ISC, Royal United Services Institute and former Independent

Reviewer of Terrorism Legislation, and the full access that they had to closed material in order to conduct those reviews. See Judgment at §§149-176.

(3) The findings of the Commissioner's 2016 Annual Report, and the nature of the inspection process conducted by the Commissioner: see Judgment at §§178-194.

(4) The thorough review of both the Intelligence Sharing Regime and the s.8(4) Regime carried out by the IPT in the course of determining the complaint made by the Applicants in 10HR (i.e. the Liberty Proceedings): see Judgment at §§21-55.

51. Two material corrections to the First Section's factual findings should be noted.

52. The **first** correction arises from the First Section's reliance on the ISC Report. The First Section stated at Judgment §§340 and 347 (in reliance on the extract of the ISC Report quoted at §157 of the Judgment), that there was not "*meaningful"* or *"robust"* independent oversight of selectors and search criteria. The First Section also appeared at §338 (again, in reliance on the ISC Report) to conclude that there was not robust oversight of the selection of bearers for interception. Those findings are wrong both in terms of power and in fact.

53. The Commissioner has always had full power to inspect and report on whatever features of the s.8(4) Regime he considers necessary. That follows, from his wide powers under sections 57 and 58 RIPA[21].

54. The Edward Snowden allegations, which prompted the ISC's Review, also prompted the Commissioner to investigate the operation of the s.8(4) Regime in detail, which he did in his 2013 Annual Report (**CB/35**), published on 4 May 2014. As may be seen from p.58 of the 2013 Annual Report, one of the matters that the Commissioner wished to investigate further was precisely the operation of selectors/search terms:

"(3) I need to undertake further detailed investigation into the actual application of individual selection criteria from stored selected material initially derived from section 8(4) interception. I have had this fully explained and even demonstrated to me. But I am currently short of sufficient detailed material necessary to make a full structural analysis and assessment of the internal process. Time has not permitted me to undertake this inquiry before writing this report."

55. That inquiry was subsequently built into the Commissioner's processes. The Commissioner stated in his 2014 Annual Report (**CB/36**), published in May 2015, that he had conducted the full structural analysis to which the 2013 Annual Report referred, and said at §6.37:

"In 2014 my office carried out the further investigations into the actual application of individual selection criteria…and, in particular reviewed the breadth and depth of the internal procedures for the selection of material to ensure that they were sufficiently strong in all respects. These investigations, which focused on GCHQ as the interception agency that makes the most use of section 8(4) warrants and selection criteria, addressed in good detail the selection criteria and related matters."

56. As to the selection of bearers for interception, an important express part of the Commissioner's function consists in determining (i) whether s.8(4) warrant applications meet the requirements of necessity and proportionality; and (ii) whether the collection of material pursuant to those warrant applications is itself necessary and proportionate, having regard to the amount, type and

[21] Under s.57, the Commissioner has a duty inter alia to keep under review the adequacy of the arrangements under s.15 RIPA i.e. the Intelligence Services' safeguards upon interception powers. Under s.58, every person holding office under the Crown has a duty to disclose or provide to the Commissioner all documents and information that he may require for the purpose of enabling him to carry out his functions under s.57.

relevance of communications intercepted. Those functions inevitably and necessarily require the Commissioner to oversee the selection of bearers for interception. See e.g. the description of the Commissioner's functions in this respect at §6.80 of the 2015 Report, **CB/37**. The Commissioner has been regularly briefed by the relevant Intelligence Services about the basis upon which bearers are selected for interception.

57. As is evident from the 2014 Annual Report, the Commissioner altered and strengthened his oversight function in relation to the operation of the s.8(4) Regime in response to the Snowden allegations, and in particular strengthened his scrutiny of the operational conduct carried out on intercepted material. See §§6.54-6.59 of the 2014 Annual Report. The 2014 Annual Report indicates that this involved detailed "end to end" analysis of the treatment of intercepted material, from the point of interception to the point of destruction: see e.g. §6.56. See too the 2015 Report at §6.79 (**CB/37**):

"*GCHQ is unique in terms of the type and scale of the interception it undertakes and therefore it is necessary to take a different inspection approach with the GCHQ inspections to ensure the process is audited from end to end".* (Emphasis added)

58. It is therefore to be noted that the ISC's conclusions, upon which the First Section relied, were in this respect in error. They evidently did not take account of the steps taken by the Commissioner set out in the 2014 Annual Report, and since reflected in the exercise of his inspection powers.

59. Finally, in order to ensure that there is no public misunderstanding of the position, the new oversight body (the Investigatory Powers Commissioner, "IPCO", who has replaced the Commissioner pursuant to the Investigatory Powers Act 2016[22]) has been specifically tasked with oversight of selectors/search terms[23].

60. The **second**, more minor, correction is to §57 of the First Section's Judgment. The First Section there stated that s.5(3) RIPA (since repealed) permitted the Secretary of State to authorise a warrant if it was necessary "*for safeguarding the economic well-being of the United Kingdom*". In fact, with effect from 17 July 2014, the Data Retention and Investigatory Powers Act 2014 ("DRIPA") amended s.5(3) RIPA so that a warrant could be obtained for the purpose of safeguarding the economic well-being of the UK only "*in circumstances appearing to the Secretary of State to be relevant to the interests of national security".* See further fn 56 below.

III THE QUESTIONS POSED BY THE COURT

Question 1: Has there been an interference with the Applicant's rights under Article 8(1) ECHR on account of the operation of the s.8(4) Regime, and if so at what stage?

61. The UK has addressed above the Court's discrete factual queries under this head in respect of the use of retained material; the nature of "selection for examination"; and the basis on which content and communications data which have been selected for examination/examined are discarded.

[22] See the First Section's Judgment at §147, explaining the expanded role and greater resources of IPCO.

[23] This being, for instance, a step provided for in the Swedish regime considered in *Centrum för Rättvisa v Sweden* (App. No. 35252/08): see the Judgment at §157.

62. As to the more general question posed by the Court, the UK accepts that the mere interception of the Applicants' communications would constitute an interference with their Article 8(1) rights; and that the nature of the s.8(4) Regime is such that all users of communications services are potentially at risk of having their communications intercepted. The UK also accepts that this is sufficient to entitle the Applicants to claim infringement of their Article 8(1) rights, on the basis set out by this Court in *Zakharov v Russia* (App. No. 47143/06) at §171.

63. Nevertheless, there are plainly degrees of interference involved. Any *meaningful* interference with Article 8(1) rights can occur only if an Applicant's communications are (at the very least) selected for examination, if not actually examined by an analyst. Their rights cannot be said to be infringed to any more than the most minimal degree, if a copy of their communications is either discarded in near-real time under the "strong selector" process, or held for a few days at most in a general "soup" of data under the "complex query" process, in both cases without any possibility of it being examined or used at all.

64. Of the various Applicants, only Amnesty International and the Legal Resources Centre have shown such a meaningful interference: see the IPT's judgment of 22 June 2015 at **CB/16**, as corrected by the letter at **CB/18**. The other Applicants have neither shown that their communications were likely to be selected for examination or examined, nor that they were in fact selected for examination/examined.

Question 2: in the event that there has been an interference under the s.8(4) Regime, was it in accordance with the law and necessary within the meaning of Article 8(2)?

65. The Court has posed 4 specific questions under the general rubric of Question 2. The structure of the UK's submissions deals both with the Court's questions, and with the general issue whether the s.8(4) Regime is in accordance with the law and necessary, under the following eight heads:

    (1) What test should apply to the foreseeability and necessity of the interception of communications: in particular, whether the well-established standards developed in the Court's case law on the interception of communications, and set out in *Weber and Saravia v Germany* (App. No. 54934/00), should be replaced in this context by some *stricter* set of rules. The answer is "no". This deals with Question 2(a) in the context of the content of communications (but not related communications data, "RCD")).
    (2) Question 2(b) i.e. the extent to which safeguards need to be made public, or can exist "below the waterline". The answer is that while safeguards should be made public to the extent possible, it is inevitable that some safeguards will exist "below the waterline", and the knowledge that such safeguards exist and are effectively overseen is an important safeguard against abuse.
    (3) Question 2(c) i.e. whether Article 8(2) requires activities to be supervised and reviewed by an independent body, and if so, how and at what stage. The answer is "yes", but it is not possible to be prescriptive about how and when this should occur, which will depend upon the nature of the regime; and the UK's oversight system manifestly meets the requirements of the Convention.
    (4) Whether the s.8(4) Regime is in accordance with the law as regards the content of communications. The answer is "yes".

(5) The answer to various specific complaints made by the Applicants about the s.8(4) Regime, concerning the supposed read-across of EU law; the width of the terms "national security" and "external communications"; and the need for subsequent notification.
(6) Whether different standards should be applied to RCD, and if so, what those standards are i.e. the answer to Questions 2(a) and 2(d) in the context of RCD. The answer is that different and somewhat less rigorous standards should be applied.
(7) Whether the s.8(4) Regime is in accordance with the law as regards RCD. The answer is "yes" with one caveat concerning certification, as explained below.
(8) Whether the s.8(4) Regime satisfies the "necessity" test, both as regards content and as regards RCD. The answer is "yes".

(1) What legal test should apply to the interception of communications?

66. The Applicants argue that the legal principles in *Weber* should no longer apply, on the purported basis that the "*world has changed*". They say the UK is now able to conduct further reaching and more intrusive surveillance, so that the privacy impact of bulk interception is particularly great. They also say the effect of the Court's case law in *Zakharov* and *Szabo v Hungary* (App. No. 37138/14) is that no interception should be carried out at all without "*reasonable suspicion*". In other words, all individuals should be individually identified and targeted before any interception takes place. They are wrong, as a matter both of fact and law.

What is the factual position concerning the intrusiveness of bulk interception?

67. If the world has changed since RIPA was enacted, that is only because the increased volume of internet traffic, and increased sophistication of those using it to threaten the UK's national security, has made the Intelligence Services' job harder. The world has *not* changed in any way which intrudes more upon the privacy rights of persons whose communications are subject to interception. The s.8(4) Regime has always operated exactly as it was expected to do, at the time it was designed, to enable the UK to secure intelligence that could not otherwise be obtained at all.

68. The s.8(4) Regime does not reflect some policy choice on the UK's part to undertake a programme of "*mass surveillance*", in circumstances where a warrant targeting a specific person or premises (as under s.8(1) RIPA) would be perfectly well suited to acquiring the external communications at issue. As the Commissioner has confirmed, and as follows from the facts at §§15-28 above, there are no other reasonable means that would enable the Intelligence Services to have access to external communications that it is adjudged necessary to secure. That is because (in simplified summary) (i) communications are sent over the internet in small pieces (i.e. "packets"), which may be transmitted separately, often by separate routes; (ii) in order to intercept a given communication of a target, while in transit over the internet, it is necessary to obtain all the "packets" associated with it, and reassemble them; and (iii) in order to reassemble the "packets", it is necessary to intercept the entirety of the contents of a bearer or bearers in order to discover whether any are intended for the target in question. In other words, the only practical way to find and reconstruct most external communication "needles" is to look through a communications "haystack".

69. The s. 8(4) regime was - to Parliament's knowledge – designed to accommodate the internet, and

Parliament was made aware of the issue as noted above[24]. Unsurprisingly, given the above, the Commissioner concluded in his 2013 Annual Report that RIPA had not become "*unfit for purposes in the developing internet age*": see the Report at §6.5.55[25]. The fact that there the internet has grown in scale does not render the safeguards under RIPA less relevant or adequate.

70. In addition, there are important practical differences between the ability of the Intelligence Services to investigate individuals and organisations within the British Islands as compared with those abroad: see Farr §§142-147 (**CB/9**). Those practical differences offer further justification for a regime of the form of the s. 8(4) Regime (Farr §149).

71. Moreover, the operation of the s.8(4) Regime is not more intrusive to privacy because it needs to sift a greater volume of communications, in a world where the volume of communications has massively increased, but less.

72. The First Section was right to observe at §316 of its judgment that: *"it would be wrong automatically to assume that bulk interception constitutes a greater intrusion into the private life of an individual than targeted interception, which by its very nature is more likely to result in the acquisition and examination of a large volume of his or her communications"*. On the contrary, individuals now communicate by a variety of different electronic methods; there is a hugely increased volume of internet communications, and encryption is ever more widely used. All those factors mean that bulk interception is likely to result in a smaller proportion of an individual's communications being obtained, let alone examined, than was previously the case; and a much smaller proportion, than could be obtained by appropriately targeted methods, if such methods were practicable.

Does the law now require reasonable suspicion?

73. The answer is "no". The imposition of such a requirement would in practice denude the interception of communications under the s.8(4) Regime of a very large portion of its utility, thereby endangering the lives of UK citizens. There is no reason in the Court's jurisprudence to do so – and specifically such a requirement is not to be found on a proper analysis of *Zakharov* or *Szabo.* There is every reason in principle not to impose it.

74. The true principle is that any interception of and access to communications must be necessary and proportionate, and must satisfy the *Weber* criteria, which the s.8(4) Regime does. The First Section was right so to conclude in the present case, and the Third Section was equally right so to conclude in *Centrum för Rättvisa v Sweden* (App. No. 35252/08). That conclusion follows from the Court's well-established case law to the effect that bulk interception is not in principle incompatible with the Convention: see *Weber* and *Liberty v UK* (App. No. 58243/00).

75. In particular, the Applicants rely on *Zakharov* to contend that "*reasonable suspicion*" against an individual is a necessary precondition for any surveillance, because the Court found that *"the authorisation authority's scope of review… must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting the person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures…"*: *Zakharov*, §260.

[24] See the remarks of the Minister (Lord Bassam of Brighton) in Parliament at **CB/38**

[25] See **CB/35**.

76. That finding at §260 of *Zakharov,* however, must be seen in its context. It concerned the sufficiency of the authorisation authority's scope of review, where the issue was the propriety of the intelligence agency's request to perform a search operation targeting the communications of a specific individual (see e.g. §§38 and 44 of the judgment). The Court accepted that the requirement for prior judicial authorisation in Russian law was an important safeguard, but found that it was insufficient in the circumstances, because the domestic court's scrutiny was limited. The domestic court had no power to assess whether there was a sufficient factual basis for targeting the individual concerned: see §§260-261. Moreover, there was no effective *post facto* judicial scrutiny either: §298. Thus, the totality of the safeguards did not provide adequate and effective guarantees against abuse: §302.

77. In short, the context in *Zakharov* concerned the nature of the available safeguards, where a particular individual had already been targeted; and unsurprisingly, the Court considered that it was important for those safeguards to include effective independent judicial oversight of that targeting decision, capable of assessing its merits. Nothing in *Zakharov* either states or implies that, in order for there to be sufficient safeguards against abuse, any target of surveillance must always be identified in advance on the basis of reasonable suspicion. Rather, the true position on the basis of the Court's jurisprudence is that:

    (1) It is the totality of safeguards against abuse within the system that is to be considered. See e.g. *Zakharov* at §§257, 270-271.
    (2) Where a decision has been made to target a particular individual, it will be necessary for a judicial authority to be able to review that decision on its merits (i.e. to determine not simply whether it was taken in accordance with proper procedures, but to assess whether it was necessary and proportionate). See *Zakharov*.
    (3) However, such judicial oversight can be either *ex ante* or *post facto*: see e.g. *Szabo* at §77, *Kennedy v UK* (App. No. 26839/05) at §167.
    (4) The s.8(4) Regime provides such oversight. The IPT is able to, and will, examine the necessity and proportionality of any interception or examination of the complainant's communications, with the benefit of full access to the evidence. See the First Section's summary of the IPT's procedure and effectiveness at §§21-55 and §§123-143. Further, the Commissioner (a senior judge) also provides effective oversight: see the First Section's judgment at §§144-145.

78. As to the Applicants' reliance on *Szabo*, the Fourth Section's observations at §71 of the judgment were in the context of its proportionality assessment and whether the type of "secret surveillance" which had been undertaken by the TEK had been demonstrated as necessary and proportionate. Again, these observations have to be seen in the context of a regime which allowed ordering of interception entirely by the Executive, with no assessment of necessity, with potential interception of individuals outside the operational range, and in the absence of any effective remedial or judicial measures.

The legal principles that apply

79. Accordingly, the UK submits that the applicable principles remain those alluded to in the First Section's Judgment at §§303-320.

80. The expression "in accordance with the law" requires "... *firstly, that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question,*

requiring that it should be accessible to the person concerned, who must, moreover, be able to foresee its consequences for him, and compatible with the rule of law ..." (see e.g. *Weber* at §84).

81. Domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to secret surveillance measures: see e.g. *Zakharov* at §229. The essential test, as recognised at §68 of *Malone v. UK* (App. No. 8691/79) is and remains whether domestic law indicates the scope of any discretion and the manner of its exercise with sufficient clarity "*to give the individual adequate protection against arbitrary interference*". The Grand Chamber has confirmed in *Zakharov* at §230 that this test remains the guiding principle when determining the foreseeability of intelligence-gathering powers. See also the First Section's Judgment at §306.

82. However, this essential test must always be read subject to the important and well-established principle that the foreseeability requirement cannot mean that an individual should be enabled to foresee when the authorities are likely to resort to secret measures so that he can adapt his conduct accordingly: *Malone* at [67]; *Leander v. Sweden* (App. No. 9248/81) at §51; *Weber*, at §93; *Zakharov* at §229; the First Section's Judgment at §306.

83. The Court has developed the following set of six "*minimum safeguards*" that need to be set out in the domestic legal framework that governs the interception of communications, in order to ensure that the "*foreseeability*" requirement is met in this specific context:

    "[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 ..." (*Weber*, at §95, *Zakharov* at §231, the First Section's Judgment at §307, "the *Weber* criteria").

84. As the Court recognised at §95 of *Weber*, the reason why such safeguards need to be in a form accessible to the public is in order to avoid "*abuses of power*". The *Weber* criteria are thus a facet of the more general principle that there must be adequate and effective guarantees against abuse. Accordingly, in determining whether the domestic safeguards meet the *Weber* criteria, account should be taken of all the relevant circumstances, including: "*the authorities competent to authorise, carry out and supervise [the measures in question], and the kind of remedy provided by the national law ...*" (*Zakharov*, §232, the First Section's Judgment at §308).

85. It is not necessary that every provision / rule of domestic law be set out in primary legislation. The Court in *Kennedy* held that the provisions of the Code could properly be taken into account in assessing foreseeability insofar as it supplemented and further explained the relevant legislative provisions: see §§156]-157. The First Section has rightly endorsed that conclusion: §325.

Question 2(b): the extent to which safeguards need to be made public, or may exist below the waterline

86. The legal framework for any interception regime must be publicly accessible. Nevertheless, as the First Section rightly recognised at §326 of its Judgment, States do not have to make public all the details of the operation of a secret surveillance regime, and it is inevitable for national security reasons that not all details can be made public. So "below the waterline" arrangements,

setting out safeguards and limitations by reference to the non-public aspects of a secret surveillance regime, not only can properly be in place, but should be in place.

87. The fact that such arrangements exist, sufficiently signalled in public documents, and overseen by the Commissioner, is an important practical aspect of the legal framework – both in ensuring practically effective implementation of the law and as relevant to the sufficiency of oversight under the Act. The IPT was right so to hold in *Liberty IPT* at §§120-121 (**CB/14**). That is consistent with the Convention principle that regard must be had to the actual operation of a surveillance system, including the checks and balances on the exercise of power and the existence or absence of any evidence of actual abuse: see *Ekimdzhiev v Bulgaria* app. 62540/00, 30 January 2008, at §92, and the First Section's Judgment at §320.

88. One facet of that test is whether effective internal safeguards – i.e. "below the waterline" arrangements – exist, and whether they are subject to independent oversight. The Commissioner's 2013 and 2014 Annual Reports confirm that the answer on both counts is "yes". See for example the Commissioner's 2014 Annual Report at §6.40, **CB/36**:

"*The related matters that my office investigated included the detail of a number of other security and administrative safeguards in place within GCHQ (which are not just relevant to interception work). These included the security policy framework (including staff vetting), the continuing instruction and training of all relevantly engaged staff in the legal and other requirements of the proper operation of RIPA 2000 with particular emphasis on Human Rights Act requirements, and the development and operation of computerised systems for checking and searching for potentially non-compliant use of GCHQ's systems and premises. I was impressed with the quality, clarity and extent of the training and instruction material and the fact that all staff are required to undertake and pass a periodic online test to demonstrate their continuing understanding of the legal and other requirements."*

(3) Question 2(c): whether Article 8(2) requires activities to be supervised by an independent body, and if so how and at what stage

89. The Court has consistently applied a sensible and non-doctrinaire approach to the issue whether independent oversight of surveillance is required, and if so at what stage. It should continue to do so. The starting point is that independent oversight (as far as relevant to the foreseeability test) is an aspect of whether the system contains sufficient safeguards against abuse. That is an intensely fact-specific question, which requires analysis of the system as a whole, rather than the application of fixed rules. So while the Court has consistently and rightly required some form of independent oversight of the system to be present as a necessary safeguard against abuse, it has declined to state that this must necessarily entail independent prior authorisation either of warrants, or of any other aspect of an interception system. That should remain the position.

90. **First,** the Court's case law is clear that independent pre-authorisation of warrants is not a precondition of lawfulness, provided that the applicable regime otherwise contains sufficient safeguards. Given the possibilities for abuse inherent in a regime of secret surveillance, it is on the whole in principle desirable to entrust supervisory control to a judge: but such control may consist of oversight after rather than before the event. Extensive *post factum* judicial oversight can counterbalance absence of pre-authorisation. See *Klass v Germany* at §51, *Kennedy* at §167, and most recently, the detailed consideration of the issue in *Szabo and Vissy* at §77[26].

[26] To the extent that *Iordachi v Moldova* app.25198/02, 10 February 2009 implies at §40 that there must in all cases be independent prior authorisation of warrants for interception, it is inconsistent with the later cases of *Kennedy* and *Szabo*,

91. **Secondly,** the Court has never suggested that independent pre-authorisation of individual decisions to task the system with particular selectors, or to examine material, would be required as a precondition of lawfulness. There is good reason for that. Such a requirement would be likely to render the entire operation of a bulk interception system impossible. The necessary basis for the operation of such a system will be the application of many thousands of selectors, in order to acquire wanted external communications or RCD. It would be wholly impracticable to require independent pre-authorisation of each such selector or decision.

92. **Thirdly,** just as in *Kennedy*, the extensive oversight mechanisms in the s.8(4) Regime here offer sufficient safeguards to render the regime in accordance with the law, without any requirement for independent (still less, judicial) pre-authorisation of warrants, let alone selectors, or individual decisions to examine material. In particular, the extensive independent (including judicial) *post factum* oversight of secret surveillance under the s.8(4) Regime compensates for the fact that s.8(4) warrants are authorised by the Secretary of State, rather than by a judge or other independent body.

93. The very same observations made by the ECtHR at §167 of *Kennedy*, in which the Court found that the oversight of the IPT compensated for the lack of prior authorisation, apply equally here:

> *"…the Court highlights the extensive jurisdiction of the IPT to examine any complaint of unlawful interception. Unlike in many other domestic systems, any person who suspects that his communications have been or are being intercepted may apply to the IPT. The jurisdiction of the IPT does not, therefore, depend on notification to the interception subject that there has been an interception of his communications. The Court emphasises that the IPT is an independent and impartial body, which has adopted its own rules of procedure. The members of the tribunal must hold or have held high judicial office or be experienced lawyers. In undertaking its examination of complaints by individuals, the IPT has access to closed material and has the power to require the Commissioner to provide it with any assistance it thinks fit and the power to order disclosure by those involved in the authorisation and execution of the warrant of all documents it considers relevant. In the event that the IPT finds in the applicant's favour, it can, inter alia, quash any interception order, require destruction of intercept material and order compensation to be paid. The publication of the IPT's legal rulings further enhances the level of scrutiny afforded to secret surveillance activities in the United Kingdom."*

94. Further, the IPT has offered further proof of its effectiveness and extensive powers since *Kennedy*, such that it is a remedy available in theory and practice, capable of offering redress to applicants complaining of both specific incidences of surveillance and the general Convention compliance of surveillance regimes*:* see the First Section's observations about the IPT at §§250-265 and §§510-513 of its Judgment.

95. Moreover, the following additional points about the applicable *post factum* independent oversight should also be made:

    (1) The Commissioner oversees the issue of warrants under the s.8(4) Regime as part of his functions, and looks at the majority of all individual warrant applications (including both targeted warrants, and s.8(4) warrants) in detail. See e.g. his 2015 Annual Report, **CB/37,** §§6.49-6.50.
    (2) The Commissioner also looks at a proportion of individual targeting decisions under the

---

and cannot stand with the general thrust of the ECtHR's case law.

s.8(4) Regime, and interviews analysts, in order to be assured that the system is working as intended: see e.g. §§56-59 in the "Facts" section above, and the 2015 Annual Report at §§6.52-6.56.

(3) More generally, the Commissioner carries out "end to end" oversight of the operation of the s.8(4) Regime, from the point of interception of material to the point of its destruction: see e.g. the 2015 Annual Report at §6.80.

(4) The ISC also provides an important means of overseeing the s.8(4) Regime as a whole, and specifically investigated the issuing of warrants in the ISC Report (see the report, pp.37-38, **CB/47**).

(4) The s.8(4) Regime is in accordance with the law: the content of communications

96. The Art. 8 interferences have a basis in domestic law, namely the s. 8(4) Regime. Further, the "accessibility" requirement is satisfied in that RIPA is primary legislation[27] and the Code is a public document. Insofar as the operation of the s. 8(4) Regime is further clarified by the Commissioner's Reports, and indeed by the ISC Report, the Anderson Report, and the Bulk Powers Review, those are also public documents.

97. As regards the foreseeability requirement, all the *Weber* criteria are met, for the reasons set out below.

(a) The "offences" which may give rise to an interception order

98. This requirement is satisfied by s. 5 of RIPA, which defines the purposes for which the Secretary of State can issue an interception warrant, provided that it is necessary and appropriate to do so, as read with the relevant definitions in s. 81 of RIPA and §§6.11-6.12 of the Code[28]. This follows, in particular, from a straightforward application of §159 of *Kennedy,* and §133 of *RE v United Kingdom* (App. No. 62498/11). The First Section's reasoning and conclusions in this respect at §§330-335 of the Judgment are right. (See further below at §§129-132 as regards the meaning of "national security").

(b) The categories of people liable to have their telephones tapped

99. As is clear from §97 of *Weber*, this second requirement in §95 of *Weber* applies both to the interception stage (which merely results in the obtaining / recording of communications) and to the subsequent selection stage (which results in a smaller volume of intercepted material being read, looked at or listened to by one or more persons).

100. As regards the **interception** stage:

[27] Insofar as the S. 8(4) Regime incorporates parts of the Intelligence Sharing and Handling regime, that also is "accessible".

[28] By section 5(2) RIPA, the Secretary of State may not issue a warrant unless he believes that the warrant is "*necessary on grounds falling within subsection (3)*", and that the conduct authorised by the warrant is proportionate. A warrant is necessary on grounds falling within s.5(3) only 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 UK, in circumstances appearing to the Secretary of State to be relevant to the interests of national security. The terms "*preventing*", "*detecting*" and "*serious crime*" are all defined in s.81 RIPA.

(1) As appears from s. 8(4)(a) and s. 8(5) of RIPA, a s. 8(4) warrant is directed primarily at the interception of external communications.
(2) The term "*communication*" is sufficiently defined in s. 81 of RIPA[29]. The term "*external communication*" is sufficiently defined in s. 20 RIPA and §5.1 of the Code.
(3) As is made clear in numerous public documents, a s. 8(4) warrant may in principle result in the interception of the entirety of the contents of a bearer or bearers. Similarly, during the Parliamentary debate on the Bill that was to become RIPA, Lord Bassam referred to intercepting the whole of a communications "*link*" (see **CB/38**).
(4) In addition, a s. 8(4) warrant may in principle authorise the interception of internal communications insofar as that is necessary in order to intercept the external communications to which the s. 8(4) warrant relates. See s. 5(6) of RIPA[30], and the reference back to s. 5(6) in s. 8(5)(b) of RIPA (which latter provision needs to be read with s. 8(4)(a) of RIPA). This point was also made clear to Parliament by Lord Bassam, and it has in any event been publicly confirmed by the Commissioner.
(5) Nevertheless, the Code makes clear that the intercepting agency should use its knowledge of the way in which international communications are routed, together with regular surveys of relevant communication links, to identify those individual communications bearers which are most likely to contain communications that meet the descriptions of material certified by the Secretary of State under s.5(3) of RIPA, and intercept only those bearers: see Code, §6.7 (and Farr §154, **CB/8**). Further, the choice of bearers is subject to the oversight of the Commissioner: see §§58-59 above.
(6) In the circumstances, and given that an individual should not be enabled "*to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly*" and in the light of the available oversight mechanisms of the ISC, IPT and Commissioner, the s. 8(4) regime sufficiently identifies the categories of people who are liable to have their communications intercepted, and sufficiently limits those categories.

101. As regards the **selection for examination** and **examination** stages:

(1) No intercepted material will be read, looked at or listened to by any person unless it falls within the terms of the Secretary of State's certificate, and unless (given s. 6(1) HRA) it is proportionate to do so in the particular circumstances of the case. See s.16(1) RIPA.
(2) The categories of communications set out in the Secretary of State's certificate must relate directly to the intelligence-gathering priorities set by the Joint Intelligence Committee and agreed by the National Security Council (see the Code at §6.14, and see too for confirmation of the factual position the ISC Report, **CB/47**, at §100, third bullet point).
(3) The Commissioner confirmed in his 2013 Report that the certificate is regularly reviewed and subject to modification by the Secretary of State[31]. The Code also makes clear that any changes to the description of material specified in the certificate must be reviewed by the

[29] "*Communication*", as defined in s.81 RIPA, means (as far as material) *"anything comprising speech, music, sounds, visual images or data of any description"* and *"signals serving either for the impartation of anything between persons, between a person and thing or between things or for the actuation or control of any apparatus."*

[30] *"(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…"*

[31] See the 2013 Report at §6.5.43, **CB/35**, and see too Farr w/s §80, **CB/9**.

Commissioner: see Code, §6.14.

(4) Material will only fall within the terms of the certificate insofar as it is of a category described therein; and insofar as the examination of it is necessary on the grounds in ss. 5(3)(a)-(c) RIPA. Those grounds are themselves sufficiently defined for the purposes of the foreseeability requirement. See §159 of *Kennedy*[32] (and see also *mutatis mutandis* §160 of *Kennedy*: "*there is an overlap between the condition that the categories of person be set out and the condition that the nature of the offences be clearly defined*"). See further at §§129-132 below as regards the meaning of "national security".

(5) Further, s. 16(2) RIPA, as read with the exceptions in s. 16(3)-(5A), places sufficiently precise limits on the extent to which intercepted material can be selected to be read, looked at or listened to according to a factor which is referable to an individual who is known to be for the time being in the British Islands and which has as its purpose, or one of its purposes, the identification of material contained in communications sent by him or intended for him. Thus, by way of example, intercepted material could not in general be selected to be listened to by reference to a UK telephone number. Before this could be done, it would be necessary for the Secretary of State to certify that the examination of that person's communications by reference to such a factor was necessary; and any such certification would need to reflect the NSC's "Priorities for Intelligence Collection"[33]. Moreover, the system ensures that, if is subsequently discovered that an individual is actually in the UK, when previously that was not known, the Intelligence Services must cease all action at that point, unless authorisation is obtained pursuant to the provisions of ss. 16(3)-(5) RIPA[34].

(6) Further, all selectors and search criteria must be listed, and must be justified as necessary and proportionate. That justification must be accessible to the Commissioner for audit: see §35 above. Thus, it is wrong to conclude that there are not robust controls over the selection of material for examination. Only material that has been selected for examination can be examined: all other material must be discarded, either immediately once selection for examination has occurred, or following a very short period (of a few days) when complex queries might be run on the data.

102. The above controls in s.16 RIPA (and the HRA) constrain all access at the selection stage, irrespective whether such access is requested by a foreign intelligence partner. Further, any such access requested by a foreign partner, as it would amount to a disclosure by the Intelligence Service in question to another person, would similarly have to comply with s. 6(1) of the HRA and be subject to the constraints in ss. 1-2 of the SSA and ss. 1-2 and 3-4 of the ISA, as read with ss. 19(3)-(5) of the CTA.

103. The above provisions do not permit indiscriminate trawling, as the Commissioner has publicly confirmed (see his 2013 Annual Report at §6.5.43, **CB/35**).

104. In the light of the above and, having regard - again - to the principle that an individual should not be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly and to the available oversight mechanisms, the s.

[32] The Applicants argue that the meaning of "*serious crime*" is insufficiently clear; but at §159 of *Kennedy* the ECtHR observes that RIPA itself contains a clear definition both of "*serious crime*" and what is meant by "*detecting*" serious crime: see section 81 RIPA.

[33] See the Code, §6.14. The Applicants have complain that "*no guidance is given as to how the Secretary of State will assess such necessity*". However, that contention is wrong. See §7.19 of the Code, p.34 of the First Section's Judgment.

[34] See e.g. §112(iv) of the ISC Report at **CB/46**.

8(4) regime sufficiently identifies the categories of people who are liable to have their communications read, looked at or listened to by one or more persons.

(c) Limits on the duration of telephone tapping

105. The s. 8(4) Regime makes sufficient provision for the duration of any s.8(4) warrant, and for the circumstances in which such a warrant may be renewed: see §161 of *Kennedy*, and the specific provisions for renewal of a warrant contained in §§6.22-6.24 of the Code[35]. Thus, under the Code, the application for renewal must be made to the Secretary of State; must contain all the detailed information set out in §6.10 of the Code; must give an assessment of the value of interception to date; and must state why interception continues to be necessary for one or more of the statutory purposes in s.5(3) RIPA, and proportionate.

106. No s.8(4) warrant may be renewed unless the Secretary of State believes that the warrant continues to be necessary on grounds falling within s.5(3) RIPA: see s.9(2) RIPA. Further, by s.9(3), the Secretary of State must cancel a s.8(4) warrant if he is satisfied that it is no longer necessary on those grounds. Detailed provision for the modification of warrants and certificates is made by s.10 RIPA.

107. §6.27 of the Code requires records to be kept of all renewals and modifications of s.8(4) warrants/certificates, and the dates on which interception was started and stopped, thus enabling the Commissioner to have the appropriate oversight.

108. The possibility that a s. 8(4) warrant might be renewed does not alter the analysis. If, in all the circumstances, a s. 8(4) interception warrant continues to be necessary and proportionate under s. 5 of RIPA each time it comes up for renewal, then the Secretary of State may lawfully renew it. The Strasbourg test does not preclude this. Rather, the test is whether there are statutory limits on the operation of warrants, once issued. There are such limits here.

109. Moreover, for completeness, it should be noted that these are not circumstances in which warrants will *"always be renewed",* contrary to the Applicants' assertion. That assertion is directly contrary to §6.7 of the Code. Further, the Commissioner's reports show that he carefully examines the justification for warrant renewals, and that the Secretary of State appropriately seeks further information about warrants where required, and refuses to authorise them if insufficient justification is provided: see e.g. §§6.41 and 6.69 of the Commissioner's 2015 Annual Report, **CB/37**.

(d)-(e) The procedure to be followed for examining, using and storing the data obtained; and the precautions to be taken when communicating the data to other parties

110. Insofar as the intercepted material cannot be read, looked at or listened to by a person pursuant to s. 16 (and the certificate in question), it is clear that it cannot be used at all. Prior to its destruction, it must of course be securely stored (§7.7 of the Code).

111. As regards the intercepted material that can be read, looked at or listened to pursuant to s. 16 (and the certificate in question), the applicable regime is well sufficient to satisfy the fourth and fifth foreseeability requirement in §95 of *Weber*. See §163 of *Kennedy*, and the following matters

[35] Note too that the provisions for renewal of a warrant contained in §§6.22-6.24 of the Code are at least as detailed as those found lawful by the ECtHR in relation to the renewal of warrants for covert surveillance under Part II RIPA, considered in *RE v United Kingdom*: see *RE* at §137.

(various of which add to the safeguards considered in *Kennedy*):

(1) Material must generally be selected for possible examination applying search terms, by equipment operating automatically for that purpose (so that the possibility of human error or deliberate contravention of the conditions for access at this point is minimised). Selectors/search terms must be justified: see above.
(2) Moreover, any analyst who examines material must create a record setting out why access to the material is required and proportionate, and consistent with the applicable certificate, and stating any circumstances that are likely to give rise to a degree of collateral infringement of privacy, and any measures taken to reduce the extent of that intrusion. See the Code, §7.16.
(3) The Code affords further protections to material accessed under the s.8(4) Regime at §§7.11-7.20. Thus, material should only be read, looked at or listened to by authorised persons receiving regular training in the operation of s.16 RIPA and the requirements of necessity and proportionality; systems should to the extent possible prevent access to material without the record required by §7.16 of the Code having been created; the record must be retained for the purposes of subsequent audit; access to the material must be limited to a defined period of time; if access is renewed, the record must be updated with the reasons for renewal; systems must ensure that if a request for renewal of access is not made within the defined period, no further access will be granted; and regular audits, including checks of the particular matters set out in the Code, should be carried out to ensure that the requirements in s.16 RIPA are met.
(4) Material can be used by the Intelligence Services only in accordance with s. 19(2) of the CTA, as read with the statutory definition of the Intelligence Services' functions (in s. 1 of the SSA and ss. 1 and 3 of the ISA) and only insofar as that is proportionate under s. 6(1) of the HRA. See also §7.6 of the Code as regards copying and §7.7 of the Code as regards storage (the latter being reinforced by the seventh data protection principle).
(5) Further, s. 15(2) RIPA sets out the precautions to be taken when communicating intercepted material that can be read, looked at or listened to pursuant to s. 16 to other persons (including foreign intelligence agencies[36]). These precautions serve to ensure *e.g.* that only so much of any intercepted material or related communications data as is "*necessary*" for the authorised purposes (as defined in s. 15(4)) is disclosed. The s. 15 safeguards are supplemented in this regard by §§7.4 and 7.5 of the Code. The obligations imposed by those provisions of the Code include that where intercepted material is disclosed to the authorities of a foreign state, the agency must take reasonable steps to ensure that the authorities have and will maintain the necessary procedures to safeguard the intercepted material, and to ensure that it is disclosed, copied, distributed and retained only to the minimum extent necessary (and it must not be further disclosed to the authorities of a third country unless explicitly agreed).
(6) In addition, any such disclosure must satisfy the constraints imposed by ss. 1-2 of the SSA and ss. 1-2 and 3-4 of the ISA, as read with ss. 19(3)-(5) of the CTA and s. 6(1) of the HRA. Further, and as in the case of the Intelligence Sharing and Handling Regime, disclosure in breach of the "arrangements" for which provision is made in s. 2(2)(a) of the SSA and ss. 2(2)(a) and 4(2)(a) of the ISA is rendered criminal by s. 1(1) of the OSA.

---

[36] *"s.15(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."

112. As already noted, the detail of the s.15 and s.16 arrangements is kept under review by the Commissioner.

(f) The circumstances in which recordings may or must be erased or the tapes destroyed

113. Section 15(3) of RIPA and §§7.8-7.9 of the Code (including the obligation to review retention at appropriate intervals, and the specification of maximum retention periods for different categories of material, which should normally be no longer than 2 years) make sufficient provision for this purpose. See *Kennedy* at §§164-165 (and note that further safeguards in §7.9 of the Code, including the specification of maximum retention periods, have been added to the Code since *Kennedy*). Both s. 15(3) and the Code are reinforced by the fifth data protection principle.

114. Further, and as noted at §40 above, the period for which communications intercepted under the s.8(4) Regime are in fact retained by the relevant Intelligence Services is, save in exceptional circumstances where a specific case for longer retention is made, no longer than a few months, after which they are automatically deleted.

Conclusion as regards the interception of communications

115. It follows that the s. 8(4) regime provides a sufficient public indication of the safeguards set out in §95 of *Weber*. As this is all that "foreseeability" requires in the present context (see §§95-102 of *Weber*), it follows that the s. 8(4) regime is sufficiently "*foreseeable*" for the purposes of the "*in accordance with the law*" requirement in Art. 8(2). The IPT was right so to conclude in the Liberty proceedings.

(5) Further issues regarding foreseeability/accessibility raised by the Applicants

116. The Applicants raise certain specific complaints about the foreseeability of the s.8(4) Regime, each of which is addressed below in order to explain why it does not affect the general conclusion on foreseeability/accessibility set out above. They are:

(1) The fact that there is no requirement for subsequent notification;
(2) The supposedly *"expansive"* definition of "external communications";
(3) The breadth of the concept of "national security" and/or "serious crime";
(4) The supposed relevance of EU law.

No requirement for subsequent notification

117. The 10 HR Applicants have asserted on the basis of *Szabo* that there should be a minimum requirement of subsequent notification to individuals, when this no longer jeopardises the purpose of surveillance. This argument is wrong. Further, as the First Section rightly pointed out at §317 of its Judgment, it is wholly impracticable, because it *"assumes the existence of clearly defined surveillance targets, which is simply not the case in a bulk interception regime"*.

118. As set out above, the *Szabo* decision has to be read in the context of a regime which contained no meaningful safeguards. The Court reached its determination on the basis that there was a failure to comply with the *Weber* criteria, and it was unnecessary for the Court to embark on the question whether enhanced guarantees were necessary (§70). Accordingly, the Court did

not purport to lay down further minimum requirements over and above *Weber*; and there was no indication in §86 that subsequent notification of surveillance measures was such a requirement. As the Court noted at §86, it was the *combination* of a complete absence of safeguards plus a lack of notification which meant that the regime could not comply with Art. 8 ECHR.

119. The work of the Intelligence Services must be conducted in secret if it is to be effective in achieving its aims. The value of intelligence work often relies on an identified target not knowing that his activities have come to the attention of the agencies, and/or not knowing what level of access to his activities the agencies have achieved. The requirement to notify a suspect of the use of bulk data tools against him, simply on the grounds that investigations have been concluded, would fundamentally undermine the work of the agencies. It may also threaten the lives of covert human intelligence sources close to him, such as a source who has provided the target's telephone number or email address to the Intelligence Services. Moreover, such a notification requirement may be wholly impractical in the case of many of the targets of interception under the s.8(4) Regime, who will be based abroad (often in locations lacking State control), and whose personal details may be unknown or imperfectly known.

120. The Government notes that this is wholly consistent with the reasoning of the Court in *Klass v Germany* at §58:

> *"In the opinion of the Court, it has to be ascertained whether it is even feasible in practice to require subsequent notification in all cases.*
>
> *The activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, as the Federal Constitutional Court rightly observed, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents. In the Court's view, in so far as the 'interference' resulting from the contested legislation is in principle justified under Article 8 (2) (see para. 48 above), the fact of not informing the individual once surveillance has ceased cannot itself be incompatible with this provision, since it is this very fact which ensures the efficacy of the 'interference'...*"

The definition of "external communications"

121. The Applicants complain about the supposedly "*expansive*" way in which the Government applies the definition of "*external communications*" in s.20 RIPA, by reference to Farr §§129-138 (**CB/8**), and contend that this "*expansive*" interpretation is insufficiently accessible. An identical complaint was rightly rejected by the IPT (see the 5 December Judgment, §§93-101 (**CB/14**)) for good reasons:

122. **First**, the definition of "*external communications*" in s.20 RIPA and the Code is itself a sufficiently clear one[37]. It draws a distinction between communications that are both sent and received within the British Islands (however they are routed), and communications that are not both sent and received within the British Islands; and the focus of the definition is upon the ultimate sender, and ultimate intended recipient, of the communication.

[37] The meaning of an "*external communication*" for the purposes of Chapter I of RIPA is stated in s. 20 of RIPA to be "*a communication sent or received outside the British Islands*". That definition is further clarified by §6.5 of the Code (which explains inter alia that communications both sent and received in the British Islands are not external, merely because they pass outside the British Islands en route).

123. Further, although the ways in which the internet may be used to communicate evolves and expands over time, the application of the definition remains foreseeable. For instance, where the ultimate recipient is *e.g.* a Google web server (in the case of a Google search), the status of the search query - as a communication - will depend on the location of the server. See Farr §§133-137[38], **CB/9**. That said, the nature of electronic communication over the internet means (and has always meant) that the factual analysis whether a particular communication is external or internal may in individual cases be a difficult one, which may only be possible to carry out with the benefit of hindsight. But that is not a question of any lack of clarity in RIPA or the Code: it reflects the nature of internet-based communications[39].

124. However, the Applicants wrongly assume that any such difficulties in applying the definition of "*external communication*" to a specific individual communication is relevant to the operation of the s. 8(4) Regime in relation to that communication. It is not:

(1) The legislative framework expressly authorises the interception of internal communications not identified in the warrant, to the extent that this is necessary to obtain the "*external communications*" that are the subject of the warrant: see s.5(6)(a) RIPA; and it is in practice inevitable that, when intercepting material at the level of communications links, both "*internal*" and "*external*" communications will be intercepted.

(2) The distinction between external and internal communications offers an important safeguard at a "macro" level, when it is determined what bearers should be targeted for interception under the s. 8(4) Regime. When deciding whether to sign a warrant under s. 8(4) RIPA, the Secretary of State will – indeed must – select communications links for interception on the basis that they are likely to contain external communications of intelligence value, which it is proportionate to intercept. Moreover, interception operations under the s. 8(4) Regime are conducted in such a way that the interception of communications that are not external is kept to the minimum necessary to achieve the objective of intercepting wanted external communications (Farr §154). However, that has nothing to do with the assessment whether, in any specific case, a particular internet-based communication is internal or external, applying the definition of "external communication" in s. 20 of RIPA and the Code.

125. In short, how the definition of "*external communication*" applies to any particular electronic communication is immaterial to the foreseeability of its interception. This is the **second** point.

126. **Thirdly**, the safeguards in ss. 15 and 16 RIPA (as elaborated in the Code) apply to internal

[38] The Applicants' case has heretofore been that the Code should explain how the distinction between "external" and "internal" communications applies to various modern forms of internet use. The difficulty with this submission is if it were correct, then each time a new form of internet communication is invented, or at least popularised, the Code would need to be amended, published in draft, and laid before both Houses of Parliament, in order specifically to explain how the distinction applied to the particular type of communication at issue. That would be both impractical and (because the question whether a communication is "external" does not determine whether it can be examined) pointless; and the "in accordance with the law" test under Art. 8 cannot conceivably impose such a requirement.

[39] For example, suppose that London-based A emails X at X's Gmail email address. The email will be sent to a Google server, in all probability outside the UK, where it will rest until X logs into his Gmail account to retrieve the email. At the point that X logs into his Gmail account, the transmission of the communication will be completed. If X is located within the British Islands at the time he logs into the Gmail account, the communication will be internal; if X is located outside the British Islands at that time, the communication will be external. Thus it cannot be known for certain whether the communication is in fact external or internal until X retrieves the email; and until X's location when he does so is analysed.

as much as to external communications, and thus the scope of application of these safeguards does not turn on the distinction between these two forms of communication.

127. **Fourthly**, it is the safeguard in s. 16(2) RIPA that affords significant protections for persons within the British Islands at the stage of selection for examination, and this provision does not turn on the definition of external communications, but on the separate concept of a "*factor ... referable to an individual who is known to be for the time being in the British Islands*"[40].

128. For all those reasons, any difference of view between the Applicants and the Government as to the precise ambit of the definition of "*external communications*" in s.20 RIPA does not render the s.8(4) Regime contrary to Article 8(2) ECHR. The IPT was right so to conclude in the Liberty proceedings.

The breadth of the concept of "national security"

129. **First,** the ECtHR has consistently held in a long line of authority that the term "national security" is sufficiently foreseeable to constitute a proper ground for secret surveillance measures, provided that the ambit of the authorities' discretion is controlled by appropriate and sufficient safeguards. The applicant in *Kennedy* similarly asserted that the use of the term "national security" as a ground for the issue of a warrant under s.5(3) RIPA was insufficiently foreseeable; and that argument was rejected in terms by the ECtHR at §159. The First Section rightly followed that reasoning: see §§331-335 of the Judgment.

130. Further, the Grand Chamber in *Zakharov* cited §159 of *Kennedy*; reiterated its observation that threats to national security may *"vary in character and be unanticipated or difficult to define in advance"*; and reasoned to the effect that a broad statutory ground for secret surveillance (such as national security) will not necessarily breach the "foreseeability" requirement, provided that sufficient safeguards against arbitrariness exist within the applicable scheme as a whole: see *Zakharov* at §§247-249 and 257[41]. In this case, for all the reasons already set out above such safeguards plainly exist, both by virtue of the detailed provisions of the Code, and by virtue of the oversight mechanisms of the Commissioner, the ISC and the IPT.

131. **Secondly**, the English Courts have not adopted a particularly unusual, surprising or broad approach to the definition of "national security". The Applicants' submission to the contrary is wrong, and none of the cases upon which they have relied supports their position (*Secretary of State for the Home Department v Rehman* [2003] 1 AC 153, *R(Corner House) v Director of the Serious Fraud Office* [2009] 1 AC 756, *R v Gul* [2014] AC 1260 and *R(Miranda) v Home*

[40] For example, London-based person A undertakes a Google search. Such a search would in all probability be an external communication, because it would be a communication between a person in the British Islands and a Google server probably located in the US (see Farr §134). Nevertheless, irrespective of whether the communication was external or internal, it could lawfully be intercepted under a section 8(4) warrant which applied to the link carrying the communication, as explained above. However, it could not be examined by reference to a factor relating to A, unless the Secretary of State had certified under section 16(3) RIPA that such examination was necessary, by means of an express modification to the certificate accompanying the section 8(4) warrant.

[41] See too *Szabo* at §64 (where the Court stated that it was "not wholly persuaded" by a submission that a reference to "terrorist threats or rescue operations" was insufficiently foreseeable, "*recalling that the wording of many statutes is not absolutely precise, and that the need to avoid excessive rigidity and to keep pace with changing circumstances means that many laws are inevitably couched in terms which, to a greater or lesser extent, are vague."*

Secretary [2014] 1 WLR 1340[42]). In *Rehman*, the House of Lords did no more than hold that national security was a "*protean concept*" which could be prejudiced by the promotion of terrorism in a foreign country by a UK resident, without any *"direct threat"* to the UK. That is unsurprising, and wholly consistent with the Court's own case law. The *Corner House, Gul* and *Miranda* cases did not address the meaning of "national security" at all, but rather the definition of "terrorism" in the Terrorism Act 2000. That is only a definition for the purposes of the Act: it does not purport to be a universal definition of "terrorism", still less of national security.

132. **Thirdly,** the s.8(4) Regime is designed so as to ensure that a person's communications cannot be examined by reference to unparticularised concerns of "national security". Rather, a specific and concrete justification must be given for each and every access to those communications; that justification must give specific reasons, which fall within the Secretary of State's certificate and broadly reflect the NSC's "Priorities for Intelligence Collection"; and the justification must be contained in an auditable record, subject to internal and external oversight. So the regime contains adequate safeguards against abuse by reference to an overbroad or nebulous approach to "national security". See the Code, §6.14, §7.16 and §7.18.

The CJEU's case law concerning data retention is irrelevant.

133. The Applicants place some reliance upon the CJEU's judgment in Joined Cases *Tele2 Sverige C-203/15* and *Watson & ors C-698/15* EU:C:2016:572, "*Watson",* 21 December 2016. *Watson* is immaterial to the questions before this Court.

134. *Watson* was a preliminary reference concerning the compatibility with EU law of requirements for communications services providers ("CSPs") to retain customer data, so that it could be made available to national authorities, in particular in the context of criminal investigations[43]. It was not concerned with the activities of national authorities themselves in the sphere of national security, nor could it have been.

135. The EU may only act within the sphere of competencies conferred upon it by the Member States in the Treaties. Matters of Member States' national security are not conferred on the EU. They are positively identified as being the sole responsibility of Member States in Article 4(2) of the Treaty on European Union ("TEU")[44]. This issue, as to whether the EU has any competence in this sort of national security sphere, is the subject of the reference to the CJEU recently made

---

[42] *Miranda* is at **CB/53.**

[43] *Watson* (**CB/57**) concerned (i) the compatibility with EU law of a requirement for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users, so that it could be made available to the national authorities for the purposes of fighting crime (such a requirement existing in Swedish law for the purposes of implementing Directive 2006/24/EC); and (ii) the issue whether *Digital Rights Ireland Ltd v Minister for Communications C-293/12* EU:C:2013:238 laid down mandatory requirements of EU law applicable to Member States' domestic regimes governing access to data retained by CSPs in accordance with national legislation.

[44] Articles 4(1) and (2) TEU provide as follows (underlining added):
"1. In accordance with Article 5, competencies not conferred upon the Union in the Treaties remain with the Member States.
2. The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State."

by the IPT in the Privacy 2 Judgment (**CB/21**).

136. As appears from that judgment, there are live issues not merely about this foundational jurisdictional issue flowing from Article 4(2) TEU. There is also a set of live issues as to whether (a) the CJEU was even purporting to consider or address the nature of any safeguards it considered necessary in a context involving state activity in the protection of national security (the Government's case is that the CJEU was not purporting to do so); and (b) how the sorts of safeguards the CJEU considered in those cases could conceivably be considered appropriate, let alone necessary, in such a context. The Court is invited to read the Privacy 2 Judgment in particular in relation to point (b).

137. It is evident that the IPT (with its intimate knowledge of the work of the Intelligence Services and the nature and operation of the safeguarding regimes) had the gravest doubts as to whether those sorts of safeguards could appropriately be applied into the very different national security context before it: see especially §§54-69 of the Privacy 2 Judgment (**CB/21**). That was particularly so given their conclusion that, if the *Watson* requirements did apply "*to measures taken to safeguard national security, in particular the [bulk communications data] regime, they would frustrate them and put the national security of the United Kingdom, and, it may be, other Member States, at risk"* (§69).

138. It is to be noted finally in this respect that this Court has had the opportunity over the years on many occasions to consider the necessary safeguards to be applied in similar contexts with potentially profound impacts on national security. Those Convention safeguards, as appears clearly from the Court's jurisprudence, sit within and are to be considered as part of the Convention scheme as a whole. That scheme represents a balance between private interests and the interests of the general community; and it involves a recognition of the proper national responsibility, subject to oversight by the Court, for the protection of the State's citizens. Given that long experience, it is unsurprising that the CJEU has repeatedly (and correctly under the EU Treaties including the Charter) emphasised that, in summary, it takes its lead on these sorts of issues from this Court's jurisprudence.

(6) Should different standards be applied to RCD, from those applied to communications? If so, what are those standards? (I.e. the Court's Questions 2(a) and (d) in the context of RCD)

Intercepting communications is in general more intrusive than obtaining communications data

139. The ECtHR recognised in §84 of *Malone* that it is less intrusive to obtain communications data than the content of communications. This remains the case even in relation to internet-based communications. For instance, obtaining the information contained in the "to" and "from" fields of an email (*i.e.* who the email is sent to, and who the email is sent by) will generally involve much less intrusion into the privacy rights of those communicating than obtaining the message content in the body of that email.

140. It is possible that aggregating communications data may in certain circumstances (and, potentially, with the addition of further information that is not communications data) yield information that is more sensitive and private than the information contained in any given individual communication. However, in general terms, content is likely to be more sensitive and private than communications data. Moreover, the most sensitive communications will always be more sensitive than whatever information can be inferred from aggregated communications data.

§10 of Mr Brown's w/s, lodged on behalf of the Applicants (**CB/4**), provides a good example. Mr Brown says that the fact that a woman has called her gynaecologist is the type of information that could be inferred from communications data. True it is, the fact that a woman has called a particular telephone number, and that that telephone number belongs to someone with the title "*Dr*", are both forms of communications data (the latter being a form of subscriber information falling in principle within s. 21(4)(b) RIPA). But the fact the doctor in question is her gynaecologist cannot be established by communications data alone (as opposed to the telephone call itself, or other information). Further, what might be said in that telephone call would always potentially be more sensitive than anything to be inferred from the fact of the telephone call itself.

141. Moreover, any information from or about a communication that is not RCD for the purposes of the statutory definition in ss.20/21 RIPA falls to be treated as content, not communications data, under the s.8(4) Regime; and RCD is only a limited subset of metadata as a whole (as the First Section put it at §355 of its Judgment, it is *"not to be confused with the much broader category of communications data"*: see further below.

What standards should be applied to RCD?

142. *Weber* concerned the interception of the content of communications (see §93 of *Weber*). The same standards applying to interception – i.e. the safeguards in §95 of *Weber* - have never previously been applied by the Court to the acquisition of communications data. This is unsurprising, and correct. As has already been noted, the covert acquisition of communications data is less intrusive in Art. 8 terms than the covert acquisition of the content of communications, and that remains true in the internet age. Thus, as a matter of principle, it is to be expected that the foreseeability requirement will be somewhat less onerous for covert powers to obtain communications data, than for covert powers to intercept the content of communications.

143. On the contrary, the Court has on numerous occasions since *Malone* reaffirmed the difference between obtaining the content of communications and other, less intrusive, forms of surveillance. For example:

(1) In *PG v UK* (App. No. 44787/98), 25 September 2001, the Court reaffirmed at §42 the difference between "metering" information i.e. obtaining a list of telephone numbers and times of calls (a form of RCD), and the content of communications, stating that the former was to be distinguished from the latter *"by its very nature"*;
(2) In *Uzun v Germany* app. No. 35623/05, 2 September 2010, the Court specifically declined to apply the "rather strict" standards in *Weber* to surveillance via GPS installed in a suspect's car, which tracked his movements in real time;
(3) In *Ben Faiza v France* (App. No. 21446/12), 8 February 2018, the Court (i) distinguished between use of a tracking device in *Uzun* and other forms of audio or visual surveillance, involving greater intrusion – see §53; and (ii) further distinguished between the greater degree of intrusion involved in geolocation in real time via a tracker, and the lesser degree of intrusion entailed in the collection of communications data *a posteriori*, showing where a suspect had previously been: see §74. RCD itself is (in part) a form of *a posteriori* location data, i.e. data of the lesser degree of intrusiveness addressed at §74 of *Ben Faiza*.

144. Instead of the list of specific safeguards in *e.g.* §95 of *Weber*, the test should therefore be the general one whether the law indicates the scope of any discretion and the manner of its exercise with sufficient clarity "*to give the individual adequate protection against arbitrary interference*"

(*Malone* at §68; *Bykov v. Russia* at §78), subject always to the critical principle that the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to obtain, access and use his communications data so that he can adapt his conduct accordingly (*c.f.* §93 of *Weber*, and §67 of *Malone*).

145. There is another important reason for this. If Member States operating a bulk interception regime were required to apply the same protections to RCD, as to content, then the likely result would simply be a watering down of the protection for content. Member States should not be discouraged from applying more stringent protections to content, because of the possibility that those protections would need to be read across to RCD, where they would be impracticable.

146. Indeed, the operation of the s.8(4) Regime exemplifies that point. The safeguard in s.16(2) RIPA requires the Secretary of State to certify the necessity of searching communications by reference to a factor referable to an individual who is known to be in the British Islands. So the Secretary of State is required personally to consider the necessity and proportionality of targeting such an individual in every case, on an individualised basis. That is an exercise which is reasonably practicable in the case of the content of the communications of one or two hundred individuals. If exactly the same exercise had to be done in relation to communications data, it would not be remotely feasible. This is partly because, historically, the selection of communications using factors referable to individuals known to be in the British Islands has for the most part taken place where the identity of the individual in question is known. However, communications data is used to a great extent to discover unknown threats. Moreover, there is a huge diversity of communications data types, and intelligence targets' use of technologies is constantly shifting. The result of these factors is that the number of queries that are made against communications data are significantly more than for content (many thousand in any given week in relation to individuals known or believed to be in the UK alone); and in a large number of such cases the identity of the individual to whom the RCD may relate is unknown, *even if* it is known or believed that they are in the British Islands. Moreover, the use of RCD is also invaluable in discounting individuals from further intelligence interest, including individuals in the UK – indeed, the use of RCD for this purpose is often deemed the most proportionate manner in which to determine whether an individual is of legitimate intelligence interest. An example of how such factors may arise would be the need to investigate a number of devices coming into the UK, possibly used by the same person, which have been used to contact known targets. The use of RCD to establish what other contacts have been made from the same devices could well establish whether there was any legitimate intelligence interest in the user or users of those devices. In order to make that assessment, it would be necessary to conduct searches of RCD using factors referable to a (possibly unknown) individual or individuals known or believed to be to be in the UK: these factors being information (*e.g.* a telephone number) relating to the communications devices that the individual or individuals hold. Exercises of this, or a comparable, type need to be carried out on a frequent basis for a number of unknown individuals: and this is only one of a number of necessary uses of RCD referable to individuals believed to be in the British Isles. Further, RCD often also has a temporal quality to it (for intelligence purposes), and having to delay conducting searches of such data pending the acquisition of an individual authority would seriously risk undermining the utility of it in intelligence terms. Requiring the Secretary of State to certify necessity and proportionality in every such individual case, in advance of searches being undertaken, could not possibly be done. So a system which required the very same protections for content and RCD could not realistically include the safeguard applied to the examination of content contained in in s.16(2) RIPA. Having to do so would result in a change of operational tradecraft by the Intelligence Agencies which would almost inevitably lessen the utility of RCD for intelligence purposes, and would in turn prejudice national security and put the

lives of UK citizens in danger.

(7) The s.8(4) Regime is in accordance with the law for the purposes of Article 8(2) as regards RCD

147. The s. 8(4) Regime gives the individual adequate protection against arbitrary interference as regards obtaining and use of RCD, with the single caveat set out in §149 below. Alternatively, if (contrary to all the above) the *Weber* criteria were to apply in this context, the criteria would also be met (again, subject to the same caveat):

(1) As a preliminary point, the controls within the s.8(4) Regime for RCD - as opposed to content - apply to only a limited subset of metadata. RCD for the purposes of the s.8(4) Regime has the statutory meaning given to it by ss.20 and 21 RIPA[45]. That meaning is not synonymous with, and is significantly narrower than, the term "metadata" used by the Applicants. The Applicants have defined "metadata" as "*structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource"*. On that definition, much "metadata" amounts to the content of communications for the purposes of the s.8(4) Regime, not RCD (since all information that is not RCD must be treated as content). For instance, email addresses or telephone numbers from the body of a communication would generate "metadata"; but would be "content" for the purposes of the s.8(4) Regime. The language or format used for a communication would be "metadata"; but again, "content" for the purposes of the s.8(4) Regime.

(2) The s. 8(4) Regime is sufficiently clear as regards the circumstances in which the Intelligence Services can **obtain** RCD. See §§98-100 above, which applies equally here.

(3) Once obtained, **access** to any related communications data must be necessary and proportionate under s. 6(1) of the HRA, and will be subject to the constraints in ss.1-2 of the SSA and ss. 1-2 and 3-4 of the ISA. Any access by any foreign intelligence partner at this stage would be constrained by ss. 15(2)(a) and 15(2)(b) of RIPA (as read with s. 15(4)); and, as it would amount to a disclosure by the Intelligence Service in question to another person would similarly have to comply with s. 6(1) of the HRA and be subject to the constraints in ss. 1-2 of the SSA and ss. 1-2 and 3-4 of the ISA, as read with ss. 19(3)-(5) of the CTA. Further, and importantly, the safeguards in §§7.1-7.10 of the Code (supplementing the s.15 "arrangements") apply here, as they do to communications. Those impose obligations including that where intercepted material is disclosed to the authorities of a foreign state, the

[45] By section 20 RIPA: *""Related communications data", in relation to a communication intercepted in the course of its transmission by means of a postal service or telecommunication system, means so much of any communications data (within the meaning of Chapter II of this Part) as-*

(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".

By section 21(4) RIPA:

"In this Chapter "communications data" means any of the following-

(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, or any part of a telecommunication system;

(c) *Any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service."*

agency must take reasonable steps to ensure that the authorities have and will maintain the necessary procedures to safeguard the intercepted material, and to ensure that it is disclosed, copied, distributed and retained only to the minimum extent necessary (and it must not be further disclosed to the authorities of a third country unless explicitly agreed).

(4) Just as for the content of communications, analysts wishing to access RCD must complete an auditable record, explaining why access is necessary and proportionate for an aim falling within the Intelligence Services' statutory purposes.

(5) Given the constraints in ss. 15 of RIPA and s. 6(1) of the HRA, communications data cannot be used (in combination with other information / intelligence) to discover *e.g.* that a woman of no intelligence interest may be planning an abortion (to use the example in Brown §10). This is for the simple reason that obtaining this information would very obviously serve none of the authorised purposes in s. 15(4). There is nothing unique about communications data (even when aggregated) here. Other RIPA powers, such as the powers to conduct covert surveillance and the use of covert human intelligence sources, might equally be said to be capable of enabling discovering of the fact that a woman of no intelligence interest may be planning an abortion (*e.g.* an eavesdropping device might be planted in her home, or a covert human intelligence source might be tasked to befriend her). But it is equally clear that these powers could not in practice be used in this way, and for precisely the same reason: such activity would very obviously not be for the relevant statutory purposes (see ss. 28(3), 29(3) and 32(3) of RIPA).

148. Further, there is good reason for s. 16 of RIPA covering access to intercepted material (*i.e.* the content of communications) and not covering access to communications data:

(1) 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 S. 8(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)). RCD is a significant resource in this regard.

(2) 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*".

149. The First Section has stated (Judgment §357) that the exemption of RCD from the safeguards applicable to accessing communications under s.16 RIPA should be *"limited to the extent necessary to determine whether an individual is, for the time being, in the British Islands".* For the reasons set out at §146 above, it would not be remotely practicable to apply exactly the same certification regime to RCD under s.16 of RIPA, as to communications. Further, the UK does not consider that complete parity of treatment is what the law requires, or indeed what the First Section can properly have intended: see §§142-146 above. Nevertheless, the UK accepts in light of the First Section's judgment that it would be desirable for there to be *some* type of certification regime for the examination of RCD using factors referable to individuals known to be in the British Islands. For that reason, the UK is taking steps to ensure that where non-content data is to be selected for examination by reference to a factor referable to a person who is believed to be in the British Islands, that must be certified as necessary and proportionate by the Secretary of State on a properly specific "thematic" basis (i.e. not individual by individual, but by reference to specified groups of individuals). An interim oversight arrangement has been agreed with the Investigatory Powers Commissioner pending the formal promulgation of those changes.

The UK also proposes to change the current code governing interception of communications under the Investigatory Powers Act 2016 to that effect.

150. The regime contains sufficient clear provision regarding the subsequent **handling, use and possible onward disclosure** by the Intelligence Services of related communications data. Section 15 RIPA and the safeguards in §§7.1-7.10 of the Code apply equally here. See §110-112 above.

151. The regime equally contains sufficiently clear provision concerning **erasure/destruction**. §§113 above applies equally here. Further, RCD obtained under the s.8(4) Regime is held for a maximum of one year before being deleted.

(8) The s.8(4) Regime satisfies the "necessity" test

152. The First Section was right to find that the s.8(4) Regime was proportionate, for the reasons it gave at §§384-386 of its Judgment.

153. The ECtHR has consistently recognised that when balancing the interests of a respondent State in protecting its national security through secret surveillance measures against the right to respect for private life, the national authorities enjoy a *"fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security"*: see e.g. *Weber* at §106, *Klass* at §49, *Leander* at §59, *Malone* at §81. Nevertheless, the Court must be satisfied that there are adequate and effective guarantees against abuse. That assessment depends on all the circumstances of the case, such as the nature, scope and duration of 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 e.g. *Zakharov* at §232.

154. To the extent that the Applicants rely on *Szabo and Vissy* for the proposition that a different test of "strict necessity" is required, it is submitted that the test set out the Grand Chamber in *Zakharov*, and in a long line of other well-established cases, is to be preferred. It represents a properly protective set of principles which balance the possible seriousness of the Article 8 interference with the real benefits to the general community of such surveillance in protecting them against acts of terrorism and other national security threats. Strict necessity as a concept is used expressly in the Convention scheme where appropriate – indicating that it should not be imported elsewhere; or, if that is permissible at all, then only with the greatest caution. There is no warrant for any stricter test in principle in the present context.

155. However, whether viewed through the prism of general necessity, or adopting the test of "strict necessity" in the respects identified in *Szabo*, the s.8(4) Regime satisfies the necessity test.

156. The rationale for the s.8(4) Regime and its operation have been addressed on a number of occasions by independent bodies, viz. the IPT, the ISC, the Commissioner, the Anderson Report, and the Bulk Powers Review. Materially, the Anderson Report, the Bulk Powers Review, the ISC Report and the IPT all conclude in terms, and with supporting analysis and detail, that less intrusive (or different) programmes could not address the legitimate needs of the UK. See above, §§15-28.

157. Although the Bulk Powers Review was not specifically tasked with opinion on whether bulk interception powers were proportionate, its conclusions are plainly highly material to that question, as summarised at §§23-25 above. At §§9.12-9.14 Lord Anderson QC stated:

"I have already summarised what I consider to be the strength of the operational case for each of the bulk powers (chapters 5-8 above). Among the other sources of evidence referred to in chapter 4 above, I have based my conclusions on the analysis of some 60 case studies, as well as on internal documents in which the SIAs offered frank and unvarnished assessments of the utility and limitations of the powers under review.

The sheer vivid range of the case studies – ranging from the identification of dangerous terrorists to the protection of children from sexual abuse, the defence of companies from cyber-attack and hostage rescues in Afghanistan – demonstrates the remarkable variety of SIA activity. Having observed practical demonstrations, questioned a large number of analysts and checked what they said against contemporaneous intelligence reports, neither I nor others on the Review team was left in any doubt as to the important part played by the existing bulk powers in identifying, understanding and averting threats of a national security and/or serious criminal nature, whether in Great Britain, Northern Ireland or further afield.

My specific conclusions, in short summary, are as follows:

(a) The bulk interception power is of vital utility across the range of GCHQ's operational areas, including counter-terrorism, cyber-defence, child sexual exploitation, organised crime and the support of military operations. The Review team was satisfied that it has played an important part in the prevention of bomb attacks, the rescuing of hostages and the thwarting of numerous cyber-attacks. Both the major processes described at 2.19 above [i.e. the "strong selector" and "complex query" process] produce valuable results. Communications data is used more frequently, but the collection and analysis of content has produced extremely high-value intelligence, sometimes in crucial situations. Just under 50% of GCHQ's intelligence reporting is based on data obtained under bulk interception warrants, rising to over 50% in the field of counter-terrorism." (emphasis added)

158. In light of the facts set out at §§15-28 above, to describe the Government's bulk interception as "*a speculative fishing exercise, designed to check the behaviour of an entire population*", as the Applicants have done, could not be further from the truth. It is a capability which is of "*vital utility*" in identifying and averting threats of a national security and/or serious criminal nature, carried out on the basis of careful assessment as to what bearers are most likely to carry communications which enable those threats to be ascertained.

159. If the Applicants wish to say that intercepting the contents of a bearer is inherently disproportionate, they must accept as a corollary the real possibility that the Intelligence Services will fail to discover major threats to the UK (such as a terrorist bomb plot, or a plot involving a passenger jet – see e.g. examples 2 and 6 in Annex 9 to the Anderson Report[46]). It would be absurd if the case law of the ECtHR required a finding of disproportionality in such circumstances, merely because the whole contents of a communications link are intercepted, even though only a tiny fraction[47] of intercepted communications are ever, and can ever be, selected for potential examination, let alone examined. On a proper analysis, it does not. See/compare *Weber* and §§29-49 above.

Question (3): Has there been an interference with the Applicants' rights under Article 8(1) on account of the operation of the Intelligence Sharing Regime, and if so, in what manner is the

[46] See **CB/48**

[47] I.e. on the basis that it is necessary and proportionate to do so, because they are of legitimate intelligence interest.

receipt of intelligence capable of giving rise to an interference with the rights of concrete individuals or organisations?

160. The answer is "no". The relevant Applicants[48] do not contend, and have put forward no evidential basis for contending, that their communications have in fact been shared with the Intelligence Services, having previously been intercepted and collected under Prism/Upstream. Rather, they assert only that their communications *"may be"* subject to foreign interception conveyed to UK authorities[49], or that they *"believe"* that to be the case[50]. In the circumstances, that mere assertion does not begin to establish that the Applicants are "directly affected" by the Intelligence Sharing Regime, such that they can properly claim to be victims of an interference with their Article 8(1) rights. Their complaint is in truth an abstract complaint about the regime itself, which the Court should not entertain.

161. The Grand Chamber has recently considered the Court's own case law and clarified the conditions under which an applicant can claim to be a victim of secret surveillance measures violating Article 8 ECHR, without having to prove that secret surveillance measures have in fact been applied to him: see *Zakharov v Russia*. *Zakharov* notes, and resolves, a potential divergence in the Court's case law between those cases suggesting that general challenges to the relevant legislative regime would be permitted in such circumstances, and those suggesting that the relevant security agencies must be reasonably likely to have applied the measures in question to the applicant. See *Zakharov* at §§164-172. The Government assumes (in the Applicants' favour) that the principles in *Zakharov* may also apply to a claim of violation of Article 8 concerning the receipt of secret intelligence from a foreign state.

162. Two conditions must be satisfied before an applicant can claim to be the victim of a relevant violation without needing to show his communications have been interfered with – see *Zakharov* at §171:

> *"Accordingly, the Court accepts that an applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures, if the following conditions are satisfied. Firstly, the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted. Secondly, the Court will take into account the availability of remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies."* (Emphasis added)

163. As to the second condition (the availability of national remedies), where the domestic system affords no effective remedy to a person who suspects he has been the victim of secret surveillance, an exception to the rule that individuals may not challenge a law *in abstracto* is justified. However, if the national system provides for effective remedies, as in the present case, an individual may claim to be a victim of a violation occasioned by the mere existence of secret measures only if he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures: *Zakharov* at §171.

---

[48] I.e. the BBW and 10 HR Applicants. The BIJ Applicants do not complain about the Intelligence Sharing Regime.

[49] See BBW Application, §§10-17;

[50] See 10 HR Application, §8.

164. Here, neither of the two conditions in §171 of *Zakharov* is satisfied. **First**, the Applicants do not belong to the group of persons who may be said to be possibly affected by the Intelligence Sharing Regime. They have put forward no basis on which they are at realistic risk of having their communications intercepted under the Prism or Upstream programmes, and shared with the Intelligence Services. In particular:

(1) The Prism and Upstream programmes permit the interception and acquisition of communications to, from or about specific tasked selectors associated with non-US persons who are reasonably believed to be outside the US. I.e. they concern unanalysed intercepted communications (and associated communications data) relating to particular individuals outside the US, not broad data mining. The First Section's finding to the contrary about Upstream is wrong.
(2) As stated in the Disclosure, the Intelligence Services have only ever made a request for such unanalysed intercepted communications (and associated communications data) where a RIPA warrant is already in place for that material, but the material cannot be collected under the warrant[51]. Any request made in the absence of a warrant would be exceptional, and would be decided upon by the Secretary of State personally: see the Code at §12.3.
(3) The conditions for intercepting communications pursuant to a RIPA warrant are as set out in s.5(3) RIPA. They are the interests of national security; the prevention or detection of serious crime; or the safeguarding of the UK's economic well-being, in circumstances appearing relevant to the interests of national security. Those conditions substantially mirror the statutory functions of the Intelligence Services under the SSA and ISA.
(4) None of the Applicants suggest that their data could be collected and shared under any of the conditions in s.5(3) RIPA. In each case, they claim that their data may be shared with the UK because of their human rights activities, or campaigning activities concerning freedom of expression. Such activities would not give any grounds for the issue of a warrant for interception of the Applicants' communications under s.5(3) RIPA. Nor, by the same token, would they give grounds for intelligence sharing without a warrant in pursuance of the Intelligence Services' statutory functions. The Applicants do not contend otherwise.

165. **Secondly,** the Applicants have available an effective remedy at national level, under which they can discover whether they have been the subject of unlawful intelligence sharing. That is a complaint to the IPT. The 10 HR Applicants complained to the IPT about whether they might have been subject to unlawful intelligence sharing. The IPT, having investigated the facts in detail, determined that they had not been. The BBW Applicants failed to complain to the IPT altogether.

166. In those circumstances, it is unnecessary and inappropriate for the Court to entertain an abstract challenge to the Intelligence Sharing Regime as a whole. For the same reason, there has been no breach of the Applicants' Article 8(1) rights. The First Section's conclusion to the contrary was based upon the misconception that Upstream was a bulk interception scheme similar to the s.8(4) Regime, which it is not: see Judgment, §395.

Question 4: If there has been an interference, was the Intelligence Sharing Regime in accordance with the law and necessary within the meaning of Article 8(2), and to what extent do the standards developed in the Court's case law on the interception of communications apply?

[51] See the IPT's 5 December Judgment, [48(2)].

The Intelligence Sharing Regime is "in accordance with the law"

167. The First Section was right to conclude that the Intelligence Sharing Regime is in accordance with the law and necessary within the meaning of Article 8(2).

168. The interferences at issue have a basis in domestic law. The statutory provisions in the Intelligence Sharing Regime[52] provide domestic law powers for the obtaining and subsequent use of communications and communications data in issue (assuming that this is necessary for one or more of the functions of the Intelligence Service in question, and proportionate for the purposes of s.6(1) HRA).

169. The law in question is accessible. It is set down in statute, and supplemented by chapter 12 of the Code. (Indeed, even prior to the issue of chapter 12 of the Code, it was "accessible" as a result of the Disclosure[53]). For these purposes, case law may form part of a corpus of accessible law: see e.g. *Huvig v France* 24 April 1990, Series A no. 176-B at §28, *Uzun v Germany* app. 35623/05 at §33.)

170. As to foreseeability in this context, the essential test, as recognised in §68 of *Malone v UK* is whether the law indicates the scope of any discretion and the manner of its exercise with sufficient clarity "*to give the individual adequate protection against arbitrary interference*". The Grand Chamber has confirmed in *Zakharov* that this test remains the guiding principle when determining the foreseeability of intelligence-gathering powers (see §230). Further, this essential test must always be read subject to the important and well-established principle that the foreseeability requirement cannot mean that an individual should be enabled to foresee when the authorities are likely to resort to secret measures so that he can adapt his conduct accordingly: *Malone* at §67; *Leander v. Sweden*, 26 March 1987, Series A no.116, at §51; and *Weber* at §93. The Intelligence Sharing Regime satisfies this test.

171. **First**, the regime is sufficiently clear as regards the circumstances in which the Intelligence Services can in principle **obtain** information from the US authorities.

172. The purposes for which such information can be obtained are explicitly set out in ss.1-2 SSA, and ss.1-2 and 3-4 ISA, which set out the functions of the Intelligence Services. They are the interests of national security, in the context of the various Intelligence Services' particular functions; the interests of the economic wellbeing of the United Kingdom; and the prevention and detection of serious crime. Thus, it is clear that e.g. GCHQ may in principle - as part of its function (in s. 3(1)(a) of ISA) of obtaining information derived from communications systems[54] - obtain communications and communications data from a foreign intelligence agency if that is *"in the interests of national security"*, with particular reference to the Government's defence and foreign policies (s.3(2)(a) ISA), or *"in the interests of the economic well-being of the United*

[52] I.e. the SSA and the ISA, as read with the CTA; the HRA; the DPA; and the OSA. In particular, the statutory powers and functions in the SSA and ISA, exercisable for the purposes set out in those Acts and in accordance with s.6 HRA, and read with s.19(2) CTA, provide the requisite domestic law powers for the Intelligence Services' obtaining and subsequent use of communications and communications data from foreign partners. See the First Section's Judgment at §§96-108.

[53] Moreover, the Disclosure was embodied in a draft of the Code, published in February 2015, with which the Government undertook to comply.

[54] Such systems fall within the scope of s. 3(1)(a) of ISA by virtue of being "equipment" producing "electromagnetic, acoustic and other emissions".

Kingdom" (s.3(2)(b) ISA), or "*in support of the prevention or detection of serious crime*" (s. 3(2)(c) of ISA); provided always that it is also necessary and proportionate to obtain information for that purpose under s. 6(1) of the HRA[55].

173. Contrary to the Applicants' contentions, those purposes are not too broad to be "in accordance with law". In fact, they are no wider in substance than the statutory purposes for which an interception warrant could be issued under s.5 RIPA (prior to its amendment by DRIPA[56]). Indeed, in certain respects, they are more tightly defined than the conditions for obtaining a warrant under s.5 RIPA (see *e.g.* s. 1(2) of the SSA, and 1(2)(a) and 3(2)(a) of the ISA, as compared with s. 5(3)(a) of RIPA[57]).

174. The statutory purposes for issue of a warrant under s.5 RIPA (in its unamended form) were considered by the Court in *Kennedy* and were found sufficiently detailed to satisfy the requirement of foreseeability, even in the context of interception of communications by the defendant state itself. See *Kennedy* at §159.

175. The Court has more recently found those very same purposes sufficiently detailed to satisfy the "foreseeability" test in the context of covert surveillance pursuant to Part II RIPA: see *RE v United Kingdom* app. 62498/11, 27 October 2015, at §133 (citing *Kennedy* with approval). (By contrast, the cases upon which the Applicants have relied– *Khan v United Kingdom* (app. 35304/97), ECHR 2000-V and *Halford v United Kingdom*, 25 June 1997, Reports of Judgments and Decisions 1997-III – are both ones concerning police surveillance, where there was at the relevant time no statutory framework regulating the conduct in question.)

176. Moreover, the circumstances in which the Intelligence Services may obtain information under the Intelligence Sharing Regime are further defined and circumscribed by the Code and Disclosure (which reflect what has always been the practice of the Intelligence Services). In particular, the Code provides the following public safeguards on obtaining information:

---

[55] The BBW Applicants are wrong to assert that the Intelligence Services may obtain information from foreign agencies "*for the purposes of any criminal proceedings*". The Intelligence Services are empowered to disclose information for the purposes of criminal proceedings (subject to other statutory safeguards upon such disclosure, such as the prohibition in s.17 RIPA on adducing intercept evidence in legal proceedings). However, such information can only be acquired in the first place if it is necessary and proportionate to do so for the statutory functions of the Services, set out above (which do not include the purposes of "any criminal proceedings"): see s.2(2)(a) SSA, and ss.2(2)(a) and 4(2)(a) ISA.

[56] With effect from 17 July 2014, the Data Retention and Investigatory Powers Act 2014 ("DRIPA") amended s.5(3) RIPA so that a warrant could be obtained for the purpose of safeguarding the economic well-being of the United Kingdom "*in circumstances appearing to the Secretary of State to be relevant to the interests of national security".* DRIPA was subject to a "sunset clause" expiring on 31 December 2016. However, this amendment to s.5(3) RIPA remained in place as a result of paragraph 9 of Schedule 9 to the Investigatory Powers Act 2016, which provides:
"The amendments made to the Regulation of Investigatory Powers Act 2000 by sections 3 to 6 of the Data Retention and Investigatory Powers Act 2014 (and those sections) continue to have effect despite section 8(3) of the Act of 2014 (sunset provision for that Act) until the provisions they amend (and those sections) are repealed by this Act in connection with the coming into force of provisions of this Act."
See also the provisions of the Code at §6.11, quoted at page 28 of the First Section's Judgment.

[57] By s. 1(2) of the SSA, one of the Security Service's functions is "*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*" (emphasis added). Similarly, the statutory definition of the national security functions of SIS and GCHQ refer to *"the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom*" (emphasis added). Compare s. 5(3)(a) of RIPA, which identifies "*the interests of national security"* as a ground for interception, without further elaboration.

(1) Save in exceptional circumstances, the Intelligence Services will only make a request for unanalysed intercepted communications and associated communications data, otherwise than in accordance with an international mutual legal assistance agreement, if a RIPA warrant is already in place covering the target's communications; the assistance of the foreign intelligence agency is necessary to obtain the communications because they cannot be obtained under that RIPA warrant; and it is necessary and proportionate for the Intelligence Services to obtain those communications. It should be noted that the circumstances are sufficiently exceptional that they have not yet ever occurred[58].
(2) If the Intelligence Services were to make a request for such material in the absence of a RIPA warrant, they would only do so if the request did not amount to a deliberate circumvention of RIPA or otherwise frustrate the objectives of RIPA. So, for example, the Intelligence Services could not make a request for material equally available by interception pursuant to a RIPA warrant. However, they could make a request for material which it was not technically feasible to obtain under Part I RIPA, and which it was necessary and proportionate for them to obtain pursuant to s.6 HRA.
(3) Further, if the Intelligence Services were to make a request for such material in the absence of a RIPA warrant, that request would be decided upon by the Secretary of State personally; and if the request was for "untargeted" material, any communications obtained would not be examined according to any factors mentioned in s.16(2)(a) and (b) RIPA, unless the Secretary of State personally considered and approved the examination of those communications by reference to such factors. In short, the same safeguards would be applied by analogy, as if the material had been obtained pursuant to a RIPA warrant.

177. **Secondly**, the Intelligence Sharing Regime is similarly sufficiently clear as regards the subsequent handling, use and possible onward disclosure of communications and communications data obtained by the Intelligence Services.

178. Under statute, handling and use is addressed by (i) s. 19(2) of the CTA[59], as read with the statutory definitions of the Intelligence Services' functions (in s. 1 of the SSA and ss. 1 and 3 of ISA); (ii) the general proportionality constraints imposed by s. 6 of the HRA and - as regards retention periods in particular - the fifth data protection principle; and (iii) the seventh data protection principle (as reinforced by the criminal offence in ss. 1(1) and 8(1) of the OSA) as regards security measures whilst the information is being stored.[60]

179. Moreover, additional safeguards as to the handling, use and onward disclosure of material obtained under the Intelligence Sharing Regime are provided by the Code. Specifically, chapter 12 of the Code provides that where the Intelligence Services receive intercepted communications content or data from a foreign state, irrespective whether it is solicited or unsolicited, analysed or unanalysed, and whether or not the communications data is associated with the content of communications, the communications content and data are subject to exactly the same internal rules and safeguards as the same categories of content or data, when the material is obtained

[58] See §48(2) of the IPT's 5 December judgment, **CB/14**

[59] *"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".*

[60] As to the fifth and seventh data protection principles, it is no answer for the Applicants to point to the "explicit exemption from the data processing principles in the context of processing data in the interests of national security", as they have done. The relevant certificates (which are publicly available) do not exempt the Intelligence Services from compliance with the fifth and seventh data protection principles. See also the First Section's Judgment, §106.

directly by the Intelligence Services as a result of interception under RIPA. That has important consequences:

(1) It means that the safeguards set out in s.15 RIPA, as expanded upon in Chapter 7 of the Code, apply to intercept material obtained under the Intelligence Sharing Regime. So for example, just as under RIPA:
   i. The number of persons to whom the material is disclosed or otherwise made available, the extent to which it is made available, the extent to which it is copied, and the number of copies that are made, must be limited to the minimum necessary for the purposes authorised in s.15(4) RIPA.
   ii. The material (and any copy) must be destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes in s.15(4) RIPA.
   iii. The arrangements for ensuring that (i) and (ii) above are satisfied must include such arrangements as the Secretary of State considers necessary to ensure the security of retained material: see s.15(5) RIPA.
   iv. The disclosure of intercepted material to authorities outside the UK is subject to the safeguards set out in §7.5 of the Code.

(2) It means that the internal rules and safeguards applicable to material obtained under the Intelligence Sharing Regime are *de facto* subject to oversight by the Commissioner, who offers an *"important safeguard against abuse of power"*: see s.57(2)(d) RIPA and *Liberty v UK* app. 58243/00, 1 July 2008 at §67.

180. **Thirdly**, when considering whether the Intelligence Sharing Regime is "*foreseeable*", the Court should take into account the available oversight mechanisms – namely, the ISC, the IPT, and (as set out above, with respect to oversight of the relevant internal "arrangements" themselves) the Commissioner. Those oversight mechanisms are important and effective, for all the reasons set out above and in the First Section's Judgment. The relevance of oversight mechanisms in the assessment of foreseeability, and in particular the existence of adequate safeguards against abuse, is very well established in the Court's case law, including in this context (see e.g. *Kennedy* at §§155-170, *Zakharov* at §§271-280).

181. The Court should also take into account in the foreseeability test, just as it did in *Kennedy* at §168, of the fact that the investigations by the oversight bodies have not revealed any deliberate abuse by the Intelligence Services of their powers. Neither the ISC nor Commissioner has found that the Intelligence Services have circumvented or attempted to circumvent UK law by receiving material under the Intelligence Sharing Regime, despite the fact that both of them have specifically investigated this allegation: see:

(1) The ISC's finding in its Statement of 17 July 2013 that the UK "*has not circumvented or attempted to circumvent UK Law*" by receiving material from the US[61];
(2) The Commissioner's rejection of the allegation that the Intelligence Services "*receive from US agencies intercept material about British citizens which could not lawfully be acquired by intercept in the UK ... and thereby circumvent domestic oversight regimes*" (see his 2013 Annual Report at §§6.8.1-6.8.6[62]).

[61] See **CB/43**. The investigation that preceded the ISC's Statement was thorough. See §5 of the Statement.

[62] See **CB/35**

182. **Finally,** for the purposes of the foreseeability test, the Court should take into account too that the IPT has examined the Intelligence Services' internal safeguards in the context of the Intelligence Sharing Regime in detail, and has found that adequate internal safeguards exist[63], and that the Regime as a whole (with the benefit of the Disclosure, now mirrored in the Code) is in accordance with the law. The fact that the applicable internal safeguards have now been examined not just by the Commissioner, but also by the domestic courts, and have been found to offer sufficient protection for the purposes of rights under the ECHR, is an important indicator that the regime as a whole provides adequate safeguards against abuse.

The Intelligence Sharing Regime satisfies the "necessity" test

183. No separate question of "necessity" arises with regard to the Intelligence Sharing Regime under Article 8 or Article 10 ECHR, distinct from the issue whether the regime is "in accordance with the law". If the regime itself is "in accordance with the law" (as it is), any issue of necessity would arise only on the individual facts concerning any occasion where intelligence was shared, since the sharing of intelligence may obviously be necessary and proportionate in some cases, but not others[64]. However, (i) the BBW Applicants do not allege that their data was in fact shared by the US authorities with the Intelligence Services, and since they brought no complaint to the IPT, no investigation has been made into any such allegation; (ii) the IPT investigated the allegation by the 10 HR applicants that there had been sharing of their data in breach of the necessity test, and did not so find.

To what extent should the standards developed in the Court's case law on the interception of communications apply?

184. There are very good reasons why the particular standards designed to apply in the context of the interception of communications, as set out in *Weber* at §95, cannot be read across to the Intelligence Sharing Regime.

185. **First,** if (contrary to all the points already made above), there has been any interference under Article 8(1), it is important to analyse what that "interference" consists in. The First Section rightly observed that the material "act" cannot be foreign states' interception of communications, over which the UK itself exercises no authority or control. Rather, it is the UK's receipt of intelligence, and its subsequent storage, examination and use: see the First Section's Judgment, §§420-421. In that context, it makes no sense at all to apply the first or second *Weber* criteria (the *"nature of the offences"* at issue, and *"definition of the categories of people liable to have their phone tapped"*). Those criteria could only sensibly apply, if the UK itself had control over the act of interception itself. It does not.

[63] See [55] of the IPT's 5 December Judgment, **CB/14**: *"Having considered the arrangements below the waterline, as described in the 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."*

[64] Note however Farr §§15-25, **CB/9,** regarding the general importance to the UK's national security interests of the intelligence it receives from the US authorities, which he states has led directly to the prevention of terrorist attacks and the saving of lives.

186. **Secondly**, this Court has expressly and repeatedly recognised that the "rather strict standards" developed in the recent Strasbourg intercept cases do not necessarily apply in other intelligence-gathering contexts: see e.g. *Uzun v. Germany* at §66. Further, this Court has never previously suggested that the form of wide-ranging and detailed scheme set out in *Weber* is necessary for intelligence sharing with foreign intelligence agencies (and see §96 of *S and Marper v. UK* (GC) nos. 30562/04 and 30566/04, ECHR 2008: domestic legislation "*cannot in any case provide for every eventuality*").

187. **Thirdly**, there is no good reason to single out intercepted communications / communications data from other types of information that might in principle be obtained from a foreign intelligence agency, such as intelligence from covert human intelligence sources, or covert audio / visual surveillance. In many contexts, the Intelligence Services may not even know whether communications provided to them by a foreign intelligence agency have been obtained as a result of interception[65]. Moreover, as Mr Farr explains, neither the sensitivity of the information in question, nor the ability of a person to predict the possibility of an investigative measure being directed against him, distinguish communications and communications data from other types of intelligence (Farr §§27-30, **CB/8**). Thus, it would be nonsensical if Member States were required to comply with the *Weber* criteria for receipt of intercept material from foreign States; but were not required to do so for any other type of intelligence that foreign States might share with them.

188. **Fourthly**, it would plainly not be feasible (or, from a national security perspective, safe) for a domestic legal regime to (i) set out in publicly accessible form (let alone set out in statute) <u>all</u> the various types of information that might be obtained, whether pursuant to a request or not, from each of the various foreign States with which the State at issue might share intelligence, (ii) define the tests to be applied when determining whether to obtain each such type of information and the limits on access and (iii) set out the handling, etc. requirements and the uses to which all such types of information may be put. See e.g. Farr §§56-61, **CB/9**.

189. **Finally,** if (contrary to the above) the *Weber* criteria were to apply in this context, the Intelligence Sharing Regime satisfies each of the six criteria through a combination of the statutory provisions governing the receipt of intelligence, and the Code, for the reasons already set out at §§171-182 above. It describes:

(1) the nature of the offences which may lead to intelligence being obtained and the persons whose communications may be obtained. Those matters are implicit within the statutory description of the purposes of which intelligence may be obtained: see §§171-175 above;
(2) the limits on the duration of such obtaining (since a RIPA warrant will be in place, save in exceptional circumstances, and such a warrant has clear limits on duration);
(3) the process for examining, using and storing data (since parallel safeguards to those under RIPA apply); and
(4) the circumstances in which the material may be erased/destroyed (since the material is treated in the same way as comparable material obtained under RIPA).

[65] The Applicants assert that the Disclosure and Code show that the Government has *"no difficulty distinguishing [intercept] from other material the UK Intelligence Services receive"*. That assertion ignores the fact that the Disclosure/Code apply to intercepted material that is either requested, or which identifies itself as the product of interception. For obvious reasons, the Intelligence Services may well receive other intercept material which does not identify itself as the product of interception.

The Applicants' further contentions concerning the Intelligence Sharing Regime

190. The Applicants contend that the Disclosure is insufficient as a safeguard, is "*obscurely drafted and vague*" and does not amount to "*law*". They also say that there should be "*prior independent authorisation*" or a requirement for "*reasonable suspicion*" before intelligence is shared (contentions that they also make with regard to the s.8(4) Regime). Finally, the BBW Applicants say that even if the Intelligence Sharing Regime was in accordance with the law as a result of the Disclosure/Code, it was not in accordance with the law at the time of their application. None of those arguments is sustainable.

191. As to the **first** argument, the Code itself mirrors the Disclosure. The Code is "*law*" for the purposes of the in accordance with the law test: see e.g. *Kennedy*. (Moreover, the Disclosure is also "*law*" for these purposes: it is a published statement, contained in publicly accessible court judgments).

192. There is no merit in the criticism that the Disclosure or Code are *"obscurely drafted"* or *"vague"* for any of the reasons asserted by the Applicants:

(1) It is entirely clear from the Disclosure/Code that the terms "*request*" and "*receipt*" would together cover all the scenarios where the relevant Intelligence Services may access foreign intercept. That would include access to databases. This alleged "*obscurity*" was not raised by 10 HR in the Liberty proceedings: no doubt, because it was not one that realistically arose.
(2) The concepts of "*analysed*" and "*unanalysed*" are also sufficiently clear. They are ordinary English words, which require no further definition. Material which has been automatically scanned and selected, but which has not been examined, is "*unanalysed*"; and material which has been examined, and conclusions drawn about it in the form of a report or analysis, is "*analysed*".
(3) It is wrong to suggest that there is no protection for communications data. As set out at §12.6 of the Code, where communications content or communications data (and whether or not the data is associated with the content of communications) are obtained in circumstances where the material identifies itself as the product of an interception, it must be subject to the same internal rules and safeguards that apply to the same categories of content or data when they are obtained directly by the intercepting agencies as a result of interception under RIPA.

193. As to the **second** argument, neither "prior independent authorisation" nor a requirement for "*reasonable suspicion*" are requirements of the s.8(4) Regime, for reasons set out above at §§73-78 and 89-95 above. So *a fortiori,* they cannot be requirements of the Intelligence Sharing Regime. In any event, there could be no sensible application of "*reasonable suspicion*" or "*prior authorisation*" requirements to circumstances where the Intelligence Services received unsolicited intercept material from a foreign state.

194. As to the **third** argument, the Court does not ignore developments since the lodging of an application in its assessment of the merits of a case; indeed, the BBW Applicants have themselves lodged further updated submissions after their original Application, on the premise that the Court should take further developments into account. The question whether an applicant is a victim of a violation of the Convention is relevant at all stages of the proceedings under the Convention: see e.g. *X v Austria*, app. 5575/72, 8 July 75, D.R.1 p. 45, *HE v Austria* (app. 10668/83), 13 May 1987, *Burdov v Russia* app. 59498/00 at §30. The Applicants' challenge is to the Intelligence Sharing Regime itself, not to particular past acts carried out under that regime. If

the Intelligence Sharing Regime is now in accordance with the law, the Applicants can no longer claim to be victims of it.

Question 5: Has there been an interference with the Applicants' rights under Article 10(1) on account of the operation of either regime, and if so, was it prescribed by law and necessary within Article 10(2)? In particular, having regard to the risk of intercepting journalists' sources, what safeguards are necessary to ensure that these regimes are compatible with Article 10?

The s.8(4) Regime

195. There are two respects in which it is necessary to consider whether the analysis under Article 10 differs from that under Article 8, as a result of the fact that the s.8(4) Regime may entail the interception, and potentially the subsequent selection for examination or examination, of confidential journalistic material.

196. **First**, the Applicants contend that Article 10 requires prior judicial authorisation before any confidential journalistic material can be intercepted, let alone searched. Indeed, this is the only respect in which they have contended in their Applications that the analysis under Article 10 is any different from the analysis under Article 8.

197. However, there is no authority in the Court's case law[66] for the proposition that prior judicial (or independent) authorisation is required for the operation of a strategic monitoring regime such as the s.8(4) Regime, by virtue of the fact that some journalistic (or NGO) material may be intercepted in the course of that regime's operation. On the contrary, the Court has drawn a sharp distinction between the strategic monitoring of communications and/or communications data, which may inadvertently "sweep up" some journalistic material; and measures that target journalistic material, particularly for the purposes of identifying sources, where prior independent authorisation will be required. See *Weber* at §151, and contrast *Sanoma Uitgevers BV v The Netherlands* app. no. 38224/03, 14 September 2010, and *Telegraaf Media v The Netherlands*.

198. The First Section followed that line of case law when it found no need for prior judicial authorisation under the s.8(4) Regime in the context of Article 10. See §492 of its Judgment:

> *"…the surveillance measures under the section 8(4) regime – like those under the G10 Act which were considered in Weber and Saravia – are not aimed at monitoring journalists or uncovering journalistic sources. Generally the authorities would only know when examining the intercepted communications if a journalist's communications had been intercepted. Consequently, [the Court] confirms that the interception of such communications could not, by itself, be characterised as a particularly serious interference with freedom of expression (Weber and Saravia, cited above, §151)."*

199. The First Section's finding reflects the IPT's own observation in the Liberty proceedings that a requirement of prior authorisation specifically for Article 10 purposes would be nugatory in this context. See the 5 December judgment[67] at §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)*

[66] Or the UK's domestic case law for that matter.
[67] See **CB/14**

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."

200. Those observations are correct. A requirement of prior judicial authorisation in respect of journalistic or NGO material under a regime of strategic (non-targeted) monitoring such as the s.8(4) Regime would simply make no sense. All that a Judge could be told is that there was a possibility that the execution of the warrant might result in the interception of some confidential journalistic/NGO material (along with other categories of confidential material). In the event that any such material was selected for examination the relevant provisions of the Code would apply.

201. The **second** issue is whether Article 10 requires special protection to be afforded to confidential journalistic communications at the point of their selection for examination. The First Section concluded that the Code gave inadequate protection to such communications, because although it contained provisions requiring consideration to be given to the interception of communications involving confidential journalistic material, such provisions *"appear to relate solely to the decision to issue an interception warrant"*: see Judgment, §493. So although such arrangements *"might provide adequate safeguards in respect of a targeted warrant under section 8(1) of RIPA, they do not appear to have any meaning in relation to a bulk interception regime"*.

202. The UK accordingly accepts that it would be appropriate for the Code to contain protective provisions, specifically designed for a bulk interception regime, governing the selection for examination of confidential journalistic material. Indeed, it has acted responsibly so as to ensure that such provisions are now contained in the new Interception of Communications Code under the Investigatory Powers Act 2016[68].

203. To that extent only, the UK accepts that the provisions of the s.8(4) Regime do not provide sufficient public protection for Article 10 rights, and are therefore not prescribed by law. (For the avoidance of doubt, the UK does not accept that there were in fact insufficient "below the waterline" protections governing confidential journalistic material at the relevant time; but it does accept that, any such protections not being public, the regime was insufficiently foreseeable in the premises and for the reasons set out in the First Section's judgment).

The Intelligence Sharing Regime

204. No separate Article 10 issue arises *at all* in relation to the Intelligence Sharing Regime, for the reasons given by the First Section, viz: (i) the BBW Applicants did not complain about breach of Article 10 in respect of confidential journalistic material in the first place; (ii) the 10 HR Applicants did not exhaust domestic remedies in relation to any complaint about the special

[68] The Interception of Communications Code for the purposes of the 2016 Act now provides at §9.41:
"Particular consideration should be given to the interception of communications or the selection for examination of content containing information where individuals might reasonably assume a high degree of confidentiality. This includes where the communications contain information that is legally privileged (see paragraphs 9.48 to 9.73); confidential journalistic material or where communications identify a journalist's source (see paragraphs 9.74-9.88)…" (Emphasis added).
§§9.74-9.88 contain detailed provisions which govern the selection for examination (and therefore, the examination) of material where the purpose of selecting material is to determine the source of journalistic information or to obtain confidential journalistic material.

protection afforded to journalists under Article 10 – see §§471-473 of the First Section's judgment; and (ii) the BIJ Applicants have not complained about the Intelligence Sharing Regime, but only about the s.8(4) Regime and the Chapter II Regime: see §476 of the First Section's judgment.

205. If any separate Article 10 issue had arisen concerning the Intelligence Sharing Regime, the answer to that issue would be exactly the same as the answer given above in relation to the s.8(4) Regime.

206. That follows from Chapter 12 of the Code:

(1) As regards obtaining communications in the first place, Chapter 12 of the Code provides that communications will only be obtained if either (i) a RIPA warrant is in place; or (ii) making the request in the absence of a RIPA warrant (which has never occurred) does not amount to an attempt to circumvent RIPA. It follows that the provisions of §§4.1-4.8 of the Code, requiring special consideration to be given to the interception of communications involving confidential journalistic material, apply either directly or by analogy.
(2) As regards the treatment of communications once obtained, including their selection for examination, relevant intercept material received from a foreign state is treated in exactly the same way under Chapter 12 of the Code as the same categories of material obtained as a result of the UK's own interception capabilities. So once foreign intercept material is in the hands of the Intelligence Services, exactly the same provisions apply to its selection for examination, as apply to communications intercepted under the s.8(4) Regime.

IV. CONCLUSION

207. In these circumstances, the Government invites the Court to declare that:

(1) The Applicants can properly claim to be victims of the s.8(4) Regime for the purposes of Article 8(1) ECHR. However, any meaningful interference with their Article 8 rights would occur only if their communications/RCD were selected for examination or examined.
(2) The s.8(4) Regime is in accordance with the law for the purposes of Article 8(2) ECHR, save in the respect set out at §149 above, concerning the searching of RCD by reference to factors referable to individuals known to be in the British Islands. The UK is acting so as to remedy this deficiency in the regime going forward.
(3) The s.8(4) Regime is prescribed by law for the purposes of Article 10 ECHR, save in the respect identified at §§201-203 above, concerning the selection for examination of confidential journalistic material. The UK has acted so as to remedy this deficiency in the regime going forward.
(4) The Applicants' rights under Article 8(1) and/or Article 10(1) have not been breached by the operation of the Intelligence Sharing Regime.

2nd May 2019

Chanaka Wickremasinghe

(Agent of the Government

of the United Kingdom)

Glossary

The 10 HR Applicants	The 10 Human Rights Organisations bringing application number 24960/15
The Anderson Report	A report of June 2015 by the Investigatory Powers Review, conducted by David Anderson QC, entitled "A Question of Trust"
The BBW Applicants	Big Brother Watch, Open Rights Group, English Pen and Dr Constanze Kurz
The BIJ Applicants	The Bureau of Investigative Journalism and Alice Ross
The British Islands	The UK, the Channel Islands and the Isle of Man (see s. 5 of and Sch. 1 to the Interpretation Act 1978)
The Bulk Powers Review	A report of August 2016 by the Independent Reviewer of Terrorism Legislation (David Anderson QC), entitled "Report of the Bulk Powers Review".
The Chapter II Regime	The regime governing the acquisition of retained communications data by public authorities, contained in Chapter II of Part I of RIPA.
The CJEU	Court of Justice of the European Union
The Code	The Interception of Communications Code of Practice, issued on 15 January 2016 under s. 71 of RIPA. The Code has now been replaced by an Interception of Communications Code of Practice issued under Sch. 7 of the Investigatory Powers Act 2016. However, references in the Submissions are to the previous version of the Code.
The Commissioner	The Interception of Communications Commissioner, appointed under s. 57(1) RIPA. The Interception of Communications Commissioner has now been replaced by the Investigatory Powers Commissioner. The last Interception of Communications Commissioner was Sir Stanley Burnton, a former High Court Judge (and previously, Sir Peter May, a former Lord Justice of Appeal).
Communications data	Certain data, as per the definition in ss. 21(4), 21(6) and 21(7) of RIPA, that relates to a communication

	but does not include its contents
CSP	Communications Service Provider
The CTA	The Counter-Terrorism Act 2008
The DPA	The Data Protection Act 1998
The Disclosure	The disclosure of certain internal safeguards within the Intelligence Sharing and s.8(4) Regimes, given by the respondents in the Liberty proceedings, and recorded by the IPT in its 5 December and 6 February Judgments.
DRIPA	Data Retention and Investigatory Powers Act 2014
External communication	A communication "sent or received outside the British islands" (see s. 20 of RIPA, and §6.1 of the Code)
FISA	The USA's Foreign Intelligence Surveillance Act 1978
FISC	Foreign Intelligence Surveillance Court, charged with overseeing activities of the US intelligence agencies under FISA
GCHQ	The Government Communications Headquarters
The HRA	The Human Rights Act 1998
The Intelligence Services	As per the definition in s. 81(1) of RIPA: the Security Service, SIS and GCHQ
The Intelligence Sharing Regime	The regime (set out in "Domestic Law and Practice") that governs the sharing of intelligence between the Intelligence Services and foreign intelligence agencies, and the handling and use of intelligence obtained as a result, in the context of the allegations made by the Applicants (i.e. allegations about the receipt of intelligence from the Prism and Upstream programmes)
Intercepted material	In relation to an interception warrant, "the contents of any communications intercepted by an interception to which the warrant relates" (see s. 20 of RIPA)
An interception warrant	A warrant issued in accordance with s. 5 of RIPA
The IPT	The Investigatory Powers Tribunal

The IPT Rules	The Investigatory Powers Tribunal Rules 2000, SI 2000/2665
The ISA	The Intelligence Services Act 1994
The ISC	The Intelligence and Security Committee of Parliament
The ISC Report	A report of 17 March 2015 by the ISC, "Privacy and Security: a Modern and Transparent Legal Framework"
The ISC's Statement of 17 July 2013	A statement made by the ISC following an investigation into the arrangements GCHQ has with its overseas counterparts for sharing intelligence, in light of allegations in the media that GCHQ had circumvented UK law by accessing information obtained by the NSA via Prism.
The Liberty proceedings	Proceedings in the IPT brought in 2013 by Liberty, Privacy, Amnesty International and various other civil liberties organisations, challenging the Intelligence Sharing and s.8(4) Regimes, in the same factual premises as are relevant to the present application
The NSA	The National Security Agency
The NSC	The National Security Council
The OSA	The Official Secrets Act 198
PCLOB	Privacy and Civil Liberties Oversight Board, an independent bipartisan agency within the US government's executive branch, charged with ensuring that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties
PCLOB's 2 July Report	A report of 2 July 2014 of PCLOB, "Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act"
The Privacy 2 Judgment	A judgment of the IPT dated 8 September 2017, concerning powers of GCHQ to obtain and handle bulk data
RCD	Related Communications Data within the meaning of s.20 of RIPA, i.e. communications data obtained by,

	or in connection with, the interception, and which relates to the communication or to the sender or recipient, or intended recipient, of the communication.
RIPA	The Regulation of Investigatory Powers Act 2000
A s. 8(1) warrant	An interception warrant that complies with s. 8(2)-(3) of RIPA
The s. 8(4) Regime	The statutory regime (set out in "Domestic Law and Practice" in the Government's Observations in the respective applications) that governs the interception of external communications and the handling and use of the intercepted material and communications data obtained as a result
A s. 8(4) warrant	An interception warrant issued under the s. 8(4) regime that complies with ss. 8(4)-(6) of RIPA
The s.16 arrangements	The safeguards applying under s.16 RIPA to the examination of intercepted material gathered under a s. 8(4) warrant
The Section 215 Programme	A US programme, conducted under the authority of s.215 of the US Patriot Act, involving the collection of telephone metadata in bulk, terminated in November 2015. The programme was unconnected with Prism and Upstream, and was conducted under different legal authority
SIS	The Secret Intelligence Service
The SSA	The Security Service Act 1989