Application No. 24960/15

IN THE EUROPEAN COURT OF HUMAN RIGHTS

BETWEEN:

10 HUMAN RIGHTS ORGANISATIONS

Applicants

-and-

THE UNITED KINGDOM

Respondent

FURTHER OBSERVATIONS OF THE GOVERNMENT OF THE UNITED KINGDOM

I Introduction

1. By way of a letter dated 11 October 2016, enclosing the Applicants' further observations and claims for just satisfaction, the Court invited the Government's response to the claims for just satisfaction and any other observations the Government wish to make.

2. These further observations are submitted in response to that invitation by the Court. They also contain the Government's response to the Third Party interventions that have made in this case[1].

3. The Government has already submitted detailed Observations on Admissibility and the Merits addressing the Intelligence Sharing and s.8(4) regimes (referred to hereinafter as "the Observations"), and responding to the specific questions posed by the Court. The Government adopts, but does not repeat, those Observations and has sought to confine these further Observations to new points of substance which have

[1] Three such interventions have been made by Third Parties: (1) The European Network of National Human Rights Institutions ("ENNHRI"); (2) The Electronic Privacy Information Center and (3) Article 19.

been raised by the Applicants or the Intervenors. Where the substance of the interventions is already addressed in the Government's Observations, the Government cross-refers to the relevant paragraphs of the Observations, rather than repeating their substance. The Government uses the same terminology in this Response as is used in the glossary to its Observations.

I. RESPONSE TO 10 HUMAN RIGHTS FURTHER OBSERVATIONS

4. In common with the way in which the Applicant's have structured their further observations, the Government proposes to address the factual assertions which are now made about the two regimes (Part 1), before making a number of legal submissions in response to the Applicants' further observations (Part 2).

THE FACTS

The section 8(4) Regime – general observations

5. Although the Applicants have correctly moved away from characterising the s.8(4) regime as one of "mass surveillance", they nevertheless seek to portray it as a regime in which the totality of communications across entire networks are the subject of substantive and meaningful invasions of privacy in an arbitrary and disproportionate manner[2].

6. But that is to mis-characterise and over-simplify the process and ignores the surgical precision with which GCHQ does (and is legally obliged to) interrogate bulk data pursuant to its statutory powers.

7. Whilst the Security and Intelligence Agencies (SIAs) do intercept the entire contents of a bearer or bearers under the s.8(4) Regime, they only examine a tiny proportion of communications or communications data from those contents, having chosen to examine them, on the basis of statutory tests of purpose, and requirements of necessity and proportionality. This is focused intelligence gathering. Without this

[2] See, in particular §35-37 and 42-46 of the Applicants' further observations.

capability, much vital intelligence would not be available to the UK for legitimate public protection purposes.

8. As explained in detail in the Observations, the s.8(4) Regime operates in this way as a matter of practical necessity. For technical reasons, it is necessary to intercept the entire contents of a bearer, in order to extract even a single specific communication for examination from the bearer: Observations, §§1.31-1.34.

9. Such an act of interception is characterised by the Court as involving an interference with Article 8(1) ECHR. But in truth, it cannot involve a substantial invasion of individuals' privacy rights unless that communication is selected for examination: in other words, unless a human examines it, or may potentially examine it. The analysis of Article 8 rights must focus upon the stage at which a communication is selected for examination; not simply upon the act of interception in itself. If the analysis fails to do this, it will fail to grapple with the true nature of the s.8(4) Regime, how it works, and what activities it permits. And the position is no different, just because communications passing over a bearer may be held temporarily (often for fractions of a second) while they are electronically filtered and subjected to search terms, to determine whether they are selected for such examination.

10. Thus, what ultimately matters for privacy rights is not the mere fact that data are subject to bulk interception. What matters is the adequacy of the safeguards that either allow or prevent such data from being examined. The Government has set out in detail in its Observations the reasons why those safeguards are well sufficient to secure individuals' Article 8 rights, by reason of the statutory framework in RIPA, the Code, the internal safeguards of the Intelligence Services, the application of tests of necessity and proportionality, and the oversight of the IPT, ISC and Commissioner.

11. A regime that operates on the basis of strict controls governing the selection of data for examination, which limits the statutory purposes for which those data can be selected for examination, and which applies tests of necessity and proportionality to such selection, cannot contravene Article 8 ECHR, merely because at the initial stage

a large amount of data is intercepted. Otherwise, the Court's judgment in *Weber and Saravia v Germany* (app. 54934/00) ("*Weber*"), which established the legal requirements governing the interception of communications in this field, would have been wrongly decided.

12. In short, it is illegitimate to suggest that bulk interception itself inevitably entails a breach of Article 8 ECHR.

The Bulk Powers Review

13. The Independent Terrorism Legislation Reviewer has produced further important factual evidence about the Intelligence Services' bulk interception practices pursuant to the s.8(4) Regime, and the intelligence need for such bulk interception. See the Report of the Bulk Powers Review (David Anderson QC), August 2016 ("the Bulk Powers Review").

14. The Bulk Powers Review evaluated the operational case for various intelligence gathering powers, in the context of the Investigatory Powers Bill (which received Royal Assent on 29 November 2016 as the Investigatory Powers Act, though most of the Act is not yet in force), which is intended to provide a new statutory framework for such powers. One of the powers considered in the Review was bulk interception, i.e. interception currently conducted under the s.8(4) Regime.

15. The Bulk Powers Review provides a helpful summary of the way in which bulk interception under the s.8(4) Regime works at §§2.13-2.18, which emphasises the important distinction between the initial interception and filtering of communications, and their selection for potential examination, set out above:

"2.14 Bulk interception involves three stages, which may be called ***collection, filtering*** *and* ***selection for examination****.*

First stage: collection
2.15 GCHQ selects which bearers to access based on an assessment of the likely intelligence value of the communications they are carrying. GCHQ does not have the capacity, or legal authority, to access every bearer in the world. Instead it focuses its resources on those links that it assesses will be the most valuable. At any given time, GCHQ has access to only a tiny fraction of all the bearers in the world.

Second stage: filtering

2.16 GCHQ's processing systems operate on the bearers which it has chosen to access. A degree of filtering is then applied to the traffic on these bearers, designed to select communications of potential intelligence value. As a result of this filtering stage, the processing systems automatically discard a significant proportion of the communications on the targeted bearers.

Third stage: selection for examination

2.17 The remaining communications are then subjected to the application of queries, both simple and complex, to draw out communications of intelligence value. Examples of a simple query are searches against a "strong selector" such as a telephone number or email address. Complex queries combine a number of criteria, which may include weaker selectors but which in combination aim to reduce the odds of a false positive. Communications that do not match the chosen criteria are automatically discarded. The retained communications are available to analysts for possible examination.

2.18 The application of these queries may still leave too many items for analysts to examine, so GCHQ must then carry out a triage process to determine which will be of most use. The triage process means that the vast majority of all the items collected are never looked at by analysts…"

16. At §§2.19, the Review summarises the two major processes that GCHQ applies to bulk interception (i.e. the "strong selector" process and "complex query" process), observing that (i) the "strong selector" process is in effect a "targeted" process, not a "bulk" process at all, because the selectors used relate to individual targets; and (ii) the "complex query" process permits methods of analysis and selection not available with the "strong selector" process, but in no way permits staff to search through communications *"at will"*. It is *"closer to true bulk interception, since it involves the collection of unselected content and/or secondary data"*. But "*as with the [strong selector process], it remains the case that communications unlikely to be of intelligence value are discarded as soon as that becomes apparent"*.

17. At §2.20, David Anderson QC observes that he has "no reason to disagree" with the ISC's assessment that the s.8(4) Regime does not collect communications indiscriminately, and that *"only the communications of suspected criminals or national security targets are deliberately selected for examination"*.

18. Chapter 5 of the Bulk Powers Review assesses the utility of bulk interception, as carried out by GCHQ under the s.8(4) Regime. That assessment was undertaken on the basis of an intensive review of closed evidence: see §5.2:

"Cathryn McGahey QC and I have inspected a great deal of closed material concerning the value of bulk interception, including warrant renewal applications (which contain details of the use to which intelligence derived from bulk interception had been put) and explanations produced for the benefit of the ISC and the Review."

19. Points made in Chapter 5 include the following:

(1) Just under half of all GCHQ intelligence reporting is based on data obtained under bulk interception warrants. For counter-terrorism intelligence reporting, this figure rises to over half: §5.9.

(2) Targeted interception cannot be viewed as a generally viable substitute for bulk interception. Even where a "strong selector" is known (e.g. a telephone number or email address), it may in an overseas context very often be necessary to intercept in bulk in order to obtain information from that selector. A targeted warrant would very often not produce the same result. See §§5.24-5.33:

(i) The location of some targets may mean that targeted interception would not be practicable (e.g. the target in Syria).

(ii) Even in more favourable overseas locations, the cooperation of local CSPs in giving effect to a targeted warrant might not be forthcoming, or might be possible only after delays.

(iii) The fragmentary nature of global communications, involving the division of communications into packets, means that a targeted warrant would not, or would not necessarily, capture all the information that GCHQ needs.

(iv) The number of overseas targets could render such a regime prohibitively cumbersome.

(v) "Contact chaining"[3] on the basis of targeted interception is a valuable technique, but has limitations. It is dependent upon the Intelligence Agencies already knowing their initial subject of interest; new subjects of interest being in contact with the initial subject; and it being possible to serve a targeted interception warrant on new subjects. Those conditions will not always be satisfied, particularly where subjects of interest are overseas. Moreover, "contact chaining" may very well not work where

[3] That is, identifying terrorist connections through interrogation of data obtained through targeted means, in order to find additional contacts who use the same form of communication.

extremists use a variety of different communications methods in an effort to conceal their activities: §§5.28-5.33.

(3) Bulk acquisition of communications data may in some circumstances be an adequate alternative to bulk interception: but it would not be noticeably less intrusive and would have a disadvantage in terms of speed (and the need for cooperation from CSPs): §5.34.

(4) Similarly, human sources of intelligence may be unavailable, and the obvious dangers to human sources must be taken into account: §5.35.

(5) Thus, in sum, no alternative source of intelligence, or combination of alternatives, would be sufficient to substitute for a bulk interception power: §5.41.

20. In the conclusion to Chapter 5 of the Bulk Powers Review, David Anderson QC revisited the conclusion he reached in the Anderson Report concerning the utility of bulk interception (see Observations, §1.35), and stated:

"5.53 This Review has given me the opportunity to revisit my earlier conclusion 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."

21. 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. 4 of those case studies were summarised (albeit in slightly less detail) in the Anderson Report, as to which see Observations, §1.36. 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. Analysis of the content of communications obtained through bulk interception indicated that the hostages' lives were in danger. The hostages were successfully 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. GCHQ did this by looking for traces of the malware within bulk data. Further analysis of the bulk data identified the infrastructure being used by the criminals to deploy and control the malware. The information obtained by GCHQ eventually led to the arrest of the gang. This is by no means an isolated: GCHQ currently 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.

Response to Applicants' factual allegations about the s.8(4) regime: §§26-32, 35-47

22. At §§26-30 of the Applicants' Further Observations, the Applicants have sought to define the terms "bulk" and "targeted", such that anything which is "bulk" is effectively indiscriminate and is to be contrasted with a "targeted" capability which is based on "*reasonable suspicion that a specific target*" has committed or is likely to commit a criminal offence or is a threat to national security. But that distinction is unhelpful and unjustified in the present context:

    a. To the extent that it implies that, as part of bulk interception, GCHQ in fact accesses communications about a wide range of people who are of no legitimate interest to the security and intelligence agencies, that is wrong. As made clear by David Anderson QC in the Bulk Powers Review, the s.8(4) regime does not permit interference with communications indiscriminately and only the communications of suspected criminals or national security targets are deliberately selected for examination.

    b. This over-simplistic distinction ignores the incremental collection, filtering and selection process which in fact takes place as set out at §§15-16 above. That careful process incorporates significant safeguards at each stage and

ensures that these activities are necessary and proportionate. Thus, whilst there may be "bulk" collection at the first stage, there is then a sequence of stages applied which ensures that the fragments of intelligence which are actually analysed and pieced together at the end of the process are appropriately targeted at those who in fact pose a threat to the UK i.e. individuals who are of legitimate intelligence interest, regardless of whether they had previously been identified as a threat by the SIAs.

c. Allied to that, it is wrong to suggest that selection other than by reference to a previously identified individual must mean that the interception is untargeted and indiscriminate. Even when there is selection at the third stage on the "complex query" basis i.e. by inputting a number of criteria to narrow down the information which is analysed, that does not mean that communications are available for GCHQ analysts to search through at will. As explained in the Bulk Powers Review, the filtering and complex search process draws out the communications of intelligence value and therefore the odds of a 'false positive' are considerably reduced (see §2.21 of that report at p25). Whilst "complex query" process is closer to true bulk interception (since it involves the collection of unselected content and/or secondary data) it would be wrong to categorise that as indiscriminate since that activity must still satisfy the statutory tests of purpose, together with necessity and proportionality, in order to be lawful. As stated by the Commissioner at §6.5.40 of his 2013 Report[4]:

"What remains after filtering (if anything) will be material which is strongly likely to include individual communications which may properly and lawfully be examined under the section 8(4) process. Examination is then effected by search criteria constructed to comply with the section 8(4) process."

d. In addition, to the extent that it is suggested that activity can only be lawful for Art. 8 ECHR purposes in this context if it is based on "reasonable grounds for suspicion" that is not consistent with the established case law in this area, as discussed in more detail at §§90-97 below.

[4] See Annex 1

23. In terms of the different stages of the bulk interception process, the three stages outlined in the Bulk Powers Review (see §15 above) set this out authoritatively and accurately and are to be preferred, in contrast to the suggested six stages at §31 of the Applicants' further observations. For example, "Initial interception" and "Extraction" are, in fact, one single process i.e. the information is initially obtained by copying it. Stage 4 is a necessary part of any analysis at Stage 3 and therefore both stages are more accurately described under the rubric of "selection for examination" (see §2.17 of the Bulk Powers Review). In addition Stage 6, i.e. any distribution of the results of analysis to other persons or agencies, is outside the scope of the current application and is subject to separate safeguards and controls.

24. Whilst it is right that s.8(4) sets no upper limit on the number of communications that may be intercepted, it does not follow that, even in principle, a single warrant could "*encompass the communications of an entire city in the UK with the residents of another country*" (see Applicants' further observations at §§35-37). That could never be necessary or proportionate (applying the safeguards set out at §§2.69-2.81 of the Observations). It is also fanciful to suggest that this could occur in practice since this could only possibly occur if all such communications were carried on a single telecommunications system and, in practice, there is extraordinary diversity in the supply of communications technologies to consumers.

25. GCHQ does not seek to contend that the limitations on its resources constitute a permissible legal safeguard in this context (contrary to the suggestion at §§38-40 of the Applicants' further observations). As made clear by the ISC it is <u>both</u> for legal reasons and due to resource constraints that GCHQ cannot conduct blanket indiscriminate interception of all communications and most importantly "*it would be unlawful for them to do so, since it would not be necessary and proportionate, as required by RIPA* (see §58 of the ISC Report set out at §1.23 of the Observations).

26. There is also no inconsistency in the Government's description of GCHQ's operations (see §41 of the Applicants' further observations). Whilst it is right that electronic communications do not traverse the internet by routes which can

necessarily be predicted, that does not mean that the first stage of the process (i.e. collection) is or could lawfully be, indiscriminate or wholly untargeted. For example, there may be a very real difference (in terms of necessity and proportionality) between identifying a bearer which carries a high proportion of e-mail traffic flowing out of Syria from one which carries e.g. You Tube videos between states which are unlikely to be of intelligence interest. Accordingly it is an unfair characterisation of the process to suggest that the first stage of the process involves access to "*an enormous amount of data relating to the lives of private individuals around the world, the vast majority of whom are not and never will be of intelligence interest to UK intelligence services*" (see §41 of the Applicants' further observations). That first stage does involve an element of selection and that is just the beginning of a process which narrows down what is actually analysed to that which is strongly likely to include communications of legitimate interest to the SIAs. The Applicants' submissions effectively boil down to a proposition that it could never be Art. 8 ECHR compliant to intercept in bulk prior to selecting for examination. But that is clearly contrary to this Court's approach in *Weber*.

27. In addition and as discussed above, it is wrong to suggest that GCHQ analysts can store and "*trawl*" through a "*large pool of information...by reference to unknown selectors that may bear little or no resemblance to criminal investigations or operations*" (see Applicants' further observations at §42). Whilst it is not understood what is meant by "unknown selectors" in this context (given that GCHQ cannot be expected to make public the selectors it uses), if this is meant to be a description of the "complex query" process at the selection stage (see §2.21 of the Bulk Powers Review), then the characterisation of that process is wholly inaccurate. These searches are designed to draw out communications of intelligence value and other communications which are not of intelligence interest are discarded. That was the clear conclusion of the ISC and Mr Anderson QC (including in the Bulk Powers Review) i.e. oversight bodies who have direct experience of the process in practice.

28. It follows that the example which is given at §§44-46 of the Applicants' further observations, namely that bulk interception could result in "*everyone's reading activities*" being "*automatically intercepted, stored and made available for analysis*" is

utterly far-fetched. Whilst, in principle, a selector could be used to identify everyone who had downloaded a particular book or article from the internet, there are safeguards in place which ensure that any selector is justified on necessity and proportionality grounds and technical measures are also in place (by way of a triage process) to ensure that a selector which produces too many items for examination is refined before the results can be looked at by an analyst. The sophistication of the selection process ensures that the system is more proportionate, not more intrusive, contrary to the impression given in the Applicants' submissions.

29. It is also misleading to suggest that "*the dragnet of bulk intercept includes routine and automated storage and analysis of the communications of human rights activists*" (§47 of the Applicants' further observations). That could never be necessary or proportionate and was contrary to the express findings of the IPT in its Third Judgment (dated 22 June 2015) in which it made clear that GCHQ had lawfully and proportionately intercepted and selected for examination communications of the two Applicants (as explained in detail at §§4.102-4.103 of the Observations).

Is the Government constrained by NCND in this context? (§§48-52)

30. At §§48-52 of the Applicants' further observations it is said that the Government is not constrained from responding more fully to the factual allegations which have been made about its bulk interception activities and is seeking to hide behind a "self-imposed" policy of Neither Confirm Nor Deny (NCND). It is also suggested that the NCND principle has been called into question by the domestic courts.

31. This ignores the fact that the NCND principle was accepted in *Kennedy v United Kingdom*[5] as a valid basis on which information could be withheld (see §187) and was also recognised in *Klass* at §58, *Weber* at §135 and *Segerstedt-Wiberg v Sweden*, judgment 6 June 2006 at §102. It remains an important mechanism through which the state discharges its positive obligations (including under Arts. 2 and 3 ECHR) to protect information which, if disclosed, would be harmful to the public interest. Most recently in the domestic setting the principle was reviewed by Lord Justice

[5] App. 26839/05, 18 May 2010

Pitchford in the context of the 'Undercover Policing Inquiry'[6] who considered evidence from a Senior Cabinet Office National Security Adviser. There was no suggestion in that careful review of the application of the principle that it was unimportant or capriciously applied (see, in particular, §§116, 127, 145-146 of that Ruling).

'New' facts: §§53-55

32. In terms of the 'new facts' referred to at §§53-55 of the Applicants' further observations (and addressed at §§4-9 of the Applicants' Factual Appendix) these are neither confirmed nor denied. As discussed above, it has been a principle of successive UK Governments neither to confirm nor deny ("NCND") assertions, allegations or speculations in relation to the Intelligence Services, whose work requires secrecy if it is to be effective.

33. In any event, as appears to be acknowledged by the Applicants at §55 of their further observations, these allegations are irrelevant to the issues which have been raised in these applications.

Intrusiveness of interception content and communications data: §§56

34. As explained at §§4.29-4.31 of the Observations, the Court has correctly recognised in *Malone v UK* (app. 8691/79, Series A no.82) that it is less intrusive in Article 8 terms to obtain communications data than the content of those communications. That remains the same even in relation to internet-based communications. The aggregation of 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 item. However, it remains the case that, if like is compared with like, the interception of communications raises greater privacy concerns. For example, the content of 50 communications is very likely to be more intrusive in

[6]Annex 2. Restriction Orders: Legal Principles and Approach Ruling 3 May 2016:

Article 8 terms than the communications data associated with those 50 communications.

The Intelligence Sharing Regime: §§33-34, 62-77, 226-231

35. In their further observations the Applicants make wide-ranging submissions about the nature of US surveillance law. It is unnecessary and inappropriate for the Court to make findings about that law in this Application.

36. The Applicants' further observations also address alleged US surveillance activities outside the scope of this Application. The Application is about the UK's alleged receipt of information from the USA's Prism and Upstream programmes[7], which the NSA operates under the authority of s.702 FISA. The Applicants address the NSA's surveillance activities under a completely different authority (Executive Order, "EO" 12333) (see §§64-68 and §77 of the Applicants' further observations and see §§10-12 of the Applicants' Factual Appendix). It is unnecessary and inappropriate to address EO 12333.

37. In those circumstances, the Government makes the following key points in response to these aspects of the Applicants' further observations.

38. **First** insofar as the intelligence activities and operations of the US Government have been the subject of official statements and/or other express avowal by the executive branch of the US Government, the Government does not adopt the NCND principle in relation to them. But some caution should be exercised when considering allegations which have not been publicly avowed by the US Government. In that regard the Government wishes to draw to the Court's attention the Executive Summary of the Review of the Unauthorized Disclosures of Former National Security Agency Contractor Edward Snowden, published by the U.S. House of Representatives on 15 September 2016[8]. In this document the House Permanent

[7] See e.g. Applicants' Additional Submissions on the Facts and Complaints at §§5-8.

[8] Annex 3. Executive Summary of the Review of the Unauthorised Disclosures of Edward Snowden published on 15th September 2016

Select Committee on Intelligence finds that "*the public narrative popularized by Snowden and is allies is rife with falsehoods, exaggerations, and crucial omissions*" (p1). They also find that it is "*not clear Snowden understood the numerous privacy protections that govern the activities of the [U.S. Intelligence Community]. He failed basic annual training for NSA employees on Section 702 of the Foreign Intelligence Surveillance Act (FISA) and complained the training was rigged to be overly difficult. This training included explanations of the privacy protections related to the PRISM program that Snowden would later disclose*" (p3). The Committee concluded that Snowden "*was, and remains, a serial exaggerator and fabricator. A close review of Snowden's official employment records and submissions reveals a pattern of intentional lying*" (p3).

39. **Secondly** it is incorrect to suggest that Presidential Policy Directive 28 ('PPD-28') places no restrictions on the collection of signals intelligence in bulk (see §64 of the Applicants' further observations). PPD-28 requires that "[*s]ignals intelligence activities shall be as tailored as feasible*" and, as noted in the Letter from Robert Litt, General Counsel of the Office of the Director of National Intelligence dated 22 February 2016 ('the Litt Letter')[9] "*[t]his means, among other things, that, whenever practicable, signals intelligence collection activities are conducted in a targeted manner rather than in bulk*".

40. **Thirdly** it is wrong to characterise Upstream and Prism as "bulk" programmes, in direct contrast to programmes which are "targeted" (see §71 of the Applicants' further observations and §§13-19 of their Factual Appendix). As made clear by David Anderson QC in the Bulk Powers Review, although the powers under FISA s.702 do concern "bulk interception" the powers are focused and targeted and bear a strong resemblance to GCHQ's 'strong selector' process. That was made clear at §§3.56-3.65 of that Report, including in the following passages:

"***There are marked similarities between the s702 programme and bulk interception as practised in the UK, particularly via the "strong selector process"*** *summarised at 2.19(a) above:*

(a) Both are ***foreign-focused capabilities****, based on the interception of a cable and the collection of "wanted" communications* ***by the application of strong selectors.***

[9] at 4-6 (Annex VI to the Privacy Shield documents) (http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf).

(b) The application of those selectors from a very early stage ***gives both the flavour of targeted capabilities****, though as explained at 2.19(a) above, the holding of communications in bulk for a short period means that a bulk warrant will be required under the Bill.*

(c) Both offer the advantages of operational scale and flexibility to service the range of foreign intelligence missions.

(d) Even the authorisation regimes are similar, with external authorisation of the intelligence purposes for which the data can be accessed and used and the procedures for targeting and handling of information, but with decisions relating to individual selectors being delegated to GCHQ / NSA.

...

The s702 arrangements continue to permit the ***targeted selection*** *and retention by the NSA of wanted communications from bulk internet traffic, in very much the same way as the strong selector process described at 2.19(a) above.* (emphasis added)

41. In those circumstances, the Applicants are wrong to assert that David Anderson QC "endorsed" Upstream as a non-targeted capability in the Bulk Powers Review.

42. Collection under s.702 of FISA is based on specific and identified targets and it may not be carried out on an indiscriminate basis. It must comply with the Fourth Amendment to the US Constitution, statutory restrictions contained in s.702 itself, and Court-approved targeting procedures.

43. The activities under s. 702 must be targeted at specific selectors such as e-mail addresses or phone numbers. The Privacy and Civil Liberties Oversight Board (PCLOB) found that the US government must make targeting "*determinations (regarding location, U.S. person status, and foreign intelligence value) about the users of each selector on an individualized basis[;] it cannot simply assert that it is targeting a particular [ ] group*."[10] The PCLOB's report led to the European Commission's finding, in its adequacy decision assessing the EU-U.S. Privacy Shield Agreement, that acquisition pursuant to s. 702 is "*carried out in a targeted manner through the use of individual selectors that identify specific communications facilities, like the target's e-mail address or telephone number, but not key words or even the names of targeted individuals*."[11]

[10] PCLOB Report at 21.
[11] *See* Adequacy Decision at para. 81 (p. 22), *available at* http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf.

44. Collection activities under s. 702 are also limited to specific and defined intelligence priorities set by policy-makers.[12] These priorities include topics such as nuclear proliferation, counterterrorism, and counter-espionage.

45. "Upstream collection" involves the acquisition of communications as they transit the telecommunications "backbone" networks (including the Internet "backbone") of US telecommunications-service providers.[13] Tasked selectors are sent to providers operating these networks after the government applies its targeting procedures to each individual selector.[14] Upon receipt of the tasked selectors, the service providers must assist the Government in acquiring communications to, from, or otherwise containing these selectors while they transit the 'backbone.'[15] Communications are filtered for the purpose of eliminating wholly domestic communications, and then scanned to capture communications containing tasked selectors.[16] Communications that successfully pass both these filtering screens are then ingested into NSA databases.[17]

46. Before communications facilities may be targeted for intelligence collection, a written certification must be submitted to and approved by the FISA Court[18] which must include targeting procedures.[19] The targeting procedures ensure that collection takes place only as authorised by statute and within the scope of the certifications. Under these limitations, as the PCLOB concluded, collection "*consists entirely of targeting specific persons about whom an individualized determination has been made*."[20]

47. Collection is targeted through the use of individual selectors, such as email addresses or telephone numbers. To target these selectors, US intelligence personnel must

---

[12] *See* Letter from Robert Litt, General Counsel of the Office of the Director of National Intelligence, dated Feb. 22, 2016, at 4-6 (Annex VI to the Privacy Shield documents) (http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf) (Litt Letter), discussed below.
[13] *See* PCLOB Report at 35; PRG Report at 141 n.137.
[14] See PCLOB Report at 36.
[15] PCLOB Report at 35–37. *See also* Litt Letter.
[16] PCLOB Report at 37.
[17] *Ibid*.
[18] 50 U.S.C. §1881a (a) and (b) – the FISA Court is a US federal court established and authorized under the Foreign Intelligence Surveillance Act of 1978 (FISA).
[19] *See* 50 U.S.C. § 1881a (d).
[20] *See* PCLOB Report at 103.

determine, pursuant to targeting procedures approved by the FISA Court, that they are likely being used to communicate foreign intelligence information that falls within the categories covered by the certification submitted to the court.[21] The reasons for selecting a target must be documented[22].

48. The Department of Justice and ODNI (Office of the Director of National Intelligence) review the documentation for every selector to assess compliance with the requirements of the targeting procedures – i.e. that all three requirements are met: that the user is reasonably believed to be (i) a non-US person, (ii) located outside the US, and (iii) who there is a valid foreign intelligence reason for targeting.[23]

49. As part of its review of the certification, the FISA Court must assess the targeting and minimization procedures against the reasonableness requirements of the Fourth Amendment. While the targeting and minimization procedures are primarily concerned with the privacy of US persons, the targeting procedures require that before a non-US person's selector is targeted for s.702 acquisition, the US government must include a written explanation for each individual tasking decision. This tasking decision contains the basis for the government's determination that collection on the particular target will likely return foreign intelligence information relevant to the subject of one of the certifications approved by the FISA Court.[24]

50. Thus, the targeting procedures protect the privacy of non-US persons by ensuring that each individual targeting decision is based upon a sufficient nexus to the foreign intelligence information sought to be obtained by one of the FISC-approved certifications. Similarly, the written certification approved by the FISA Court must include minimization procedures. The minimization procedures for s.702 have been

[21] 50 U.S.C. §1801(e). For example, the US might target the user of a specific email address or telephone number based on credible information indicating that the email address or telephone number (a "selector") is believed to be used by a foreign terrorist operating overseas.
[22] For example, the government would specify how it was able to reasonably assess that the selector is used by a foreigner located outside the US and what foreign intelligence information (e.g., terrorism) the government expects to obtain from targeting the user of the selector.
[23] 50 U.S.C. §1881a(l); *see also* NSA Director of Civil Liberties and Privacy Report, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702* (hereinafter "NSA Report") at 4, available at http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.
[24] *See* PCLOB Recommendations Assessment Report, February 5, 2016, at 14-15.

publicly released.[25] These procedures focus on US persons but also provide important protections to non-US persons.

51. The US Intelligence Community must also comply with the privacy protections afforded to non-US persons by Presidential Policy Directive 28 (PPD-28) – see §§1.13-1.14 of the Observations (and see also the Litt Letter). This extends certain protections afforded to the personal information of US persons to non-US person information (and see further §141 below)[26].

52. In those circumstances, the programmes which are carried out under the authority of s.702 of FISA can properly be described as "targeted" and certainly do not involve the indiscriminate bulk collection of data.

53. **Finally**, in §69 of their further observations, the Applicants refer to media reports which describe Prism (collection under s.702 of FISA) as a programme under which the US was "*tapping directly into central servers*". However, as the Applicants concede in the Factual Appendix (see §19), that statement is inaccurate. An accurate description of how the programme operates can be found in the PCLOB Report dated July 2014 (see the Observations at §1.8).

LEGAL FRAMEWORK

The Applicants' summary of the legal framework §§82-126

54. The Government has set out in detail the legal framework which applies to the Intelligence Sharing and s.8(4) regimes at pp59-103 of the Observations. In terms of the Applicants' further observations on the current legal framework, the Government makes the following key submissions in response.

[25] The minimization procedures are available at http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf; http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf; and http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf.

[26] NSA's unclassified and publicly available PPD-28 procedures apply to all of NSA's signals intelligence activities, including activities undertaken under s.702 - *see, e.g.*, NSA PPD-28 Implementation Procedures, Section 7.2.

55. As regards the intelligence sharing regime:

    a. It is inaccurate to say (at §89 of the Applicants' further submissions), that when the Applicants initiated proceedings in the IPT there was "*no information in the public domain setting out the rules governing intelligence sharing between the UK Government and foreign intelligence agencies*". As set out at §§2.1-2.22 of the Observations that regime was set out in primary legislation.

    b. In terms of the Disclosure which was recorded in the IPT's 5 December and 6 February Judgments (see §93 of the Applicants' further observations), since it formed part of a judicial decision it can be taken into account in assessing "forseeability" for Art. 8(2) ECHR purposes – see the Observations at §2.23 and footnote 63. Therefore, prior to being incorporated into the Code, the domestic position was the same as a result of the 5 December 2014 and 6 February 2015 IPT judgments.

56. In terms of the oversight provided by the Investigatory Powers Tribunal (see §§96-100 of the Applicants' further observations):

    a. The IPT decision in *Human Rights Watch v Secretary of State for the Foreign and Commonwealth Office et al* [2016] UKIP Trib 15/165/CH, 16 May 2016, was a response to a worldwide campaign by Privacy International which encouraged individuals to bring claims in the IPT in order to find out "*if GCHQ illegally spied on you*". When addressing whether a sample of claimants had victim status to bring ECHR claims, the IPT applied the recent guidance in *Zakharov v Russia*, 4 December 2015, Application No. 47143/06[27]. That was

[27] The IPT concluded: "*We are satisfied that the appropriate test for us to operate, which would accord with Zakharov and our obligations under RIPA, is whether in respect of the asserted belief that any conduct falling within subsection s.68(5) of RIPA has been carried out by or on behalf of any of the Intelligence Services, there is any basis for such belief; such that the "individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or legislation permitting 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). This continues to be the low hurdle for a claimant that this Tribunal has traditionally operated*."

not an "abandoning" of the approach noted by this Court in *Kennedy*[28]; it was a legitimate application of the victim test at §171 of *Zakharov*. As the IPT itself noted in the final sentence of §46 of its judgment "*This continues to be the low hurdle for a claimant that this Tribunal has traditionally operated.*"

b. There is nothing improper, as a matter of principle, in the IPT receiving briefings from the SIAs as part of their work. The IPT is a specialist tribunal and the nature of its casework means that it is necessary for its members to have a level of background understanding regarding the agencies' practices and procedures. The meeting which occurred at Thames House on 28 September 2007 (as recorded in a Note for File dated 15 November 2007) was an entirely appropriate example of that and the suggestion that it somehow undermines the independence or effectiveness of the IPT is strongly resisted.

c. As is clear from a proper reading of the Note for File which recorded that meeting:

    i. The purpose of the visit was a "general briefing", including about MI5's data handling techniques and the growth and changes to MI5 and the scale of the threat that it was facing.

    ii. As part of the data handling presentation MI5 indicated that, for the purposes of IPT proceedings, it would not routinely conduct searches of "reference data-bases" i.e. databases containing information about the population generally (e.g. the Voter's Roll or telephone directories), for any mention of a complainant's name and such searches would only be carried out if the data was "*relevant or had been relied on in the course of an investigation*" (see Annex C to the Note for File).

    iii. That was an entirely sensible and proportionate suggestion, since the fact that a complainant's name was on e.g. a Voter roll which had

[28] See the Applicants' further observations at §97.

never been accessed by officers at MI5 could not conceivably be relevant to whether there had been unlawful conduct in relation to an individual.

iv. As made clear from the Note for File the meeting was an opportunity for MI5 to make clear what its standard position would be. It would be open to the IPT on a case by case basis and in response to any particular complaint to decide that such an approach should not be followed and to require more extensive searches as necessary[29].

> Indeed, that has very recently occurred in domestic proceedings in the IPT concerning the lawfulness of bulk personal datasets, where the IPT has ordered the Respondents to carry out searches of their databases (including their Bulk Personal Datasets and Bulk Communications Datasets)"[30]

d. In addition, it cannot sensibly be suggested that this meeting in any way undermines the independence or effectiveness of the IPT's examination of the s.8(4) or intelligence sharing regimes:

i. The complaints were not about the holding of bulk personal datasets i.e. "reference data-bases" which have been the subject of separate and more recent proceedings in the IPT[31]. They were about interception under the s.8(4) RIPA regime and intelligence sharing with the US. (Similarly, in these proceedings, there is no complaint about the use of bulk personal datasets, which are the subject of an entirely different legal regime and therefore wholly outwith the scope of the application.)

---

[29] That is consistent with the standard form of words which MI5 uses when responding to an IPT complaint which makes clear the position it has adopted as regards searches of reference data. That standard form of words is as follows: *""When checking our records in response to complaints to the IPT, we would not normally search reference databases containing information about the general population, eg the electoral roll, telephone directories etc, for a trace of the complainant's name. We would only do so if it appeared relevant to the complaint and/or the Tribunal specifically requested it. This was discussed and agreed with Tribunal members when they visited Thames House on 28 September 2007. In this case, we have not checked reference databases for any mention of Mr [name redacted]. If the Tribunal requires us to do so, please let us know*."

[30] IPT Bulk Data Directions Searches Order 12 December (Annex 8 attached)

[31] Annex 4. See the recent judgment of the IPT in *Privacy International v Secretary of State for Foreign and Commonwealth Affairs & Others* [2016] UKIPTrib 15_110-CH

ii. The meeting occurred six years before the Applicants brought claims in the IPT and only one of those who attended the meeting was part of the panel of five who heard the complaints.

iii. The Applicants' suggestion that reference data such as the Voter's roll or telephone directories should have been searched as part of their complaint about "bulk interception" is therefore not understood.

iv. The searches which were conducted in the IPT proceedings were plainly adequate, not least because unlawful conduct was identified in respect of two of the complainants.

v. The IPT was assisted throughout the proceedings by Counsel to the Tribunal (CTT) who was able to make submissions (as appropriate) on the adequacy of the search process by GCHQ and the other respondents (GCHQ being the primary respondent given the nature of the allegations in the proceedings).

57. In addition, the Applicants' criticisms of the ISC and the Commissioner are misplaced (see §§101-107 of the Applicants' further observations). Whatever the position historically, it cannot be said that the ISC has devoted little attention to scrutinising the Government's interception programmes, as is evident from its detailed report in March 2015 discussed at e.g. §§1.3, 1.19, 1.21, 1.23-1.24, 1.26, 1.33 of the Observations.

58. As to the suggestion that the part-time status of the Commissioner means that he is unable to provide effective oversight, that has not been suggested by the Commissioner himself. In his 2013 Annual Report he stated that his investigations are "*thorough and penetrating*" and that he has "*no hesitation in challenging the public*

authorities wherever this has been necessary" (at §6.3.3[32]). That sentiment was also reiterated e.g. in his 2015 Annual Report[33].

59. At §§108-115 and §137 of the Applicants' further observations it is said that certain proposed changes to the UK domestic legal framework for investigatory powers, as set out in the Investigatory Powers Bill 2016 (which received Royal Assent on 29 November 2016 as the Investigatory Powers Act, though most of the Act is not yet in force), demonstrate that the current legal framework is "unfit for purpose" and that the Government's position in these proceedings is "unsustainable". But it is important to recognise that the Investigatory Powers Act deals with a wide range of powers, the vast majority of which are beyond the scope of this application. The intention of the Act is to provide an up to date framework for the use (by the SIAs, law enforcement and other public authorities) of investigatory powers to obtain communications and communications data[34]. It addresses not just the interception of communications, but also the retention and acquisition of communications data and equipment interference activity. It will essentially consolidate and build upon the range of current statutory powers in these areas.

60. That a need has been identified for the updating and consolidating of existing legislation, cannot lead to the conclusion that the s.8(4) regime or the intelligence sharing regime is unlawful. That was not the conclusion of the IPT, having investigated these matters in considerable detail. Nor was that any part of the Joint Committee's Report on the Draft Investigatory Powers Bill (see §113 of the Applicants' submissions), whose remit was not to opine on the compatibility of those two regimes with the ECHR[35].

[32] Annex 1. ***Commissioner's Annual Report 2013***

[33] Annex 5. Commissioner's Annual Report 2015. At 2.2 he stated: "*The Commissioner is independent of Government and Parliament and must report half-yearly7 to the Prime Minister on the carrying out of his functions. Independent oversight plays a key role in contributing to accountability. The purpose of oversight is to ensure that there are strong checks and balances, demanding and visible safeguards, and that public authorities are held to account*."

[34] See the Explanatory Notes to the Bill at Annex 7.

[35] See the Joint Committee on the Draft Investigatory Powers Bill, Report, HL Paper 93-HC 651 at Annex No. 26 of the Applicants' Reply. The role of the Joint Committee was to conduct pre-legislative scrutiny of the draft Bill and to make recommendations about the Bill.

Applicants' summary of the procedural history: §§116-126

61. The Government has set out the procedural history to these Applications at pp53-59 of the Observations. In particular it is to be noted that the Applicants are wrong to suggest that they were not represented at the closed hearing on 10 September 2014 at which time the IPT considered the sensitive arrangements governing the s.8(4) and intelligence sharing regimes. As explained at §§7.32-7.35 of the Observations Counsel to the Tribunal (CTT) was appointed in the domestic IPT proceedings and, in practice in this case, performed an essentially similar function to that of a special advocate (see §10 of the 5 December judgment). In those circumstances it is misleading to state that there was no one representing the interests of the applicants in the closed hearing.

LEGAL SUBMISSIONS

Intercepting communications data is as intrusive as intercepting content: §§-134

62. The general answer to this assertion is set out at §§4.29-4.33 and 4.57-4.64 of the Observations i.e. in summary:

(1) The Court has correctly recognised in *Malone v UK* (app. 8691/79, Series A no.82) that it is less intrusive in Article 8 terms to obtain communications data than the content of those communications (see §34 above).

(2) As a result, the Court has rightly not applied the *Weber* safeguards to the acquisition of communications data (as opposed to content).

(3) Similarly, the Court has not applied the *Weber* safeguards to other forms of surveillance (e.g. the installation of GPS in a suspect's car – see *Uzun v Germany* app. 35623/05): which is a strong indicator that the *Weber* criteria should not apply to the acquisition of related communications data under the s.8(4) Regime.

(4) Therefore, the test should be the general one whether the law indicates the scope and manner of any discretion with sufficient clarity to give the individual

adequate protection against arbitrary interference. The s.8(4) Regime satisfies that test as regards communications data, for all the reasons in §§4.57-4.64 of the Observations.

(5) In any event, it should be noted that the s.8(4) Regime distinguishes between communications content, and "related communications data". "Related communications data" has a specific statutory meaning which is not synonymous with "metadata", or "behavioural data. Much "metadata" or "behavioural data" is content for the purposes of the s.8(4) Regime, and is thus subject to the controls for content. For example, information about the internet pages that a user visits on a particular site would be content, not RCD for the purposes of the s.8(4) Regime.

(6) Further, if the *Weber* safeguards did apply to "related communications data", those safeguards would on a proper analysis be met by the s.8(4) Regime.

63. As explained at §§4.17-4.27 of the Observations, *Digital Rights Ireland* is not relevant to the current application, not least because that case did not concern a national regime or any provision governing access to, or use of, retained data by national law enforcement authorities. Nor does the quotation from §27 of the judgment (see §130 of the Applicants' further observations) address the comparative level or intrusiveness as between content and communications data.

64. Further the Advocate General in *Tele2 Sverige* & *Watson*[36] was addressing (in Part 6 of his opinion) the proportionality of "*general data retention obligations*" (§250) including "*the retention of data relating to all communications effected within the national territory procure in the fight against serious crime*" (§251). It was in that specific context that he referred to the risks associated with access to such data being great or even greater than those arising from access to the content of communications (§§257-259). And he specifically contrasted "*targeted surveillance measures*" when reaching these conclusions which he considered were different from "*general data retention obligations*" (§256). For the avoidance of doubt, the Government reserves the right to

[36] Joined Cases C-203/15

make further submissions on the relevance of these proceedings once judgment has been handed down by the CJEU.

65. Similarly it is not correct to equate any powers to obtain related communications data under the s.8(4) regime with the US's telephony collection programme under s.215 of the USA Patriot Act ("the s.215 Power") (see §§133 of the Applicants' further observations).

    a. First it is to be noted that PCLOB found not only that the s.215 Power raised serious constitutional concerns, but also that it had *"shown minimal value in safeguarding the nation from terrorism"*. In part as a result of PCLOB's findings, the s.215 Power was allowed to lapse by the USA, and was replaced by a different programme under the USA Freedom Act which addressed the issues raised by PCLOB.

    b. Secondly, the collection of telephony metadata pursuant to the s.215 Power is not remotely equivalent to powers exercised pursuant to the s.8(4) Regime. The s.215 Power did not concern interception at all. It authorised the bulk acquisition of telephone records generated by certain telephone companies in the United States, and their storage in a single database. That is not what the s.8(4) Regime authorises, or does. Rather, the closer analogue to the s.8(4) Regime is the USA's surveillance programme under s.702 FISA: a power that PCLOB found to be both constitutional and of high and increasing value. See generally the Bulk Powers Review at §§3.50-3.65 and §§40-52 above.

Forseeability and accessibility: §§135-138

66. To the extent that it is sought to be suggested that *Zakharov* introduces any new (and heightened) test of forseeability in this context, that is not accepted. In this context, the essential test remains 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: see §68 of *Malone v UK*. The Grand

Chamber confirmed in *Zakharov* that this test remains the guiding principle when determining the foreseeability of intelligence-gathering powers (see §230).

Internal versus external communications: §§139-

67. This has been addressed in detail at §§4.66-4.76 of the Observations. In addition:

    a. It was very well understood at the time RIPA was passed that the s.8(4) Regime would necessarily entail the interception of all communications flowing down a bearer or bearers; and that this would mean intercepting both "internal" and "external" communications. Precisely those points were made in Parliament by Lord Bassam of Brighton when the Bill which became RIPA was debated: see Observations, §1.37. Moreover, RIPA itself provides for, and authorises, the necessary interception of internal communications in the course of the execution of a s.8(4) warrant for the interception of external communications: see s.5(6) RIPA.

    b. The description in Mr Farr's witness statement of how the definition of "external communications" in s.20 RIPA applies to particular forms of internet-based communication is no more than the application of a clear definition to certain common and current forms of internet usage. In any event, and as already explained in the Observations, the question precisely how the definition of "external communication" applies to particular forms of internet usage is substantially irrelevant to the operation of the s.8(4) Regime. See Observations, §§4.71-4.76.

    c. Contrary to what is asserted at §§141-142 of the Applicants' further observations, the distinction which Mr Farr draws between communications which are received inside and outside the UK is entirely consistent with what was said to Parliament (and what is set out in the Code). If e.g. a communication is received by a platform in the US and is intended to be seen by a wide audience then it is logical that it would be classified as 'external' (see Mr Farr at §§134-138). Moreover, Mr Farr also makes the point (see §137

of his statement) that if e.g. an e-mail is being sent to a specific individual, then the question whether or not the communication was internal or external would depend upon where that individual was located and not on how the e-mail was routed. Consequently there is nothing in Mr Farr's evidence which contradicts the assurances given to Parliament when RIPA was debated.

d. The Government has accepted that the nature of electronic communications over the internet means (and has always meant) that the *factual* analysis of whether a particular communication is internal or external may, in individual cases, be a difficult one (see §4.70 of the Observations). But any such difficulties in how the distinction applies to any *particular* communication is irrelevant in circumstances where it is in practice inevitable (and entirely foreseeable) that, when intercepting material at the level of communications links, both internal and external communications will be intercepted (see §4.71 of the Observations).

e. Importantly the safeguards at the selection for examination stage for communications intercepted under a s.8(4) warrant do not make any distinction between internal or external communications: the safeguards apply equally to both. That means that the s.16 safeguards are not somehow "lost" for UK-based persons if their communications are categorised as external communications (see §§4.73-4.76 of the Observations)[37].

f. Any complexities which may arise in practice in terms of the definition of external and internal communications, do not demonstrate an "apparent indifference" towards the importance of ensuring that there is a clear and accessible regime for bulk interception (as asserted at §§146-147 of the Applicants' further observations). It is a recognition that the way in which

[37] For example, in the case of a Google search, or a YouTube viewing, if the searcher or viewer were in the British Islands, GCHQ could only have selectors that were referable to them as they would be the only individual in relation to whom communications with Google and YouTube could be selected, and such selection would accordingly be done in accordance with the requirements of s.16 RIPA. Whether the communication to be selected were in fact external or internal would be irrelevant. Their interception under the applicable s.8(4) warrant would be lawful (whether by virtue of s.8(4) or s.5(6)(a)), but GCHQ could not examine them if the Secretary of State had not certified that their examination was necessary by means of a modification to the certificate accompanying the s.8(4) warrant (see §4.75 of the Observations).

modern communications systems work will, in practice, inevitably lead to difficult decisions as to how particular communications can be categorised under any legal system. It also involves a proper focus on the essential test for forseeability, namely 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: see §68 of *Malone v UK* and §230 of *Zakharov*. The safeguards which apply regardless of whether the communication is internal or external are central to that.

The framework for analysing the claims: §§148-156

68. The Applicants assert that there is a material difference between the strategic monitoring considered in *Weber* and the s.8(4) regime (see §§148-150). They also assert that the "minimum safeguards" in *Weber* are no longer sufficient to address modern forms of communication surveillance (§§152-156 of the Applicants' further observations).

69. Neither proposition is correct. First there are close parallels with the regime which was considered in *Weber,* as explained in detail at §§4.11-4.12 of the Observations. To assert, as the Applicants do, that the persons liable to be affected by s.8(4) are "*every person who uses the internet*" is a gross and inaccurate exaggeration for the reasons explained in detail at §§5-29 above. It is also important to recognise that the test is not whether, in one or more respects, the s. 8(4) Regime is somehow broader or less tightly defined than the German strategic monitoring regime at issue in *Weber*, not least because the strategic monitoring in that case satisfied the "in accordance with the law" requirement by some margin, in that the Art. 8 complaint in *Weber* was thrown out as "manifestly ill-founded": §138.

70. Secondly to the extent that it is suggested that the decision of the Fourth Section in *Szabo* suggests that the minimum safeguards in *Weber* need to be enhanced in this particular context, that is not accepted.

71. The observations made in *Szabo* were made in the context of a regime which, it was found, allowed ordering of interception entirely by the Executive, with no assessment of strict necessity, with potential interception of individuals outside the operational range and in the absence of any effective remedial or judicial measures (see §17 and §52). Those cumulative factors led the Court to find a violation of Article 8 ECHR. Crucially (and pertinent to the distinction between mass interception and mass surveillance) the Court found there to be no or no adequate controls preventing the examination of communications following interception.

72. In the judgment the Court expressly acknowledged that bulk interception was proportionate in order to meet modern security threats, but that the issue was whether the applicable safeguards were adequate, at §68:

> "[I]*t is a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies in pre-empting such attacks, including the massive monitoring of communications susceptible to containing indications of impending incidents* […] *In the face of this progress the Court must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights*".

73. Insofar as the Court identified a need to enhance Convention case-law on interception (§70), this was for the purpose of addressing <u>surveillance</u> practices, specifically involving the acquisition and retention of detailed profiles of intimate aspects of citizens' lives. As addressed in detail at the outset of these further Observations (and at §§1.21-1.25 of the main Observations), the s.8(4) regime is not one of "mass surveillance".

Alleged absence of mandatory minimum safeguards: §§157-183

(1) The nature of the "offences" which may give rise to an interception order

74. At §§159-160 of the Applicants' further observations it is suggested that bulk interception cannot be lawful in the absence of suspicion that a particular offence has been or may have been committed.

75. This is not what the law requires. It is not mandated by Article 8 ECHR, and it 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.

76. 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. See for example the Bulk Powers Review at §5.3:

"Bulk interception is a capability designed to obtain foreign-focused intelligence and identify individuals, groups and organisations overseas that pose a threat to the UK. It allows the security and intelligence agencies to intercept the communications of individuals outside the UK and then filter and analyse that material in order to identify communications of intelligence value.

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)

77. See too 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."

(Emphasis added)

78. See also the ISC's Report[38] 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…"

79. Turning to the various examples of the use of bulk interception powers under the s.8(4) Regime given in Appendix 8 to the Bulk Powers Review, and set out at §22 above, well over half of the examples 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. The need to undertake target discovery in the present circumstances is readily apparent from the increased terrorist threat in Europe, as exemplified by the state of emergency in France following the Paris attacks of November 2015.

80. Further, even where a known target has been identified, the reasonable basis for targeting that individual's communications may not be that they are themselves engaged in planning or committing criminal acts. A person may be a legitimate intelligence target whether or not they are involved in criminality or analogous acts: for instance, an employee of a hostile foreign government, or a person in contact with a terrorist.

81. In this context, the requirements of s.5 of RIPA, as read with the relevant definitions in s.81 of RIPA and with §§6.11-6.12 of the Code are plainly sufficient as recently affirmed by this Court in *RE v United Kingdom* at §133.

***(2) The categories of people liable to have their communications intercepted:* §§161-169**

[38] Annex 6 to the Observations.

82. For the reasons set out at §5-29 above it is not correct that the initial interception stage is indiscriminate or "virtually limitless" as sought to be contended for by the Applicants (and whether in terms of communications data or otherwise). Consequently the material differences with the regime in *Weber* are not accepted. As set out at §4.42 of the Observations, the categories of persons liable to have their communications intercepted are sufficiently identified at the interception stage.

83. As regards §167 of the Applicants' further observations:

    a. The certificate sets out the categories of communications that GCHQ may examine and the categories directly relate to the intelligence-gathering priorities set out by the Joint Intelligence Committee and agreed by the National Security Council (see ISC Report at §100, 3rd bullet and see also the Code at §6.14).

    b. The Commissioner confirmed in his 2013 Report that the certificate is regularly reviewed and is subject to modification by the Secretary of State (see §6.5.43 and also see the evidence of Mr Farr at §80).

    c. The oversight of the certificate which is provided by the Commissioner is also made clear in the Code (at §6.14) which states: "*The Interception of Communications Commissioner must review any changes to the descriptions of material specified in a certificate.*"

    d. The ISC report also makes clear that the Foreign Secretary was satisfied that "*strategic environmental issues*" reflect a legitimate UK requirement for intelligence (see §103).

    e. As stated at §104 of the ISC Report, following a review by the Foreign Secretary, the certificate is reviewed at least annually by the Secretary of State.

In those circumstances there are substantive limitations on the categories of people whose information can be selected for examination.

(3) Limits on the duration of interception: §170

84. It is not accepted that the time limits in s.9(6) of RIPA are "effectively meaningless". There can be no "long-term rolling renewals" of warrants since there are safeguards in place to ensure that any renewals are necessary and proportionate:

    a. The application for renewal must be made to the Secretary of State, and must contain all the detailed information set out in §6.10 of the Code, just as with the original warrant application (see §6.22 of the Code[39]). The Code states at §6.22 with regard to the renewal application:

    "…the applicant must give an assessment of the value of interception to date and explain why it is considered that interception continues to be necessary for one or more of the statutory purposes in section 5(3), and why it is considered that interception continues to be proportionate."

    b. 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: s. 9(2). Further, by s. 9(3), the Secretary of State must cancel a s. 8(4) warrant if he is satisfied that the warrant is no longer necessary on grounds falling within s. 5(3). Detailed provision is made for the modification of warrants and certificates by s. 10 RIPA.

    c. §6.27 of the Code also requires records to be kept of copies of all renewals and modifications of s. 8(4) warrants / certificates, and the dates on which interception is started and stopped (and §5.17 of the 2002 Code was to like effect).

(4) The procedure to be followed for examining, using and storing the data obtained: §§171-178

[39] See also to parallel effect §5.12 of the 2002 Code.

85. The Government's detailed case on this topic is to be found at §§4.51-4.53 of the Observations. In terms of the further criticisms which have been made by the Applicants, the Government responds by making the following key points:

    a. 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:

        i. 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)). Communications data is a significant resource in this regard.

        ii. 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*".

    b. The programmes referred to at §172 of the Applicants' further observations are neither confirmed nor denied and in any event do not form the subject matter of this application.

    c. Whilst it is right that internal communications can be read if they are selected by reference to a factor which is not by reference to an individual known to be in the British Islands, there are extensive safeguards in place to protect against arbitrary interference. Those are set out at §4.52 of the Observations and have been largely ignored by the Applicants. In addition the system ensures that, even if it is subsequently discovered that an individual is

actually in the UK, when previously that was not known, the SIAs must cease all action at that point (see §112(iv) of the ISC Report).

d. As to the suggestion that s.16(3) of RIPA does not provide the same rigour as a s.8(1) warrant, this is not accepted, as explained at §4.44 of the Observations. In addition, David Anderson QC, after investigating the position in detail in his report 'A Question of Trust', concluded as follows at §6.56(a):

"Most UK-based individuals who are subjects of interest to the security and intelligence agencies or law enforcement are however targets of s8(1) warrants issued by the relevant Secretary of State, which will authorise the interception of all their communications, where necessary with the assistance of GCHQ."

e. It is not the case that there is no regulation or oversight of the use of selectors and search criteria:

   i. The detail of the s.15 and s.16 RIPA arrangements is kept under review by the Commissioner (see §4.53 of the Observations).

   ii. The Code contains express provisions which require records to be kept of the arrangements for securing that only material which has been certified for examination (in accordance with the statutory purposes and tests of necessity and proportionality) is, in fact, read, looked at or listened to (see §6.28 and §§7.16-7.18 in the context of s.16 RIPA). In practice that means that a necessity and proportionality justification must be prepared for any selectors and search criteria which are used.

f. Finally the IPT's Third Judgment dated 22 June 2015 does not support the contention that the procedures for examining, using and storing data are inadequate. That single error does not undermine the overall effectiveness of the safeguards. In addition it is to be noted that the IPT concluded that the "*the selection for examination was proportionate*" (see §15). The Tribunal also indicated that it was "*satisfied that no use whatever was made by the intercepting*

agency of any intercepted material, nor any record retained, and that the Sixth Claimant has not suffered material detriment, damage or prejudice as a result of the breach."

(5) The precautions to be taken when communicating intercepted material to other parties: §§179-181

86. The Applicant's suggestion that there should be a requirement for individualised reasonable suspicion is addressed in detail at §90-97 below.

87. As to the safeguards for the dissemination of intercepted information and any related communications data, it is to be noted that s.15(2) of RIPA is supplemented by the Code and by the constraints imposed by other primary legislation as explained at §4.52(4) and §2.92 of the Observations.

(1) In addition the Applicants have misread *Weber* in the submissions made at §180. At §40 of Weber it was noted that the Federal Constitutional Court had made clear that the transmission of data was proportionate if it served an important legal interest and if there was a sufficient factual basis for the suspicion that "*criminal offences were being planned or had been committed*" (emphasis added). Given that any disclosure under the s.8(4) regime must satisfy the requirements of s.15(2) as supplemented by 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, there is not a material difference between the s.8(4) regime and the strategic monitoring system in *Weber* in this regard.

(6) The circumstances in which data obtained may or must be erased or the records destroyed: §§182-183

88. The Applicants' case that these safeguards are "unclear" is not understood. For the reasons set out at §4.54 of the Observations this requirement is obviously met.

89. There is also no suggestion in the IPT's Third Judgment of 22 June 2015 that the "technical"[40] retention period error in respect of Amnesty International was a systemic problem. Had that been the case the IPT can be expected to have said so in that judgment. In addition the IPT specifically addressed this in its judgment in *Human Rights Watch v Secretary of State for the Foreign and Commonwealth Office et al* [2016] UKIP Trib 15/165/CH, 16 May 2016, at §44, concluding that:

"We are satisfied that there was not... some kind of systemic or wide-ranging failure by the Respondents by virtue of what was disclosed in Liberty/Privacy No 3. There were, as described in paragraphs 5 and 6 above, two relatively minor breaches of procedure."

Further minimum safeguards? §§184-200

No requirement for individual reasonable suspicion

90. At §§185-187 of their further observations the Applicants assert that there should be a minimum requirement of reasonable suspicion that a sender or recipient has committed an offence. In support of that contention the Applicants rely on *Zakharov* and *Szabo*.

91. The true principle to be derived from the authorities on Article 8 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: see Observations, §§4.40-4.56. Any attempt to frame a narrower rule which (for example) outlaws any interception, save where a target has already been identified before the interception takes place, is contrary to the whole thrust of the Court's case law, which permits "strategic monitoring": see *Weber,* where the challenge to the German state's regime in this respect was not only dismissed, but declared manifestly ill-founded. The Applicants impermissibly elevate the Court's particular findings on the specific facts

[40] See §14 of the IPT's Third Judgment dated 22 June 2015 where the IPT stated: "*We are satisfied however that the product was not accessed after the expiry of the relevant retention time limit, and the breach can thus be characterised as technical, though (as recognised by the Tribunal in the Belhadj Judgment) requiring a determination to be made. Though technical, the breach constitutes both "conduct" about which complaint may properly be made under section 65 of RIPA and a breach of Article 8 ECHR… The Tribunal is satisfied that Amnesty… has not suffered material detriment, damage or prejudice as a result of the breach, and that the foregoing Open Determination constitutes just satisfaction, so there will be no award of compensation."*

of certain cases into statements of general principle, rather than findings on particular facts in a particular context.

92. 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.

93. 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 not sufficient in the circumstances, because the domestic court's scrutiny was limited. In particular, 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.

94. 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.

95. 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* at §167.

(4) The s.8(4) Regime provides such oversight. It 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 Observations, §§2.39-2.45.

96. As to the Applicants' reliance on *Szabo*, as the Applicants themselves accept (see §186(2) of the further observations), 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, it was found, allowed ordering of interception entirely by the Executive, with no assessment of strict necessity, with potential interception of individuals outside the operational range and in the absence of any effective remedial or judicial measures.

97. For the reasons explained at §§13-21 above, the Bulk Powers Review demonstrates that the bulk interception powers in the s.8(4) regime are necessary and proportionate, even where the intelligence services are searching for the communications of individuals who have not already been identified as a target and in order to identify threats to the UK. That does not "obviate" any meaningful

assessment of proportionality as that Review and the case studies referred to therein amply demonstrate.

Prior independent authorisation: §§188-193

98. The suggestion that there should be prior independent authorisation of s.8(4) warrants has been comprehensively addressed at §§4.96-4.99 of the Observations. That this is not a minimum requirement was made expressly clear in *Szabo* at §77. This is a situation in which there is extensive independent (including judicial) *post factum* oversight.

99. Neither *Digital Rights Ireland* or *Tele 2 & Watson* (Advocate General Opinion) are relevant in this context. Neither of those cases lay down definitive mandatory requirements relevant to the present context and the Government reserves the right to make further submissions on the latter case following the judgment from the CJEU.

Subsequent notification of interception measures: §§194-200

100. As to the suggestion that there should be a minimum requirement of subsequent notification to individuals of interception measures:

a. That was not a proposition which was advanced domestically before the IPT in these proceedings.

b. As set out above, the *Szabo* decision has to be read in the context of a regime which was entirely deficient in terms of safeguards of the Executive action in question. The Court reached its determination on the basis that there was a failure to comply with the *Weber* minimum safeguards and it was unnecessary for the Court to embark on the question whether enhanced guarantees were necessary (§70). Accordingly, there was no suggestion that the Court was laying down further minimum requirements over and above the *Weber* minimum criteria 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.

c. The Opinion of the Advocate General in *Tele 2* & *Watson* does not support the proposition that there should be a minimum requirement of notification. §236 of his Opinion (cited at §195 of the Applicants'' further observations) was addressing the question of supervision by an independent body, not subsequent notification of data retention (or surveillance measures).

d. Finally it is not correct to say that the Commissioner has been "strongly critical" of "unnecessary limitations" on his oversight (see §§199-200 of the Applicants' further observations). The matters set out at §200 of the Applicants' further submissions formed part of a "wish list" of elements which the Commissioner would have like to have seen in the Investigatory Powers Bill 2016 to strengthen the current oversight of surveillance powers. It was not a suggestion that the current s.8(4) regime was unlawful without subsequent notification to individuals of surveillance measures.

Necessity and proportionality of the s.8(4) regime: §201-214

101. At §§201-214 of the Applicants' further observations it is said that the "bulk interception regime" is unnecessary and disproportionate. In this regard the Government repeats §§4.84-4.95 of the Observations and makes the following additional points.

Strict necessity

102. The Court 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.

103. To the extent that the Applicants rely on *Szabo* for the proposition that a test of "strict necessity" is required, it is submitted that the test previously set out by the Grand Chamber and in the other long-standing cases just referred to is to be preferred. It represents a properly protective set of principles which balance both 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. Strict necessity as a concept is used expressly in the Convention scheme – 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.

104. 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.

The necessity and proportionality of the s.8(4) regime

105. 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 and the ISC in its report of 17 March 2015 (the ISC Report) all conclude in terms, and with supporting analysis and detail, that less intrusive (or different) programmes could not address legitimate needs of the UK. See above and Observations, §§1.21-1.35.

106. Although it is correct that the Independent Reviewer in the Bulk Powers Report was not specifically tasked with opinion on whether bulk interception powers were proportionate (see §204 of the Applicants' further observations), the conclusions of that review and plainly highly material to that question, as summarised at §§13-21 above. At §§9.12-9.14 he 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)

107. In the light of the conclusions of this review, to describe the Government's bulk interception as "*a speculative fishing exercise, designed to check the behaviour of an entire population*" (see §212 of the Applicants' further observations) could not be further from the truth. It is a capability which is of "*vital utility*" in identifying, understanding and averting threats of a national security and/or serious criminal nature.

108. As to the Applicants' reliance on cases involving the bulk *retention* of data (see §§203, 207-209 of the Applicants' further observations), those are irrelevant to the issues raised in this application which involves bulk interception followed by

targeted selection of material. This is not a situation where there is bulk retention of data on an "indiscriminate" basis (see §§207-208 of the Applicants' further observations).

109. Finally it is the case that the bulk interception process involves the discarding of unwanted communications and it does not permit "*the storing and analysing of collateral data*" (see the Applicants' further observations at §213). That was made clear in the Bulk Powers Review at §§2.16 and 2.17. The second (filtering) stage involves discarding those bearers least likely to be of intelligence value and the third (selection) stage involves automatically discarding all communications that do not match the chosen selection criteria.

The lawfulness of the intelligence sharing regime: §§232-250

110. At §§232-250 of the Applicants' further observations it is submitted that "*the standards applicable to interception*" under Art 8 ECHR should also apply "*when access is given to intercepted material even if the actual initial interception was carried out by a foreign intelligence service*"[41].

111. The assertion that the *Weber* safeguards should apply to the sharing of intelligence between the US and UK is misguided, for reasons set out in the Observations at §§3.29-3.36. In short summary:

a. There is no Article 8 case of the Court suggesting that the *Weber* criteria should be applied in the distinct factual context where the intelligence agencies of the respondent State have merely obtained information from a foreign State.

b. The Court has expressly indicated that the "rather strict standards" developed in recent Strasbourg intercept cases do not necessarily apply in other intelligence-gathering contexts[42].

[41] See, in particular, §243.
[42] See Observations at §3.32.

c. 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 sources or from surveillance. In many cases, the Intelligence Services may not even know whether information from an intelligence agency does derive from interception. Moreover, there is no particular reason why such information should be more sensitive than information from any other source. But it would not plainly be neither feasible nor (from a national security perspective) safe for a domestic legal regime to set out all the various types of intelligence that might be obtained from a foreign State; define the tests to be applied when determining whether to obtain them, and the limits on access; and set out the handling, etc. requirement and the uses to which all such types of information might be put.

112. This is not to place form over substance (see §§235-236 of the Applicants' further observations). 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: Mr Farr §§27-30. 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.

113. There is also no contradiction in the Government's policies, including in the Code. Whilst the Government has been able to formulate rules for the requesting and handling of 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) (see §239-240 of the Applicants' further observations), that does not mean that it would be feasible to formulate rules for all the different types of information which might be shared by foreign governments. If the *Weber* criteria apply to the obtaining of intercept material from a foreign intelligence agency, and if

the intelligence sharing regime does not satisfy those criteria, then it is difficult to see how the Intelligence Services could lawfully obtain any information from a foreign intelligence agency about an individual that derived from covert human intelligence sources, covert audio/visual surveillance or covert property searches. But that would be a remarkable, and deeply concerning, conclusion - not least given that intelligence sharing is (and has for many years been) vital to the effective operation of the Intelligence Services (see Mr Farr §§15-26).

114. As to the suggestion that the intelligence sharing regime was substantively defective prior to December 2015 (as well as being insufficiently signposted in public) (see §§246-247 of the Applicants' further observations), for the reasons set out at §§90-99 above, there is no requirement for prior judicial authorisation or any requirement for individual reasonable suspicion.

115. In terms of the Disclosure which was recorded in the IPT's 5 December and 6 February Judgments (see §248 of the Applicants' further observations), since it formed part of a judicial decision it can be taken into account in assessing "forseeability" for Art. 8(2) ECHR purposes – see the Observations at §2.23 and footnote 63. Therefore, prior to being incorporated into the Code, the domestic position was the same as a result of the 5 December and 6 February judgments.

116. It is also inaccurate to speak merely of a "note" setting out the Government's policy. The substance of the note was reflected in the IPT's judgments and is now set out in the Code, which is itself "law" for the purposes of the "in accordance with the law" requirement (see e.g. *Kennedy* and §3.38 of the Observations). In any event the Disclosure is also "law" for these purposes: it is a published statement, contained in publicly accessible court judgments.

117. Finally there is no merit in the criticism that the Disclosure (as now reflected in Chapter 12 of the Code) is obscurely drafted or vague (see §248(2)-(4) of the Applicants' further observations).

a. It is clear that the terms "request" and "receipt" would cover all the scenarios where the SIA that carry out the relevant activities can access material intercepted by foreign intelligence agencies in the circumstances mentioned in §248(2). The access to databases or raw material referred to at §248(2) of the Applicants' further submissions would, on a straightforward application of the Code, be covered by it.

b. The concepts of "analysed" and "unanalysed" are also sufficiently clear (§248(3)). 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".

c. It is wrong to suggest that there is no protection for communications data (§248(4)). 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 by the intercepting agencies or otherwise received from a government of another state 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.

Victim Status

118. The Government does not repeat the submissions about victim status made at §§3.2-3.6 and §4.1 of the Observations. For the avoidance of doubt the Government made clear in its Observations that it was accepted that the South African Legal Resources Centre and Amnesty International did satisfy the victim test in the context of the s.8(4) regime – see §4.1 of the Observations and see §255 of the Applicants' further observations.

119. As regards the intelligence sharing regime, the US programmes referred to at §256 of the Applicants' further submissions, which are said to operate under Executive Order 12333, do not form the subject-matter of this application, which is specifically limited to the Prism and Upstream programmes (which are authorised under s.702 of FISA). In those circumstances it is impermissible for the Applicants to seek to rely on those programmes in support of the contention that they are victims for the purposes of the intelligence sharing regime complaints.

Article 14 ECHR: §§262-271

120. This is addressed in detail at §§8.1-8.16 of the Observations.

121. In terms of whether there is a relevant difference of treatment:

a. It is not the case that the IPT came to the conclusion that the s.16 safeguards have a "disproportionately prejudicial effect" on non-British nationals (see §266 of the Applicants' further observations). That was the *submission* which was made to the IPT by the Applicants, as recorded at §144 of the First Judgment (5 December 2014). But the IPT did not have to determine that submission, because it reached the very clear conclusion that any difference in treatment could, in any event, be justified (see §148 of the First Judgment and the reference to "*any indirect discrimination is sufficiently justified*"). In those circumstances the Government is not seeking to challenge a finding which was made by the IPT in this regard (as suggested at §§265-266 of the Applicants' further observations).

b. As regards the Applicants' analysis of *Magee v United Kingdom*[43], including with reference to *Carson v United Kingdom* App. No. 42184/05, 16 March 2010, any difference in treatment is not on the grounds of "residence" (see §70 of *Carson*), but on the grounds of current location. That is not a relevant difference of treatment for the purposes of Art. 14 ECHR.

[43] App. No. 28135/95, ECtHR 6 June 2000

122. On the question of justification (even if there is (which is denied) a relevant different of treatment), the Applicants' further observations (§§270-271) can be answered as follows:

a. The field of national security is a paradigm example of where a state's margin of appreciation is wide – see *Weber* at §106, *Klass* at §49, *Leander* at §59, *Malone* at §81. The *Stec* test is not inappropriate in the present context (see §271(3) of the Applicants' further observations);

b. The factors relied upon by the Government in support of any difference in treatment were compelling and obvious and are not in any way diminished by a lack of witness evidence to support them. It was "*quite plain*" to the IPT that "*the imposition of a requirement for a s.16(3) certificate in every case would radically undermine the efficacy of the s.8(4) regime, given the pre-eminent role of that regime in the identification of threats to UK national security from abroad*" (§148 of the First (5 December 2014) judgment). There is no proper basis for this court departing from that conclusion of the expert domestic tribunal in this area.

c. There is no inconsistency between the Government's case and its explanation of how the s.8(4) regime works. As set out at §16 above, the selection stage of the s.8(4) process may involve "strong selectors" but it can also involve the "complex query" process. In many cases the SIAs will not know who the individual is and that is wholly unsurprising given the current nature of the terrorist threat which the UK faces – as discussed at §§8.14-8.16 of the Observations.

d. Finally the distinction is not irrational for the reasons explained at §§8.13-8.16 of the Observations. The Government has a panoply of powers to investigate a person present in the UK and that distinction justifies any relevant difference in treatment.

Article 6 ECHR

Determination of civil rights and obligations

123. The suggested distinctions which are asserted by the Applicants at §§272-277 of the Applicants' further observations are unsustainable. In determining whether Art. 6(1) applies to the Applicants' complaints it cannot be relevant whether a domestic tribunal already exists or not. The question is whether the supervisory measures in question are within the scope of the definition of 'civil rights' in Art. 6(1). As recognised by the Grand Chamber in *Ferrazzini* at §24[44], that concept is "autonomous" and thus it cannot be interpreted solely by reference to the domestic law of the respondent State. In addition the Tribunal is specifically designed to operate under the constraints recognised by the Court at §57 of *Klass* (and upon which the Court's conclusion in *Klass* under Art. 6 was based). In particular, a complainant in the Tribunal is not permitted to participate in any factual inquiry that the Tribunal may conduct into the allegations that he has made: eg. the fact of any interception remains secret throughout (save, of course, where the Tribunal finds unlawfulness to have occurred). Thus the fact that RIPA offers individuals the additional safeguard (under Art. 8) of an unlimited right to complain to the Tribunal cannot in itself make Art. 6 apply to such disputes.

124. In *Klass* the Commission reached the clear conclusion that Art. 6 does not apply to state interference on security grounds and there is no good reason why that should not apply in this context. That approach is entirely consistent with the Court's more general jurisprudence on the meaning of "civil rights and obligations" for the reasons set out at §§7.6-7.8 of the Observations.

Fairness

125. The Applicants have raised two new matters which they say are relevant to the assessment of whether the IPT proceedings were compliant with Art. 6(1) ECHR (assuming it applied). They rely on the 28 September 2007 meeting at Thames House (see §§281-283 and also §§98-100 of the Applicants' further observations) and they

[44] App. No. 44759/98, 12 July 2001

also rely on the administrative error which the IPT initially made in its Third Judgment when it mistakenly attributed a finding on breach of Art 8 ECHR to the wrong complainant.

126. In terms of the meeting of September 2007 (recorded in a Note for File dated 15 November 2007) this has been addressed at §§56(b)-(d) above. There is no merit in the suggestion that this undermines the independence or effectiveness of the IPT nor can there be any sensible suggestion that the searches which were conducted in this case were not reasonable or proportionate.

127. As to the reliance on the error made by the IPT, the IPT made clear in its letter dated 1 July 2015 that there had been a mistaken attribution in the judgment which arose after all judicial consideration had taken place and did not result from any failure by the Respondents to make disclosure. That is not a matter which can appropriately lead to the criticism that it demonstrates a lack of rigour in the Tribunal's proportionality assessment. The IPT's judgment (including its proportionality assessment) was reached after full consideration of the relevant material in closed sessions, where the applicants' interests were represented by CTT.

Article 10 ECHR

128. The Article 10 ECHR aspect of the complaints has been addressed in detail at §§6.2-6.39 of the Observations. In response to the Applicants' further observations at §§286-294, the Government makes the following key points:

a. It is to be noted that it was agreed between the parties during the IPT proceedings that, save for the question of prior judicial authorisation, no separate argument arose in relation to Article 10(2), over and above that arising under Article 8(2) (see the IPT's First Judgment dated 5 December 2014 at §149).

b. The Applicants rely on *Sanoma Uitgevers BV v The Netherlands*[45] (see §290 of their further observations), but that was a case concerned with targeted measures to compel disclosure of journalistic sources rather than a regime of strategic monitoring in the course of which journalistic (or NGO) material might be intercepted (*Weber*). It was in that context that the Court identified the importance of prior authorisation by a Judge or other independent body.

c. It is not correct to characterise the relevant provisions of the Code (which do not exhaustively define "confidential communications") as "*nothing more than restatements of "considerations" which may be taken into account*" (see §293 of the Applicants' further observations). As set out at §6.26 of the Observations the Code provides for a series of practical steps which must be taken in terms of the retention, destruction, handling and dissemination of confidential information and that includes notifying the Commissioner of any such material which is retained and making any such information available to him on request.

d. As to proportionality and necessity, the Applicants do not explain how it would be practical or feasible to screen out human rights NGO's privileged communications from the collection stage of the s.8(4) interception regime. It is also material to note that the IPT was entirely satisfied that the communications of Amnesty and the South African Legal Resources Centre had been "lawfully and proportionately" intercepted and accessed/selected for examination (see §§14-15 of the Third Judgment dated 22 June 2015). The effect of the Applicants' submissions is that it could never be necessary or proportionate to subject human rights NGO's communications to s.8(4) activity or the intelligence sharing regime and that is contradicted by the specific findings which the IPT made in these cases.

JUST SATISFACTION – PARA 24

[45] [2011] EMLR 4

129. The Government notes that the Applicants' position is that a reasoned finding of breach of the Convention would be sufficient just satisfaction and they do not seek their costs (see §24 of the Applicants' further observations). In those circumstances it is unnecessary for the Government to make any substantive submissions on this topic.

II REPLY TO INTERVENORS' SUBMISSIONS

European Network of National Human Rights Institutions ("ENNHRI")

Article 6 ECHR: §§8-17

130. ENNHRI's submissions on Article 6 ECHR proceed on a fundamental misunderstanding of what occurred in the domestic IPT proceedings. In particular:

a. The IPT did not "refuse" to direct disclosure of the SIA's sensitive internal guidance concerning the treatment of NGO material. As set out in detail at §§7.37-7.38 of the Observations, the IPT reasonably and appropriately concluded that the issue of NGO confidence had been raised far too late in the domestic proceedings to be considered and the IPT cannot properly be criticised for taking that approach.

b. The IPT did not refuse to consider the Respondents' NCND policy. By agreement between the parties that issue did not arise for determination by the Tribunal (see §13 of the First Judgment dated 5 December 2014).

c. It is not correct to state that the Applicants were not represented in the closed hearing – as explained at §§7.43-7.44 of the Observations the Applicants had the benefit of CTT who was instructed to represent their interests during the closed hearing. Overall there was no unfairness in the procedures which were adopted.

d. In addition, CTT was able to make submissions on the sensitive arrangements which were relevant to the complaints.

131. At §§12 of ENNHRI's submissions it is said that the proceedings in the IPT must have involved the determination of "civil rights" because this was a situation whereby a "judicial body was entrusted with a judicial task". This has been addressed at §119 above. The fact that RIPA offers individuals the additional safeguard (under Art. 8) of an unlimited right to complain to the Tribunal cannot in itself make Art. 6 apply to such disputes.

132. For the reasons set out in detail at §§7.11-7.50 of the Observations, even if Art. 6(1) did apply to the IPT proceedings, those proceedings were fair. To the extent that it is suggested at §16 of ENNHRI's submissions that proceedings could never be fair (whether under the ICCPR or the ECHR) in circumstances where a party is not provided with full disclosure, that is in direct conflict with the decision in *Kennedy v United Kingdom*, where the Court held that the need to keep secret sensitive and confidential information justified the strong restrictions on disclosure of relevant information in proceedings before the IPT in the UK (see §§7.26-7.31 of the Observations). The decision in *ZZ (France) v SSHD*[46] (relied upon by ENNHRI at §17) also acknowledges the possibility of derogation from disclosure requirements for reasons of national security: see §§57-59 and §§64-69. It is not authority for the proposition that there could never be circumstances in which sensitive material was considered in the absence of a party to proceedings.

Article 10: §§18-30

133. The relevance of the case law and other sources cited at §§22-26 of ENNHRI's submissions is not understood. This is not a situation where there has been punishment, prosecution/imprisonment or suppression of journalists or NGOs, nor can it sensibly be suggested that this jurisprudence applies "indirectly" (see §28 of ENNHRI's submissions).

[46] Case C-300/11

134. In terms of the definition of "national security" (see §24 & §27 of ENNHRI's submissions), for the reasons set out at §§4.77-4.81 of the Observations that concept is not "amorphous" in the way it applies to the to the s.8(4) regime, which is designed to ensure that a person's communications cannot be examined simply by reference to unparticularised concerns of "national security". Further, the s.8(4) regime does have precisely those checks and balances to prevent misuse which are called for at §29 of ENNHRI's submissions, for the reasons set out at §§4.32-4.83 and §§6.2-6.30 of the Observations and §§62-89 above.

135. The s.8(4) regime is also proportionate (whether under Art 8 or Art 10 ECHR) for the reasons explained at §§4.84-4.95 and at §§101-109 above.

Article 14: §§31-38

136. As to ENNHRI's submissions on Article 14 ECHR:

a. This is not a situation where there is discrimination on the grounds of nationality. Any difference in treatment is on the grounds of current location and that is not a relevant difference of treatment for the purposes of Art. 14 ECHR, as explained at §§8.3-8.5 of the Observations and at §121 above.

b. In addition, even if there is a relevant difference of treatment (which is not admitted) it is clearly justified for the reasons given at §§8.7-8.16 of the Observations and at §122 above. It is to be noted that ENNHRI's submissions do not attempt to engage with the rational justification for any difference of treatment which is relied upon by the Government and which was straightforwardly accepted by the IPT in its First Judgment of 5 December 2014 – see §§141-148 of the First Judgment dated 5 December 2014.

Electronic Privacy Information Centre ("EPIC")

137. The EPIC submissions make wide-ranging and inaccurate submissions about the nature of US surveillance and US Surveillance law. It is unnecessary and

inappropriate for the Court to make findings about that law (or indeed any future developments in it) in this Application.

138. The EPIC submissions also address alleged US surveillance activities outside the scope of this Application. The Application is about the UK's alleged receipt of information from the USA's PRISM and Upstream programmes, which the NSA operates under the authority of s.702 FISA[47]. EPIC's submissions address the NSA's surveillance activities under a completely different authority (Executive Order, "EO" 12333). It is unnecessary and inappropriate to address EO 12333.

139. It is also unnecessary to address any US activities under s.215 of the US Patriot Act. As set out at §65 above and at §1.7 of the Observations, any activities under that power are of no relevance to this application.

140. As to the allegation that the Upstream and Prism programmes (governed by s.702 FISA powers) are "*largely ignored by US oversight bodies*" and lack legal protections for non-US persons (see §§12-13 of EPIC's submissions), that is not accepted. The Government repeats the submissions made at §§40-52 above. In addition:

141. The US Government's authority to collect "foreign intelligence information" under s.702 of FISA is limited by a number of requirements which have to be examined together to appreciate the limits on this activity.

a. **First**, whilst the definition of "foreign intelligence information" in s. 702 includes "*information with respect to a foreign power or foreign territory that relates to . . . the conduct of the foreign affairs of the United States*" (see 50 U.S.C.

[47] See e.g. Application §4: "*The two programmes which are challenged by this Application are:*
4.1 The soliciting or receipt and use by the UK intelligence services ("UKIS") of data obtained from foreign intelligence partners, in particular the US National Security Agency's "PRISM" and "UPSTREAM" programmes (herafter "receipt of foreign intercept data"), and
4.2 The acquisition of worldwide and domestic communications by the Government Communications Headquarters ("GCHQ")…"
(Emphasis added).

§1801(e))[48], the US may only target specific non-US persons located outside of the US who possess or who are likely to communicate foreign intelligence information that is tied to a specific topical certification issued by the US Attorney General and the US Director of National Intelligence and approved by the Foreign Intelligence Surveillance Court (FISC or FISA Court).

b. More specifically, as part of the US government's application to the FISC, the Attorney General and Director of National Intelligence must specify the categories of foreign intelligence information that the US government is seeking to acquire.[49] And before the certification can be approved, the FISC must determine that the identified categories of foreign intelligence information intended to be collected by the certifications meet the statutory definition of foreign intelligence information.[50] FISC opinions also make clear that s. 702 collection is targeted and must be specifically tied to an identifiable certification. [51]

c. **Secondly**, collection activities under s. 702 must be targeted in the manner described at §§40-52 above.

d. The targeting procedures protect the privacy of non-US persons by ensuring that each individual targeting decision is based upon a sufficient nexus to the

[48] Specifically, 50 U.S.C. § 1801(e) provides:

(e) "Foreign intelligence information" means--

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against--

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to--

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

[49] *See* the July 2014 report on s.702 by the Privacy and Civil Liberties Oversight Board (PCLOB), an independent executive branch agency (hereafter the PCLOB Report), at 23.

[50] *See* PCLOB Report at 6.

[51] *See* FISC Opinion by Judge Hogan reauthorizing certification in 2014. https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

foreign intelligence information sought to be obtained by one of the FISC-approved certifications. Similarly, the written certification approved by the FISA Court must include minimization procedures. The minimization procedures for s.702 have been publicly released.[52] These procedures focus on US persons but also provide important protections to non-US persons.

e. For example, communications acquired under s. 702, whether of US persons or non-US persons, are stored in databases with strict access controls. The data may be reviewed only by intelligence personnel who have been trained about the minimization procedures and who have a reason to access the data.[53] The data can only be queried to identify foreign intelligence information or, in the case of the FBI only, evidence of a crime.[54] The minimization procedures (and PPD-28, discussed below) limit how long data acquired pursuant to s. 702 may be retained.[55] Further, the information may be disseminated only if there is a valid foreign intelligence or law enforcement purpose; the mere fact that one party to the communication is not a US person is insufficient.[56] Moreover, NSA's s. 702 minimization procedures state that non-US person communications may only be retained, used, and disseminated "*in accordance with other applicable law, regulation, and policy*."

[52] The minimization procedures are available at http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf; http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf; and http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf.

[53] *See* NSA Report at 4.

[54] *See, e.g.*, NSA Minimization Procedures at 6-7, *available at* http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf.

[55] *See* NSA Minimization Procedures, *supra* n. 29; PPD-28 Section 4.

[56] FBI PPD-28 procedures available at http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties. *See also* "USSID SP0018: Supplemental Procedures for the Collection, Processing, Retention and Dissemination of Signals Intelligence Information and Data Concerning Personal Information of Non-United States Persons" (January 12, 2015) (NSA PPD-28 Implementation Procedures).

f. **Thirdly**, collection activities under s. 702 are limited to specific and defined intelligence priorities set by policy-makers.[57] These priorities include topics such as nuclear proliferation, counterterrorism, and counter-espionage.

g. **Finally**, collection activities conducted pursuant to s.702 must comply with the privacy protections afforded to non-US persons by Presidential Policy Directive 28 (PPD-28) - see §§1.13-1.14 of the Observations (and see also the Litt Letter). This extends certain protections afforded to the personal information of U.S. persons to non-U.S. person information[58]. It explicitly provides that the personal information of non-U.S. persons acquired during the US' signals intelligence operations shall be afforded privacy protections comparable to the protections afforded to US persons. PPD-28 and IC elements' implementing procedures are publicly available. For example, the NSA Supplemental PPD-28 Procedures state that the United States Signals Intelligence System (USSS) must, "*[w]henever practicable, use one or more selection terms in order to focus collection on specific foreign intelligence targets (e.g., a specific, known international terrorist or terrorist group)*" and the procedures further provide that the USSS "*may not disseminate [personal information of a non-US person] solely because of a person's foreign status*."[59] Additionally, subject to only limited exceptions, NSA is prohibited from retaining information collected pursuant to its signals intelligence activities for more than five years. Section 4(a)(i) of PPD-28.

142. In those circumstances the assertion that US Law does not provide adequate oversight or protection for the collection of non-US persons' data (see §§11-13, §19 and §28-30 of EPIC's submissions) is simply untrue.

Global Campaign for Free Expression (Article 19)

[57] *See* Letter from Robert Litt, General Counsel of the Office of the Director of National Intelligence, dated Feb. 22, 2016, at 4-6 (Annex VI to the Privacy Shield documents) (http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf) (Litt Letter), discussed below.

[58] NSA's unclassified and publicly available PPD-28 procedures apply to all of NSA's signals intelligence activities, including activities undertaken under s.702 - s*ee, e.g.*, NSA PPD-28 Implementation Procedures, Section 7.2.

[59] *See* Sections 4.2 and 7.2 of NSA PPD-28 Implementation Procedures.

143. Article 19's submissions are premised on the erroneous basis that the UK SIA's engage in the "*indiscriminate interception, storage and analysis of online communications*" (see §3). As explained in the Observations and at §§5-21 above, that is an inaccurate description of the s.8(4) regime.

144. As to Article 19's submissions at §§4-6, it is to be noted that the Government has accepted (at 6.1 of the Observations) that NGOs engaged in the legitimate gathering of information of public interest in order to contribute to public debate may properly claim the same Art. 10 ECHR protections as the press. In principle, therefore, the obtaining, retention, use or disclosure of the applicants' communications and communications data may potentially amount to an interference with their Art. 10 rights, at least where the communications in question are quasi-journalistic ones, relating to their role as "social watchdogs".

145. As set out in more detail in the Government's Observations (§§6.2-6.9), the principles to be applied regarding the Applicants' Article 10 challenge are materially the same as those relevant to the Article 8 question. The Government reiterates the Court's finding to this effect in *Telegraaf Media* (§90), where it held that the essential requirements of lawfulness were the same for both articles, and observed that the two apparently different provisions ("*in accordance with the law*" in Article 8 and "*prescribed by law*" in Article 10) were identical in the French text of the Convention (where both require that interference be "*prevue(s) par la loi*", §89).

146. Despite Article 19's detailed submissions to the effect that bulk interception might have a chilling effect on the freedom of NGOs and the press (see §§10-14) the proper and proportionate response to these concerns is not, as Article 19 would appear to suggest, a prohibition on bulk interception. It is to ensure that any interception of journalistic or NGO material, if and when that occurs through the operation of the s.8(4) interception regime, be subject not only to the statutory safeguards enshrined in RIPA which apply to all intercepted data (*inter alia*, the requirement of certification with explicit justification, limitations on duration of

interception and disposal of material), but be subject also to the enhanced safeguards set out in the Code.

147. In terms of the submissions at §§15-24 of Article 19's intervention and the particular reliance placed on the September 2014 report of the UN Special Rapporteur, his call for states to justify "*with particularity*" the tangible counter-terrorism advantages which had accrued from "*mass surveillance technology*" was based on extremely broad assumptions about the type of activity which might be taking place (including in the US), which does not accurately reflect the s.8(4) regime[60].

148. Similarly, the reports relied upon at §§25-27 of Article 19's submissions, which, in large part address indiscriminate, untargeted, secret collection of data under "mass surveillance programmes" bear no relation to the s.8(4) regime, as properly understood. The *Digital Rights Ireland* case is also irrelevant for the reasons set out at §§4.17-4.27 of the Observations.

149. The assertion that surveillance must be targeted and based on reasonable grounds for suspicion (with particular reliance on *Zakharov v Russia*) has been addressed at §§90-97 above and those submissions are not repeated.

150. The suggestion that there should be prior independent authorisation of s.8(4) warrants has been comprehensively addressed at §§4.96-4.99 of the Observations. That this is not a minimum requirement was made expressly clear in *Szabo* at §77. This is a situation in which there is extensive independent (including judicial) *post factum* oversight.

Anna McLeod

[60] For example, his reference to collecting "*all communications all the time indiscriminately*" (at §18, p7) and "*the systemic interference with the Internet privacy rights of a potentially unlimited number of innocent people located in any part of the world*" (at §59, p21) are not a fair or accurate characterisation of the s.8(4) regime.

Anna McLeod

Agent of the Government of the United Kingdom

16 December 2016