

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

GRAND CHAMBER

# CASE OF BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM

*(Applications nos. 58170/13, 62322/14 and 24960/15)*

JUDGMENT

Art 8 • Private life • Convention compliance of secret surveillance regime including bulk interception of communications and intelligence sharing • Need to develop case-law in light of important differences between targeted interception and bulk interception • Adapted test for examining bulk interception regimes through global assessment • Focus on "end-to-end safeguards" to take into account increasing degree of intrusion into privacy rights as bulk interception process moves through different stages • Fundamental deficiencies present in bulk interception regime, through absence of independent authorisation, failure to include categories of selectors in application for warrant, and failure to subject to prior internal authorisation selectors linked to identifiable individuals • Sufficient foreseeability and safeguards in regime for receipt of intelligence from foreign intelligence services • Regime for acquisition of communications data from communications service providers not "in accordance with law"

Art 10 • Freedom of expression • Insufficient protection of confidential journalist material under electronic surveillance schemes

STRASBOURG

25 May 2021

*This judgment is final but it may be subject to editorial revision.*



**In the case of Big Brother Watch and Others v. the United Kingdom,**

The European Court of Human Rights, sitting as a Grand Chamber composed of:

Robert Spano, *President*,
Jon Fridrik Kjølbro,
Angelika Nußberger,
Paul Lemmens,
Yonko Grozev,
Vincent A. De Gaetano,
Paulo Pinto de Albuquerque,
Faris Vehabović,
Iulia Antoanella Motoc,
Carlo Ranzoni,
Mārtiņš Mits,
Gabriele Kucsko-Stadlmayer,
Marko Bošnjak,
Tim Eicke,
Darian Pavli,
Erik Wennerström,
Saadet Yüksel, *judges*,

and Søren Prebensen, *Deputy Grand Chamber Registrar*,

Having deliberated in private on 11 July 2019, on 4 and 6 September 2019 and on 17 February 2021,

Delivers the following judgment, which was adopted on the last-mentioned date:

# PROCEDURE

1. The case originated in three applications (nos. 58170/13, 62322/14 and 24960/15) against the United Kingdom of Great Britain and Northern Ireland lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by the companies, charities, organisations and individuals listed in the annex ("the applicants") on 4 September 2013, 11 September 2014 and 20 May 2015 respectively.

2. The applicants were represented by Mr D. Carey, of Deighton Pierce Glynn Solicitors; Ms R. Curling, of Leigh Day and Co. Solicitors; and Ms E. Norton, of Liberty. The United Kingdom Government ("the Government") were represented by their Agent, Mr C. Wickremasinghe, of the then Foreign and Commonwealth Office.

3. The applicants complained about the scope and magnitude of the electronic surveillance programmes operated by the Government of the United Kingdom.

4. The applications were communicated to the Government on 7 January 2014, 5 January 2015 and 24 November 2015. In the first case, leave to intervene was granted to Human Rights Watch, Access Now, Dutch Against

Plasterk, Center for Democracy & Technology, European Network of National Human Rights Institutions and the Equality and Human Rights Commission, the Helsinki Foundation for Human Rights, the International Commission of Jurists, Open Society Justice Initiative, The Law Society of England and Wales, and Project Moore. In the second case, leave to intervene was granted to the Center for Democracy & Technology, the Helsinki Foundation for Human Rights, the International Commission of Jurists, the National Union of Journalists and the Media Lawyers' Association. In the third case, leave to intervene was granted to ARTICLE 19, the Electronic Privacy Information Center, and the Equality and Human Rights Commission.

5. On 4 July 2017 a Chamber of the First Section decided to join the applications and hold an oral hearing. That hearing took place in public in the Human Rights Building, Strasbourg, on 7 November 2017. On 13 September 2018 a Chamber of that Section, composed of Linos-Alexandre Sicilianos, Kristina Pardalos, Aleš Pejchal, Ksenija Turković, Armen Harutyunyan, Pauliine Koskelo and Tim Eicke, judges, and Abel Campos, Section Registrar, gave judgment. The Chamber unanimously declared inadmissible the complaints made by the applicants in the third of the joined cases concerning Article 6, Article 10, in so far as the applicants relied on their status as non-governmental organisations (NGOs), and Article 14, and declared admissible the remainder of the complaints made by those applicants. By a majority, it declared admissible the complaints made by the applicants in the first and second of the joined cases. Also by a majority, it held that there had been a violation of Articles 8 and 10 of the Convention in respect of both the section 8(4) regime and the Chapter II regime, and it held that there had been no violation of Article 8 of the Convention in respect of the intelligence sharing regime. The partly concurring, partly dissenting opinion of Judge Koskelo, joined by Judge Turković, and the joint partly dissenting and partly concurring opinion of Judges Pardalos and Eicke were annexed to the judgment.

6. On 12 December 2018 and 11 December 2018 respectively, the applicants in the first and third of the joined cases requested the referral of the case to the Grand Chamber in accordance with Article 43 of the Convention. On 4 February 2019, the panel of the Grand Chamber granted that request.

7. The composition of the Grand Chamber was determined according to the provisions of Article 26 §§ 4 and 5 of the Convention and Rule 24 of the Rules of Court.

8. The applicants and the Government each filed observations (Rule 59 § 1) on the admissibility and merits of the case.

9. The President of the Grand Chamber granted leave to intervene in the written procedure, in accordance with Article 36 § 2 of the Convention and

Rule 44 § 3, to the Governments of France, Norway and the Netherlands, and to the United Nations Special Rapporteur on the promotion of the right to freedom of opinion and expression.

10. A hearing took place in public in the Human Rights Building, Strasbourg, on 10 July 2019.

There appeared before the Court:

(a) *for the Government*

Mr C. WICKREMASINGHE, *Agent*,
Mr J. EADIE QC,
Mr J. MITFORD, *Counsel*,
Mr R. YARDLEY,
Ms L. MORGAN,
Mr H. MAWBY,
Mr T. RUTHERFORD,
Mr J. KEAY-BRIGHT, *Advisers*;

(b) *for the applicants*

Mr B. JAFFEY QC,
Ms H. MOUNTFIELD QC,
Mr C. MCCARTHY,
Mr R. MEHTA,
Ms G. SARATHY
Mr D. HEATON, *Counsel*,
Mr D. CAREY,
Ms R. CURLING, *Advisers*.

11. The Court heard addresses by Mr Eadie, Mr Jaffey and Ms Mountfield, as well as their replies to questions.

# THE FACTS

## I. BACKGROUND

12. The three applications were introduced following revelations by Edward Snowden concerning the electronic surveillance programmes operated by the intelligence services of the United States of America and the United Kingdom.

13. The applicants, who are listed in the appendix, all believed that due to the nature of their activities, their electronic communications were likely to have either been intercepted by the United Kingdom intelligence services; obtained by the United Kingdom intelligence services after being intercepted by foreign governments; and/or obtained by the United Kingdom authorities from communications service providers (CSPs).

## II. RELEVANT INTERNET SECRET SURVEILLANCE SCHEMES

14. Internet communications are primarily carried over international sub-marine fibre optic cables operated by CSPs. Each cable may carry several "bearers", and there are approximately 100,000 of these bearers joining up the global Internet. A single communication over the Internet is divided into "packets" (units of data) which may be transmitted separately across multiple bearers. These packets will travel via a combination of the quickest and cheapest paths. Consequently, some or all of the packets of any particular communication sent from one person to another, whether within the United Kingdom or across borders, may be routed through one or more other countries if that is the optimum path for the CSPs involved.

### A. United Kingdom

#### *1. Bulk interception*

15. The Edward Snowden revelations made in 2013 indicated that the Government Communications Headquarters (GCHQ, being one of the United Kingdom intelligence services) was running an operation, codenamed "TEMPORA", which allowed it to tap into and store huge volumes of data drawn from bearers. The United Kingdom authorities neither confirmed nor denied the existence of an operation codenamed TEMPORA.

16. However, according to the March 2015 Report of the Intelligence and Security Committee of Parliament ("the ISC report" – see paragraphs 142-149 below), GCHQ was operating two major processing systems for the bulk interception of communications.

17. The first of the two processing systems referred to in the ISC report was targeted at a very small percentage of bearers. As communications flowed across the targeted bearers, the system compared the traffic against a list of "simple selectors". These were specific identifiers (for example, an email address) relating to a known target. Any communications which matched the simple selectors were collected; those that did not were automatically discarded. Analysts then carried out a "triage process" in relation to collected communications to determine which were of the highest intelligence value and should therefore be opened and read. In practice, only a very small proportion of the items collected under this process were opened and read by analysts. According to the ISC report, GCHQ did not have the capacity to read all communications.

18. The second processing system was targeted at an even smaller number of bearers (a subset of those accessed by the process described in the paragraph above) which were deliberately targeted as those most likely to carry communications of intelligence interest. This second system had two stages: first, the initial application of a set of "processing rules"

designed to discard material least likely to be of value; and secondly, the application of complex queries to the selected material in order to draw out those likely to be of the highest intelligence value. Those searches generated an index, and only items on that index could be examined by analysts. All communications which were not on the index had to be discarded.

19. The legal framework for bulk interception in force at the relevant time is set out in detail in the "relevant domestic law" section below. In brief, section 8(4) of the Regulation of Investigatory Powers Act 2000 ("RIPA" – see paragraph 72 below) allowed the Secretary of State to issue warrants for the "interception of external communications", and pursuant to section 16 RIPA (see paragraphs 84-92 below) intercepted material could not be selected to be read, looked at or listened to, "according to a factor which is referable to an individual who is known to be for the time being in the British Islands".

*2. Intelligence sharing*

20. Chapter 12 of the Interception of Communications Code of Practice ("the IC Code" – see paragraph 116 below) set out the circumstances in which the United Kingdom intelligence services could request intelligence from foreign intelligence services, and the procedures which had to be followed for making such a request. Chapter 12 was added to the IC Code after the Investigatory Powers Tribunal ("the IPT") ordered the intelligence services to disclose their arrangements for intelligence sharing in the course of the proceedings brought by the applicants in the third of the joined cases ("the *Liberty* proceedings" – see paragraphs 28-60 below).

*3. Acquisition of communications data from communications service* providers

21. Chapter II of RIPA and the accompanying Acquisition and Disclosure of Communications Data Code of Practice governed the process by which certain public authorities could request communications data from CSPs (see paragraphs 117-121 below).

## B. United States of America

22. The National Security Agency (NSA) acknowledged the existence of two operations, called PRISM and Upstream.

*1. PRISM*

23. PRISM was a programme through which the United States government obtained intelligence material (such as communications) from Internet service providers (ISPs). Access under PRISM was specific and targeted (as opposed to a broad "data mining" capability). The United States

administration stated that the programme was regulated under the Foreign Intelligence Surveillance Act, and applications for access to material through PRISM had to be approved by the Foreign Intelligence Surveillance Court ("FISC").

24. Documents from the NSA leaked by Edward Snowden suggested that GCHQ had had access to PRISM since July 2010 and used it to generate intelligence reports. GCHQ acknowledged that it had acquired information from the United States, which had been obtained via PRISM.

*2. Upstream*

25. According to the leaked documents, the Upstream programme allowed the collection of content and communications data from fibre-optic cables and infrastructure owned by American CSPs. This programme had broad access to global data, in particular that of non-US citizens, which could then be collected, stored and searched using keywords (for further details, see paragraphs 261-264 below).

## III. DOMESTIC PROCEEDINGS IN THE FIRST AND SECOND OF THE JOINED CASES

26. The applicants in the first of the joined cases (application no. 58170/13) sent a pre-action protocol letter to the United Kingdom Government on 3 July 2013 setting out their complaints and seeking declarations that sections 1 and 3 of the Intelligence Services Act 1994 (see paragraphs 108 and 110 below), section 1 of the Security Service Act 1989 (see paragraph 106 below) and section 8 RIPA (see paragraph 66 below) were incompatible with the Convention. In their reply of 26 July 2013, the Government stated that the effect of section 65(2) RIPA was to exclude the jurisdiction of the High Court in respect of human rights complaints against the intelligence services, but that the applicants' complaints could have been raised before the IPT. The IPT was a specialised tribunal established under RIPA to hear allegations by citizens of wrongful interference with their communications as a result of conduct covered by RIPA, and it was endowed with exclusive jurisdiction to investigate any complaint that a person's communications had been intercepted and, where interception had occurred, to examine the authority for such interception (see paragraphs 122-133 below). However, no further action was taken by these applicants.

27. The applicants in the second of the joined cases (application no. 62322/14) did not bring any domestic proceedings as they did not believe that they had an effective remedy for their Convention complaints.

# IV. DOMESTIC PROCEEDINGS IN THE THIRD OF THE JOINED CASES

28. The ten human rights organisations which are the applicants in the third of the joined cases (application no. 24960/15) each lodged a complaint before the IPT between June and December 2013 (hereinafter "the *Liberty* proceedings"). They alleged that the intelligence services, the Home Secretary and the Foreign Secretary had acted in violation of Articles 8, 10 and 14 of the Convention by: (i) accessing or otherwise receiving intercepted communications and communications data from the United States government under the PRISM and Upstream programmes ("the PRISM issue"); and (ii) intercepting, inspecting and retaining their communications and their communications data under the TEMPORA programme ("the section 8(4) issue").

29. On 14 February 2014, the IPT ordered that the ten cases be joined. It subsequently appointed Counsel to the Tribunal (see paragraph 132 below), whose function was to assist the IPT in whatever way it directed, including by making representations on issues in relation to which not all parties could be represented (for example, for reasons of national security).

30. In their response to the applicants' claims, the Government adopted a "neither confirm nor deny" approach, that is to say, they declined to confirm or deny whether the applicants' communications had actually been intercepted. It was therefore agreed that the IPT would determine the legal issues on the basis of assumed facts to the effect that the NSA had obtained the applicants' communications and communications data via PRISM or Upstream and had passed them to GCHQ, where they had been retained, stored, analysed and shared; and that the applicants' communications and communications data had been intercepted by GCHQ under the TEMPORA programme and had been retained, stored, analysed and shared. The question was whether, on these assumed facts, the interception, retention, storage and sharing of data was compatible with Articles 8 and 10, taken alone and together with Article 14 of the Convention.

## A. The hearing

31. The IPT, composed of two High Court judges, a circuit judge and two senior barristers, held a five-day, public hearing from 14 to 18 July 2014. The Government requested an additional closed hearing in order to enable the IPT to consider GCHQ's unpublished – described during the public hearing as "below the waterline" – internal arrangements for processing intercept material. The applicants objected, arguing that the holding of a closed hearing was not justified and that the failure to disclose the arrangements to them was unfair.

32. The request for a closed hearing was granted pursuant to Rule 9 of the IPT's Rules of Procedure (see paragraph 129 below). On 10 September 2014 a closed hearing took place at which the IPT was "assisted by the full, perceptive and neutral participation ... of Counsel to the Tribunal", who performed the following roles: (i) identifying documents, parts of documents or gists that ought properly to be disclosed; (ii) making such submissions in favour of disclosure as were in the interests of the claimants and open justice; and (iii) ensuring that all the relevant arguments (from the claimants' perspective) on the facts and the law were put before the IPT.

33. In the closed hearing, the IPT examined the internal ("below the waterline") arrangements regulating the conduct and practice of the intelligence services. On 9 October 2014 it notified the applicants that it was of the view that there was some closed material which could be disclosed. It explained that it had invited the Government to disclose the material and that the Government had agreed to do so. The material was accordingly provided to the applicants in a note ("the 9 October disclosure") and the parties were invited to make submissions to the IPT on the disclosed material.

34. The applicants sought information on the context and source of the disclosure but the IPT declined to provide further details. The applicants made written submissions on the disclosure.

35. The respondents subsequently amended and amplified the disclosed material.

36. Following final disclosures made on 12 November 2014, the 9 October disclosure provided as follows:

> "The US Government has publicly acknowledged that the Prism system and Upstream programme ... permit the acquisition of communications to, from, or about specific tasked selectors associated with non-US persons who are reasonably believed to be located outside the United States in order to acquire foreign intelligence information. To the extent that the Intelligence Services are permitted by the US Government to make requests for material obtained under the Prism system (and/or ... pursuant to the Upstream programme), those requests may only be made for unanalysed intercepted communications (and associated communications data) acquired in this way.
>
> 1. A request may only be made by the Intelligence Services to the government of a country or territory outside the United Kingdom for unanalysed intercepted communications (and associated communications data), otherwise than in accordance with an international mutual legal assistance agreement, if either:
>
> a. a relevant interception warrant under [RIPA] has already been issued by the Secretary of State, the assistance of the foreign government is necessary to obtain the communications at issue because they cannot be obtained under the relevant RIPA interception warrant and it is necessary and proportionate for the Intelligence Services to obtain those communications; or
>
> b. making the request for the communications at issue in the absence of a relevant RIPA interception warrant does not amount to a deliberate circumvention of RIPA or otherwise contravene the principle established in *Padfield v. Minister of Agriculture,*

*Fisheries and Food* [1968] AC 997 [that a public body is required to exercise its discretionary powers to promote (and not to circumvent) the policy and the objects of the legislation which created those powers] (for example, because it is not technically feasible to obtain the communications *via* RIPA interception), and it is necessary and proportionate for the Intelligence Services to obtain those communications. In these circumstances, the question whether the request should be made would be considered and decided upon by the Secretary of State personally. Any such request would only be made in exceptional circumstances, and has not occurred as at the date of this statement.

...

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

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

4. The internal 'arrangements' of those of the Intelligence Services that receive unanalysed intercepted material and related communications data from interception under a s.8(4) warrant specify (or require to be determined, on a system-by-system basis) maximum retention periods for different categories of such data which reflect the nature and intrusiveness of the particular data at issue. The periods so specified (or determined) are normally no longer than 2 years, and in certain cases are significantly shorter (intelligence reports that draw on such data are treated as a separate category, and are retained for longer). Data may only be retained for longer than the applicable maximum retention period where prior authorisation has been obtained from a senior official within the particular Intelligence Service at issue on the basis that continued retention of the particular data at issue has been assessed to be necessary and proportionate (if the continued retention of any such data is thereafter assessed no longer to meet the tests of necessity and proportionality, such data are deleted). As far as possible, all retention periods are implemented by a process of automated deletion which is triggered once the applicable maximum retention period has been reached for the data at issue. The maximum retention periods are overseen by, and agreed with the Commissioner. As regards related communications data in particular, Sir Anthony May made a recommendation to those of the Intelligence Services that receive unanalysed intercepted material and related communications data from interception under a s8(4) warrant, and the interim Commissioner (Sir Paul Kennedy) has recently expressed himself to be content with the implementation of that recommendation.

5. The Intelligence Services' internal 'arrangements' under [the Security Services Act 1989], [the Intelligence Services Act 1994] and ss.15-16 of RIPA are periodically reviewed to ensure that they remain up-to-date and effective. Further, the Intelligence Services are henceforth content to consider, during the course of such periodic reviews, whether more of those internal arrangements might safely and usefully be put

into the public domain (for example, by way of inclusion in a relevant statutory Code of Practice)."

## B. First judgment of the Investigatory Powers Tribunal dated 5 December 2014

37. The IPT issued its first judgment on 5 December 2014. The judgment addressed the arrangements then in place for intercepting communications and receiving communications intercepted by foreign intelligence services.

### *1. The PRISM issue*

38. The IPT accepted that the PRISM issue engaged Article 8 of the Convention, albeit at a "lower level" than the regime under consideration in *Weber and Saravia v. Germany* ((dec.), no. 54934/00, ECHR 2006-XI). As a consequence, the authorities involved in processing communications received from foreign intelligence services had to comply with the requirements of Article 8, particularly in relation to their storage, sharing, retention and destruction. In the IPT's view, following *Bykov v. Russia* ([GC], no. 4378/02, §§ 76 and 78, 10 March 2009) and *Malone v. the United Kingdom* (2 August 1984, Series A no. 82), in order for the interference to be considered "in accordance with the law", there could not be unfettered discretion for executive action; rather, the nature of the rules had to be clear and the ambit of the rules had – in so far as possible – to be in the public domain. However, it considered it plain that in the field of national security, much less was required to be put in the public domain and the degree of foreseeability required by Article 8 had to be reduced, otherwise the whole purpose of the steps taken to protect national security would be at risk (citing *Leander v. Sweden*, 26 March 1987, § 51, Series A no. 116).

39. The IPT continued:

> "41. We consider that what is required is a sufficient signposting of the rules or arrangements insofar as they are not disclosed ... We are satisfied that in the field of intelligence sharing it is not to be expected that rules need to be contained in statute (*Weber*) or even in a code (as was required by virtue of the Court's conclusion in *Liberty v.* [*the United Kingdom*, no. 58243/00, 1 July 2008]). It is in our judgment sufficient that:
>
> (i) Appropriate rules or arrangements exist and are publicly known and confirmed to exist, with their content sufficiently signposted, such as to give an adequate indication of it (as per *Malone* ...).
>
> (ii) They are subject to proper oversight."

40. The IPT noted that arrangements for information sharing were provided for in the statutory framework set out in the Security Service Act 1989 (see paragraphs 105-106 below) and the Intelligence Services Act

1994 (see paragraphs 107-110 below). It further referred to a witness statement made in the above-mentioned *Liberty* proceedings by Charles Farr, the Director-General of the Office for Security and Counter Terrorism at the Home Office, which explained that the statutory framework set out in those Acts was underpinned by detailed internal guidance, including arrangements for securing that the services only obtained the information necessary for the proper discharge of their functions. He further indicated that staff received mandatory training on the legal and policy framework in which they operated, including clear instructions on the need for strict adherence to the law and internal guidance. Finally, he stated that the full details of the arrangements were confidential since they could not be published safely without undermining the interests of national security.

41. The IPT acknowledged that as the arrangements were not made known to the public, even in summary form, they were not accessible. However, the IPT considered it significant that the arrangements were subject to oversight and investigation by the Intelligence and Security Committee of Parliament (ISC) and the independent Interception of Communications Commissioner ("the IC Commissioner"). Furthermore, it itself was in a position to provide oversight, having access to all secret information, and being able to adjourn into closed hearing to assess whether the arrangements referred to by Mr Farr existed and were capable of giving the individual protection against arbitrary interference.

42. Having considered the "below the waterline" arrangements, the IPT was satisfied that the 9 October disclosure (as subsequently amended – see paragraphs 33 and 36 above) provided a clear and accurate summary of that part of the evidence given in the closed hearing, and that the rest of the evidence given in closed hearing was too sensitive for disclosure without risk to national security or to the "neither confirm nor deny" principle. It was further satisfied that the preconditions for requesting information from the government of the United States of America were clear: there had to exist either a section 8(1) warrant, or a section 8(4) warrant within whose ambit the proposed target's communications fell, together, if the individual was known to be in the British Islands, with a section 16(3) modification (see paragraph 86 below). Any request pursuant to PRISM or Upstream in respect of intercept or communications data was therefore subject to the RIPA regime, unless it fell within the wholly exceptional scenario outlined in 1(b) of the material disclosed after the first hearing. However, a 1(b) request had never occurred.

43. The IPT nevertheless identified the following "matter of concern":

> "Although it is the case that any request for, or receipt of, intercept or communications data pursuant to Prism and/or Upstream is ordinarily subject to the same safeguards as in a case where intercept or communication data are obtained directly by the Respondents, if there were a 1(b) request, albeit that such request must go to the Secretary of State, and that any material so obtained must be dealt with pursuant to RIPA, there is the possibility that the s.16 protection might not apply. As

> already indicated, no 1(b) request has in fact ever occurred, and there has thus been no problem hitherto. We are however satisfied that there ought to be introduced a procedure whereby any such request, if it be made, when referred to the Secretary of State, must address the issue of s.16(3)."

44. However, subject to this caveat, the IPT reached the following conclusions:

> "(i) Having considered the arrangements below the waterline, as described in this judgment, we are satisfied that there are adequate arrangements in place for the purpose of ensuring compliance with the statutory framework and with Articles 8 and 10 of the Convention, so far as the receipt of intercept from Prism and/or Upstream is concerned.
>
> (ii) This is of course of itself not sufficient, because the arrangements must be sufficiently accessible to the public. We are satisfied that they are sufficiently signposted by virtue of the statutory framework to which we have referred and the Statements of the ISC and the Commissioner quoted above, and as now, after the two closed hearings that we have held, publicly disclosed by the Respondents and recorded in this judgment.
>
> (iii) These arrangements are subject to oversight.
>
> (iv) The scope of the discretion conferred on the Respondents to receive and handle intercepted material and communications data and (subject to the s.8(4) issues referred to below) the manner of its exercise, are accordingly (and consistent with *Bykov* – see paragraph 37 above) accessible with sufficient clarity to give the individual adequate protection against arbitrary interference."

45. Lastly, the IPT addressed an argument raised by Amnesty International only; namely, that the United Kingdom owed a positive obligation under Article 8 of the Convention to prevent or forestall the United States from intercepting communications, including an obligation not to acquiesce in such interception by receiving its product. However, the IPT, citing *M. and Others v. Italy and Bulgaria* (no. 40020/03, § 127, 31 July 2012), noted that "the Convention organs have repeatedly stated that the Convention does not contain a right which requires a High Contracting Party to exercise diplomatic protection, or espouse an applicant's complaints under international law, or otherwise to intervene with the authorities of another State on his or her behalf". The IPT therefore rejected this submission.

### *2. The section 8(4) issue*

46. The IPT formulated four questions to be decided in order to determine whether the section 8(4) regime (which provided the legal framework for the bulk interception of external communications) was compatible with the Convention:

> "(1) Is the difficulty of determining the difference between external and internal communications ... such as to cause the s.8(4) regime not to be in accordance with law contrary to Article 8(2) [of the Convention]?

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

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

(4) Is s.16(2) indirectly discriminatory contrary to Article 14 of the Convention, and, if so, can it be justified?"

47. In relation to the first question, the applicants had contended that following the "sea-change in technology since 2000", substantially more communications were now external, and as a result the internal/external distinction in section 8(4) was no longer "fit for purpose". While the IPT accepted that the changes in technology had been substantial, and that it was impossible to differentiate at interception stage between external and internal communications, it found that the differences in view as to the precise definition of "external communications" did not *per se* render the section 8(4) regime incompatible with Article 8 § 2 of the Convention. In this regard, it considered that the difficulty in distinguishing between "internal" and "external" communications had existed since the enactment of RIPA and the changes in technology had not materially added to the quantity or proportion of communications which could or could not be differentiated as being external or internal at the time of interception. At worst, they had "accelerated the process of more things in the world on a true analysis being external than internal". In any case the distinction was only relevant at interception stage. The "heavy lifting" was done by section 16 RIPA, which prevented intercepted material being selected to be read, looked at or listened to "according to a factor which is referable to an individual who is known to be for the time being in the British Islands" (see paragraphs 84-92 below). Furthermore, all communications intercepted under a section 8(4) warrant could only be considered for examination by reference to that section.

48. In respect of the second question, the IPT held that the section 16 safeguards, which applied only to intercept material and not to related communications data, were sufficient. Although it concluded that the *Weber* criteria also extended to communications data, it considered that there was adequate protection or safeguards by reference to section 15 RIPA (see paragraphs 77-82 below). In addition, in so far as section 16 offered greater protection for communications content than for communications data, the difference was justified and proportionate because communications data were necessary to identify individuals whose intercepted material was protected by section 16 (that is, individuals known to be in the British Islands).

49. Turning to the third question, the IPT concluded that the section 8(4) regime was sufficiently compliant with the *Weber* criteria (being the criteria set out in *Weber and Saravia*, cited above, § 95; see also paragraphs 274

and 335 below) and was in any event "in accordance with the law". With regard to the first and second requirements, it considered that the reference to "national security" was sufficiently clear (citing *Esbester v. the United Kingdom* (dec.), no. 18601/91, 2 April 1993, and *Kennedy v. the United Kingdom*, no. 26839/05, 18 May 2010); the absence of targeting at the interception stage was acceptable and inevitable, as it had been in *Weber*; on their face, the provisions of paragraph 5.2 of the IC Code, together with paragraphs 2.4, 2.5, 5.3, 5.4, 5.5 and 5.6 (see paragraph 96 below), were satisfactory; there was no call for search words to be included in an application for a warrant or in the warrant itself, as this would unnecessarily undermine and limit the operation of the warrant and might in any event be entirely unrealistic; and there was no requirement for the warrant to be judicially authorised.

50. In considering the third, fourth, fifth and sixth of the *Weber* criteria, the IPT had regard to the safeguards in sections 15 and 16 RIPA, the IC Code, and the "below the waterline" arrangements. It did not consider it necessary that the precise details of all the safeguards should be published or contained in either statute or code of practice. Particularly in the field of national security, undisclosed administrative arrangements, which by definition could be changed by the executive without reference to Parliament, could be taken into account, provided that what was disclosed indicated the scope of the discretion and the manner of its exercise. This was particularly so when, as was the case here, the IC Code referred to the arrangements, and there was a system of oversight (being the IC Commissioner, the IPT itself and the ISC) which ensured that these arrangements were kept under review. The IPT was satisfied that, as a result of what it had heard at the closed hearing, there was no large databank of communications data being built up and there were adequate arrangements in respect of the duration of the retention of data and their destruction. As with the PRISM issue, the IPT considered that the section 8(4) arrangements were sufficiently signposted in statute, in the IC Code, in the IC Commissioner's reports and, now, in its own judgment.

51. As regards the fourth and final question, the IPT did not make any finding as to whether there was in fact indirect discrimination on grounds of national origin as a result of the different regimes applicable to individuals located in the British Islands and those located outside, since it considered that any indirect discrimination was sufficiently justified on the grounds that it was harder to investigate terrorist and criminal threats from abroad. Given that the purpose of accessing external communications was primarily to obtain information relating to those abroad, the consequence of eliminating the distinction would be the need to obtain a certificate under section 16(3) RIPA (which exceptionally allowed access to material concerning persons within the British Islands intercepted under a section 8(4) warrant – see

paragraph 86 below) in almost every case, which would radically undermine the efficacy of the section 8(4) regime.

52. Finally, the applicants had argued that the protection afforded by Article 10 of the Convention applied to investigatory NGOs in the same way it applied to journalists. Amnesty International initially alleged before the IPT that there were likely to be no adequate arrangements for material protected by legal professional privilege, a complaint which was subsequently "hived off" to be dealt with in the *Belhadj* case (see paragraphs 99-101 below), to which Amnesty International was joined as an additional claimant. No similar argument was made in respect of NGO confidence until 17 November 2014 (after the first and second open hearings). As the IPT considered that this argument could have been raised at any time, in its judgment it had been raised "far too late" to be incorporated into the ambit of the proceedings.

53. With regard to the remaining Article 10 complaints, the IPT noted that there was no separate argument over and above that arising in respect of Article 8. Although the IPT had regard to *Sanoma Uitgevers B.V. v. the Netherlands* ([GC], no. 38224/03, 14 September 2010), it emphasised that the applicants' case did not concern targeted surveillance of journalists or NGOs. In any case, in its view, in the context of untargeted monitoring via a section 8(4) warrant, it would be "clearly impossible" to anticipate a judicial pre-authorisation prior to the warrant limited to what might turn out to impact upon Article 10. Although the IPT accepted that an issue might arise in the event that, in the course of examination of the contents, some question of journalistic confidence arose, there were additional safeguards in the IC Code in relation to treatment of such material.

54. Following the publication of the judgment, the parties were invited to make submissions on whether, prior to the disclosures made to the IPT, the legal regime in place in respect of the PRISM issue complied with Articles 8 and 10, and on the proportionality and lawfulness of any alleged interception of their communications. The IPT did not see any need for further submissions on the proportionality of the section 8(4) regime as a whole.

### C. Second judgment of the Investigatory Powers Tribunal dated 6 February 2015

55. In its second judgment of 6 February 2015, the IPT considered whether, prior to its December 2014 judgment, the PRISM or Upstream arrangements breached Article 8 and/or 10 of the Convention.

56. It agreed that it was only by reference to the 9 October disclosure as amended (see paragraphs 33 and 36 above) that it was satisfied the regime was "in accordance with the law". The IPT was of the view that without the disclosures made, there would not have been adequate signposting, as was

required under Articles 8 and 10. It therefore made a declaration that prior to the disclosures:

> "23. ... [T]he regime governing the soliciting, receiving, storing and transmitting by UK authorities of private communications of individuals located in the UK, which have been obtained by US authorities pursuant to Prism and/or ... Upstream, contravened Articles 8 or 10 ECHR, but now complies."

## D. Third judgment of the Investigatory Powers Tribunal dated 22 June 2015, as amended by its letter of 1 July 2015

57. The third judgment of the IPT, published on 22 June 2015, determined whether the applicants' communications obtained under PRISM or Upstream had been solicited, received, stored or transmitted by the United Kingdom authorities in contravention of Articles 8 and/or 10 of the Convention; and whether the applicants' communications had been intercepted, viewed, stored or transmitted by the United Kingdom authorities so as to amount to unlawful conduct or in contravention of Articles 8 and/or 10.

58. The IPT made no determination in favour of eight of the ten applicants. In line with its usual practice where it did not find in favour of a claimant, it did not confirm whether or not their communications had been intercepted. However, the IPT made determinations in relation to two applicants. The identity of one of the organisations was wrongly noted in the judgment and the error was corrected by the IPT's letter of 1 July 2015.

59. In respect of Amnesty International, the IPT found that email communications had been lawfully and proportionately intercepted and accessed pursuant to section 8(4) RIPA but that the time-limit for retention permitted under the internal policies of GCHQ had been overlooked and the material had therefore been retained for longer than permitted. However, the IPT was satisfied that the material had not been accessed after the expiry of the relevant retention time-limit and that the breach could be characterised as a technical one. It amounted nonetheless to a breach of Article 8 and GCHQ was ordered to destroy any of the communications which had been retained for longer than the relevant period and to deliver one hard copy of the documents within seven days to the IC Commissioner to retain for five years in case they were needed for any further legal proceedings. GCHQ was also ordered to provide a closed report within fourteen days confirming the destruction of the documents. No award of compensation was made.

60. In respect of the Legal Resources Centre, the IPT found that communications from an email address associated with the applicant had been intercepted and selected for examination under a section 8(4) warrant. Although it was satisfied the interception was lawful and proportionate and that selection for examination was proportionate, the IPT found that the

internal procedure for selection had not been followed. There had therefore been a breach of the Legal Resources Centre's Article 8 rights. However, the IPT was satisfied that no use was made of the material and that no record had been retained so the applicant had not suffered material detriment, damage or prejudice. Its determination therefore constituted just satisfaction and no compensation was awarded.

# RELEVANT LEGAL FRAMEWORK AND PRACTICE

## I. RELEVANT DOMESTIC LAW

### A. Interception of communications

#### *1. Warrants: general*

61. Section 1(1) RIPA (which has now been replaced by the Investigatory Powers Act 2016) rendered unlawful the interception of any communication in the course of its transmission by means of a public postal service or a public telecommunication system unless it took place in accordance with a warrant under section 5 ("intercept warrant").

62. Section 5(2) allowed the Secretary of State to authorise an intercept warrant if he or she believed that it was necessary for the reasons set out in section 5(3), namely that it was in the interests of national security, for the purpose of preventing or detecting serious crime, or for safeguarding the economic well-being of the United Kingdom (in so far as those interests are also relevant to the interests of national security – see paragraphs 3.5 and 6.11 of the IC Code at paragraph 96 below); and that the conduct authorised by the warrant was proportionate to what was sought to be achieved by that conduct. In assessing necessity and proportionality, account had to be taken of whether the information sought under the warrant could reasonably have been obtained by other means.

63. Section 81(2)(b) RIPA defined "serious crime" as crime which satisfied one of the following criteria:

> "(a) that the offence or one of the offences that is or would be constituted by the conduct is an offence for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more;
>
> (b) that the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose."

64. Section 81(5) provided:

> "For the purposes of this Act detecting crime shall be taken to include–
>
> (a) establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed; and
>
> (b) the apprehension of the person by whom any crime was committed;

> and any reference in this Act to preventing or detecting serious crime shall be construed accordingly ..."

65. Section 6 provided that in respect of the intelligence services, only the Director General of MI5, the Chief of MI6 and the Director of GCHQ could have applied for an intercept warrant.

66. There were two types of intercept warrant to which sections 5 and 6 applied: a targeted warrant as provided for by section 8(1), and an untargeted warrant as provided for by section 8(4).

67. By virtue of section 9 RIPA, a warrant issued in the interests of national security or for safeguarding the economic well-being of the United Kingdom ceased to have effect at the end of six months, and a warrant issued for the purpose of detecting serious crime ceased to have effect after three months. At any time before the end of those periods, the Secretary of State was able to renew the warrant (for periods of six and three months respectively) if he or she believed that the warrant continued to be necessary on grounds falling within section 5(3). The Secretary of State was required to cancel an interception warrant if he or she was satisfied that the warrant was no longer necessary on grounds falling within section 5(3).

68. Pursuant to section 5(6), the conduct authorised by an interception warrant had to be taken to include the interception of communications not identified by the warrant if necessary to do what was expressly authorised or required by the warrant; and the obtaining of related communications data.

69. Section 21(4) defined "communications data" as

> "(a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;
>
> (b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person—
>
> i. of any postal service or telecommunications service; or
>
> ii. in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;
>
> (c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service."

70. The March 2015 Acquisition and Disclosure of Communications Data Code of Practice referred to these three categories as "traffic data", "service use information", and "subscriber information". Section 21(6) RIPA further defined "traffic data" as data which identified the person, apparatus, location or address to or from which a communication was transmitted, and information about a computer file or program accessed or run in the course of sending or receiving a communication.

71. According to section 20 RIPA, "related communications data", in relation to a communication intercepted in the course of its transmission by means of a postal service or telecommunication system, meant "so much of any communications data as was obtained by, or in connection with, the interception"; and related "to the communication or to the sender or recipient, or intended recipient, of the communication".

*2. Warrants: section 8(4)*

**(a) Authorisation**

72. "Bulk interception" of communications was carried out pursuant to a section 8(4) warrant. Section 8(4) and (5) RIPA allowed the Secretary of State to issue a warrant for "the interception of external communications in the course of their transmission by means of a telecommunication system".

73. At the time of issuing a section 8(4) warrant, the Secretary of State was also required to issue a certificate setting out a description of the intercepted material which he or she considered it necessary to examine, and stating that he or she considered the examination of that material to be necessary for the reasons set out in section 5(3) (that is, that it was necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or for safeguarding the economic well-being of the United Kingdom – so far as those interests are also relevant to the interests of national security; see sections 3.5 and 6.11 of the IC Code at paragraph 96 below).

**(b) "External" communications**

74. Section 20 defined "external communication" as "a communication sent or received outside the British Islands".

75. In the course of the *Liberty* proceedings, Charles Farr, the Director General of the Office for Security and Counter Terrorism, indicated that two people in the United Kingdom who emailed each other were engaging in "internal communication" even if the email service was housed on a server in the United States of America; however, that communication could nevertheless be intercepted as a "by-catch" of a warrant targeting external communications. On the other hand, a person in the United Kingdom who communicated with a search engine overseas was engaging in an external communication, as was a person in the United Kingdom who posted a public message (such as a tweet or Facebook status update), unless all the recipients of that message were in the British Islands.

76. Giving evidence to the ISC in October 2014, the Secretary of State for Foreign and Commonwealth Affairs considered that:

> "In terms of an email, if one or both of the sender or recipient is overseas then this would be an external communication.

In terms of browsing the Internet, if an individual reads the Washington Post's website, then they have 'communicated' with a web server located overseas, and that is therefore an external communication.

In terms of social media, if an individual posts something on Facebook, because the web server is based overseas, this would be treated as an external communication.

In terms of cloud storage (for example, files uploaded to Dropbox), these would be treated as external communications, because they have been sent to a web server overseas."

### *3. Specific safeguards under the Regulation of Investigatory Powers Act 2000*

#### (a) Section 15

77. Pursuant to section 15(1) RIPA, it was the duty of the Secretary of State to ensure, in relation to all interception warrants, that such arrangements were in force as he or she considered necessary for securing that the requirements of subsections (2) and (3) were satisfied in relation to the intercepted material and any related communications data; and, in the case of warrants in relation to which there were section 8(4) certificates, that the requirements of section 16 were also satisfied.

78. Section 15(2) RIPA provided as follows:

"The requirements of this subsection are satisfied in relation to the intercepted material and any related communications data if each of the following–

a. the number of persons to whom any of the material or data is disclosed or otherwise made available,

b. the extent to which any of the material or data is disclosed or otherwise made available,

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

d. the number of copies that are made,

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

79. Section 15(3) provided:

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

80. Under section 15(4) something was necessary for the authorised purposes if, and only if, it continued to be, or was likely to become, necessary as mentioned in section 5(3) of the Act (that is, it was necessary in the interests of national security, for the purpose of preventing or detecting serious crime; for the purpose of safeguarding the economic well-being of the United Kingdom (in so far as those interests are also relevant to the interests of national security – see paragraphs 3.5 and 6.11 of the IC Code at paragraph 96 below); or for the purpose of giving effect to the

provisions of any international mutual assistance agreement); it was necessary for facilitating the carrying-out of any of the interception functions of the Secretary of State; it was necessary for facilitating the carrying-out of any functions of the IC Commissioner or of the IPT; it was necessary to ensure that a person conducting a criminal prosecution had the information needed to determine what was required by his or her duty to secure the fairness of the prosecution; or it was necessary for the performance of any duty imposed on any person under public records legislation.

81. Section 15(5) required that the arrangements in place for securing compliance with section 15(2) had to include such arrangements as the Secretary of State considered necessary for securing that every copy of the material or data that was made was stored, for so long as it was retained, in a secure manner.

82. Under section 15(6) the arrangements to which section 15(1) referred were not necessary to secure that the requirements of section 15(2) and (3) were satisfied in so far as they related to any of the intercepted material or related communications data, or any copy of any such material or data, possession of which had been surrendered to any authorities of a country or territory outside the United Kingdom. However, such arrangements were required to secure, in the case of every such warrant, that possession of the intercepted material and data and of copies of the material or data were surrendered to authorities of a country or territory outside the United Kingdom only if the requirements of section 15(7) were satisfied. Section 15(7) provided:

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

83. Section 17 RIPA provided that as a general rule no evidence could be adduced, disclosure made or other thing done in connection with legal proceedings which would disclose the content or related communications data of an intercepted communication.

#### (b) Section 16

84. Section 16 set out additional safeguards in relation to the interception of "external" communications under section 8(4) warrants.

Section 16(1) required that intercepted material could only be read, looked at or listened to by the persons to whom it became available by virtue of the warrant if and to the extent that it had been certified as material the examination of which was necessary as mentioned in section 5(3) of the Act; and fell within section 16(2). Section 20 defined "intercepted material" as the contents of any communications intercepted by an interception to which the warrant related.

85. Section 16(2) provided:

> "Subject to subsections (3) and (4), intercepted material falls within this subsection so far only as it is selected to be read, looked at or listened to otherwise than according to a factor which–
>
> a. is referable to an individual who is known to be for the time being in the British Islands; and
>
> b. has as its purpose, or one of its purposes, the identification of material contained in communications sent by him, or intended for him."

86. Under section 16(3), intercepted material fell within section 16(2), notwithstanding that it was selected by reference to one of the factors mentioned in that subsection, if it was certified by the Secretary of State for the purposes of section 8(4) that the examination of material selected according to factors referable to the individual in question was necessary as mentioned in subsection 5(3) of the Act; and the material related only to communications sent during a period specified in the certificate that was no longer than the permitted maximum.

87. The "permitted maximum" was defined in section 16(3A) as follows:

> "(a) in the case of material the examination of which is certified for the purposes of section 8(4) as necessary in the interests of national security, six months; and
>
> (b) in any other case, three months."

88. Under section 16(4), intercepted material also fell within section 16(2), even if it was selected by reference to one of the factors mentioned in that subsection, if the person to whom the warrant was addressed believed, on reasonable grounds, that the circumstances were such that the material would fall within that subsection; or the conditions set out in section 16(5) were satisfied in relation to the selection of the material.

89. Section 16(5) provided:

> "Those conditions are satisfied in relation to the selection of intercepted material if –
>
> (a) it has appeared to the person to whom the warrant is addressed that there has been such a relevant change of circumstances as, but for subsection (4)(b), would prevent the intercepted material from falling within subsection (2);
>
> (b) since it first so appeared, a written authorisation to read, look at or listen to the material has been given by a senior official; and
>
> (c) the selection is made before the end of the permitted period."

90. Under section 16(5A), the "permitted period" meant:

> "(a) in the case of material the examination of which is certified for the purposes of section 8(4) as necessary in the interests of national security, the period ending with the end of the fifth working day after it first appeared as mentioned in subsection (5)(a) to the person to whom the warrant is addressed; and
>
> (b) in any other case, the period ending with the end of the first working day after it first so appeared to that person."

91. Section 16(6) explained that a "relevant change of circumstances" meant that it appeared that either the individual in question had entered the British Islands; or that a belief by the person to whom the warrant was addressed in the individual's presence outside the British Islands was in fact mistaken.

92. Giving evidence to the ISC in October 2014, the Secretary of State for Foreign and Commonwealth Affairs explained that:

> "When an analyst selects communications that have been intercepted under the authority of an 8(4) warrant for examination, it does not matter what form of communication an individual uses, or whether his other communications are stored on a dedicated mail server or in cloud storage physically located in the UK, the US or anywhere else (and in practice the individual user of cloud services will not know where it is stored). If he or she is known to be in the British Islands it is not permissible to search for his or her communications by use of his or her name, e-mail address or any other personal identifier."

### *4. Interception of Communications Code of Practice*

93. Section 71 RIPA provided for the adoption of Codes of Practice by the Secretary of State in relation to the exercise and performance of his or her powers and duties under the Act. Draft Codes of Practice had to be laid before Parliament and were public documents. They could only enter into force in accordance with an order of the Secretary of State. He or she could only make such an order if a draft of the order had been laid before Parliament and approved by a resolution of each House.

94. Under section 72(1) RIPA, a person exercising or performing any power or duty relating to interception of communications had to have regard to the relevant provisions of a code of practice. The provisions of a Code of Practice could, in appropriate circumstances, be taken into account by courts and tribunals under section 72(4) RIPA.

95. The IC Code was issued pursuant to section 71 RIPA. The IC Code in force at the relevant time was issued in 2016.

96. The relevant part of that IC Code provided as follows (footnotes omitted):

> "3.2. There are a limited number of persons who can make an application for an interception warrant, or an application can be made on their behalf. These are:
>
> - The Director-General of the Security Service.
> - The Chief of the Secret Intelligence Service.

- The Director of the Government Communications Headquarters (GCHQ).
- The Director-General of the National Crime Agency (NCA handles interception on behalf of law enforcement bodies in England and Wales).
- The Chief Constable of the Police Service of Scotland.
- The Commissioner of the Police of the Metropolis (the Metropolitan Police Counter Terrorism Command handles interception on behalf of Counter Terrorism Units, Special Branches and some police force specialist units in England and Wales).
- The Chief Constable of the Police Service of Northern Ireland.
- The Commissioners of Her Majesty's Revenue & Customs (HMRC).
- The Chief of Defence Intelligence.
- A person who, for the purposes of any international mutual assistance agreement, is the competent authority of a country or territory outside the UK.

3.3. Any application made on behalf of one of the above must be made by a person holding office under the Crown.

3.4. All interception warrants are issued by the Secretary of State. Even where the urgency procedure is followed, the Secretary of State personally authorises the warrant, although it is signed by a senior official.

**Necessity and proportionality**

3.5. Obtaining a warrant under RIPA will only ensure that the interception authorised is a justifiable interference with an individual's rights under Article 8 (right to respect for private and family life) of the European Convention on Human Rights (ECHR) if it is necessary and proportionate for the interception to take place. RIPA recognises this by first requiring that the Secretary of State believes that the authorisation is necessary for one or more of the following statutory grounds:

- In the interests of national security;
- To prevent or detect serious crime;
- To safeguard the economic well-being of the UK so far as those interests are also relevant to the interests of national security.

3.6. These purposes are set out in section 5(3) of RIPA. The Secretary of State must also believe that the interception is proportionate to what is sought to be achieved by that conduct. Any assessment of proportionality involves balancing the seriousness of the intrusion into the privacy or property of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative, operational or capability terms. The warrant will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that there is a potential threat to national security (for example) may not alone render the most intrusive actions proportionate. No interference should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

3. GENERAL RULES ON INTERCEPTION WITH A WARRANT

...

3.7. The following elements of proportionality should therefore be considered:

• Balancing the size and scope of the proposed interference against what is sought to be achieved;

• Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;

• Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;

• Evidencing, as far as reasonably practicable, what other methods have been considered and were either not implemented or have been employed but which are assessed as insufficient to fulfil operational objectives without the addition of the intercept material sought.

...

**Duration of interception warrants**

3.18. Interception warrants issued on serious crime grounds are valid for an initial period of three months. Interception warrants issued on national security/economic well-being of the UK grounds are valid for an initial period of six months. A warrant issued under the urgency procedure (on any grounds) is valid for five working days following the date of issue unless renewed by the Secretary of State.

3.19. Upon renewal, warrants issued on serious crime grounds are valid for a further period of three months. Warrants renewed on national security/economic well-being of the UK grounds are valid for a further period of six months. These dates run from the date on the renewal instrument.

3.20. Where modifications to an interception warrant are made, the warrant expiry date remains unchanged. However, where the modification takes place under the urgency provisions, the modification instrument expires after five working days following the date of issue, unless it is renewed in line with the routine procedure.

3.21. Where a change in circumstance leads the intercepting agency to consider it no longer necessary, proportionate or practicable for a warrant to be in force, the agency must make a recommendation to the Secretary of State that it should be cancelled with immediate effect.

...

4. SPECIAL RULES ON INTERCEPTION WITH A WARRANT

**Collateral intrusion**

4.1. Consideration should be given to any interference with the privacy of individuals who are not the subject of the intended interception, especially where communications relating to religious, medical, journalistic or legally privileged material may be involved, or where communications between a Member of Parliament and another person on constituency business may be involved or communications between a Member of Parliament and a whistle-blower. An application for an interception warrant should state whether the interception is likely to give rise to a degree of collateral infringement of privacy. A person applying for an interception warrant must also consider measures, including the use of automated systems, to reduce the extent of collateral intrusion. Where it is possible to do so, the application should specify those measures. These circumstances and measures will be taken into account by the Secretary of State when considering a warrant application made under section 8(1) of RIPA. Should an interception operation reach the point where

individuals other than the subject of the authorisation are identified as investigative targets in their own right, consideration should be given to applying for separate warrants covering those individuals.

**Confidential information**

4.2. Particular consideration should also be given in cases where the subject of the interception might reasonably assume a high degree of privacy, or where confidential information is involved. This includes where the communications relate to legally privileged material; where confidential journalistic material may be involved; where interception might involve communications between a medical professional or Minister of Religion and an individual relating to the latter's health or spiritual welfare; or where communications between a Member of Parliament and another person on constituency business may be involved.

4.3. Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking. See also paragraphs 4.26 and 4.28 – 4.31 for additional safeguards that should be applied in respect of confidential journalistic material.

...

**Communications involving confidential journalistic material, confidential personal information and communications between a Member of Parliament and another person on constituency business**

4.26. Particular consideration must also be given to the interception of communications that involve confidential journalistic material, confidential personal information, or communications between a Member of Parliament and another person on constituency business. Confidential journalistic material is explained at paragraph 4.3. Confidential personal information is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and the material in question relates to his or her physical or mental health or to spiritual counselling. Such information can include both oral and written communications. Such information as described above is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence, or is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. For example, confidential personal information might include consultations between a health professional and a patient, or information from a patient's medical records.

...

4.28. Where the intention is to acquire confidential personal information, the reasons should be clearly documented and the specific necessity and proportionality of doing so should be carefully considered. If the acquisition of confidential personal information is likely but not intended, any possible mitigation steps should be considered and, if none is available, consideration should be given to whether special handling arrangements are required within the intercepting agency.

4.29. Material which has been identified as confidential information should be retained only where it is necessary and proportionate to do so for one or more of the authorised purposes set out in section 15(4). It must be securely destroyed when its retention is no longer needed for those purposes. If such information is retained, there must be adequate information management systems in place to ensure that continued retention remains necessary and proportionate for the authorised statutory purposes.

4.30. Where confidential information is retained or disseminated to an outside body, reasonable steps should be taken to mark the information as confidential. Where there is any doubt as to the lawfulness of the proposed handling or dissemination of confidential information, advice should be sought from a legal adviser within the relevant intercepting agency and before any further dissemination of the material takes place.

4.31. Any case where confidential information is retained should be notified to the Interception of Communications Commissioner as soon as reasonably practicable, as agreed with the Commissioner. Any material which has been retained should be made available to the Commissioner on request.

4.32. The safeguards set out in paragraphs 4.28 – 4.31 also apply to any section 8(4) material (see chapter 6) which is selected for examination and which constitutes confidential information.

...

6. INTERCEPTION WARRANTS (SECTION 8(4))

6.1. This section applies to the interception of external communications by means of a warrant complying with section 8(4) of RIPA.

6.2. In contrast to section 8(1), a section 8(4) warrant instrument need not name or describe the interception subject or a set of premises in relation to which the interception is to take place. Neither does section 8(4) impose an express limit on the number of external communications which may be intercepted. For example, if the requirements of sections 8(4) and (5) are met, then the interception of all communications transmitted on a particular route or cable, or carried by a particular CSP, could, in principle, be lawfully authorised. This reflects the fact that section 8(4) interception is an intelligence gathering capability, whereas section 8(1) interception is primarily an investigative tool that is used once a particular subject for interception has been identified.

6.3. Responsibility for the issuing of interception warrants under section 8(4) of RIPA rests with the Secretary of State. When the Secretary of State issues a warrant of this kind, it must be accompanied by a certificate. The certificate ensures that a selection process is applied to the intercepted material so that only material described in the certificate is made available for human examination. If the intercepted material cannot be selected to be read, looked at or listened to with due regard to proportionality and the terms of the certificate, then it cannot be read, looked at or listened to by anyone.

**Section 8(4) interception in practice**

6.4. A section 8(4) warrant authorises the interception of external communications. Where a section 8(4) warrant results in the acquisition of large volumes of communications, the intercepting agency will ordinarily apply a filtering process to automatically discard communications that are unlikely to be of intelligence value. Authorised persons within the intercepting agency may then apply search criteria to select communications that are likely to be of intelligence value in accordance with the terms of the Secretary of State's certificate. Before a particular communication may be accessed by an authorised person within the intercepting agency, the person must provide an explanation of why it is necessary for one of the reasons set out in the certificate accompanying the warrant issued by the Secretary of State, and why it is proportionate in the particular circumstances. This process is subject to internal audit and external oversight by the Interception of Communications Commissioner. Where

the Secretary of State is satisfied that it is necessary, he or she may authorise the selection of communications of an individual who is known to be in the British Islands. In the absence of such an authorisation, an authorised person must not select such communications.

**Definition of external communications**

6.5. External communications are defined by RIPA to be those which are sent or received outside the British Islands. They include those which are both sent and received outside the British Islands, whether or not they pass through the British Islands in the course of their transmission. They do not include communications both sent and received in the British Islands, even if they pass outside the British Islands en route. For example, an email from a person in London to a person in Birmingham will be an internal, not external communication for the purposes of section 20 of RIPA, whether or not it is routed via IP addresses outside the British Islands, because the sender and intended recipient are within the British Islands.

**Intercepting non-external communications under section 8(4) warrants**

6.6. Section 5(6)(a) of RIPA makes clear that the conduct authorised by a section 8(4) warrant may, in principle, include the interception of communications which are not external communications to the extent this is necessary in order to intercept the external communications to which the warrant relates.

6.7. When conducting interception under a section 8(4) warrant, an intercepting agency must use its knowledge of the way in which international communications are routed, combined with regular surveys of relevant communications links, to identify those individual communications bearers that are most likely to contain external communications that will meet the descriptions of material certified by the Secretary of State under section 8(4). It must also conduct the interception in ways that limit the collection of non-external communications to the minimum level compatible with the objective of intercepting wanted external communications.

**Application for a section 8(4) warrant**

6.8. An application for a warrant is made to the Secretary of State. Interception warrants, when issued, are addressed to the person who submitted the application. The purpose of such a warrant will typically reflect one or more of the intelligence priorities set by the National Security Council (NSC).

6.9. Prior to submission, each application is subject to a review within the agency making the application. This involves scrutiny by more than one official, who will consider whether the application is for a purpose falling within section 5(3) of RIPA and whether the interception proposed is both necessary and proportionate.

6.10. Each application, a copy of which must be retained by the applicant, should contain the following information:

- Background to the operation in question:

– Description of the communications to be intercepted, details of the CSP(s) and an assessment of the feasibility of the operation where this is relevant; and

– Description of the conduct to be authorised, which must be restricted to the interception of external communications, or the conduct (including the interception of other communications not specifically identified by the warrant as foreseen under section 5(6)(a) of RIPA) it is necessary to undertake in order to carry out what is authorised or required by the warrant, and the obtaining of related communications data.

- The certificate that will regulate examination of intercepted material;
- An explanation of why the interception is considered to be necessary for one or more of the section 5(3) purposes;
- A consideration of why the conduct to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct;
- Where an application is urgent, supporting justification;
- An assurance that intercepted material will be read, looked at or listened to only so far as it is certified and it meets the conditions of sections 16(2)-16(6) of RIPA; and
- An assurance that all material intercepted will be handled in accordance with the safeguards required by sections 15 and 16 of RIPA (see paragraphs 7.2 and 7.10 respectively).

**Authorisation of a section 8(4) warrant**

6.11. Before issuing a warrant under section 8(4), the Secretary of State must believe the warrant is necessary:

- In the interests of national security;
- For the purpose of preventing or detecting serious crime; or
- For the purpose of safeguarding the economic well-being of the UK so far as those interests are also relevant to the interests of national security.

6.12. The power to issue an interception warrant for the purpose of safeguarding the economic well-being of the UK (as provided for by section 5(3)(c) of RIPA), may only be exercised where it appears to the Secretary of State that the circumstances are relevant to the interests of national security. The Secretary of State will not issue a warrant on section 5(3)(c) grounds if a direct link between the economic well-being of the UK and national security is not established. Any application for a warrant on section 5(3)(c) grounds should therefore identify the circumstances that are relevant to the interests of national security.

6.13. The Secretary of State must also consider that the conduct authorised by the warrant is proportionate to what it seeks to achieve (section 5(2)(b)). In considering necessity and proportionality, the Secretary of State must take into account whether the information sought could reasonably be obtained by other means (section 5(4)).

6.14. When the Secretary of State issues a warrant of this kind, it must be accompanied by a certificate in which the Secretary of State certifies that he or she considers examination of the intercepted material to be necessary for one or more of the section 5(3) purposes. The purpose of the statutory certificate is to ensure that a selection process is applied to intercepted material so that only material described in the certificate is made available for human examination. Any certificate must broadly reflect the 'Priorities for Intelligence Collection' set by the NSC for the guidance of the intelligence agencies. For example, a certificate might provide for the examination of material providing intelligence on terrorism (as defined in the Terrorism Act 2000) or on controlled drugs (as defined by the Misuse of Drugs Act 1971). The Interception of Communications Commissioner must review any changes to the descriptions of material specified in a certificate.

6.15. The Secretary of State has a duty to ensure that arrangements are in force for securing that only that material which has been certified as necessary for examination for a section 5(3) purpose, and which meets the conditions set out in section 16(2) to section 16(6) is, in fact, read, looked at or listened to. The Interception of

Communications Commissioner is under a duty to review the adequacy of those arrangements.

**Urgent authorisation of a section 8(4) warrant**

6.16. RIPA makes provision (section 7(l)(b)) for cases in which an interception warrant is required urgently, yet the Secretary of State is not available to sign the warrant. In these cases the Secretary of State will still personally authorise the interception but the warrant is signed by a senior official, following discussion of the case between officials and the Secretary of State. RIPA restricts the issue of warrants in this way to urgent cases where the Secretary of State has personally and expressly authorised the issue of the warrant (section 7(2)(a)), and requires the warrant to contain a statement to that effect (section 7(4)(a)).

6.17. A warrant issued under the urgency procedure lasts for five working days following the date of issue unless renewed by the Secretary of State, in which case it expires after three months in the case of serious crime or six months in the case of national security or economic well-being, in the same way as other section 8(4) warrants.

**Format of a section 8(4) warrant**

6.18. Each warrant is addressed to the person who submitted the application. A copy may then be served upon such providers of communications services as he or she believes will be able to assist in implementing the interception. CSPs will not normally receive a copy of the certificate. The warrant should include the following:

- A description of the communications to be intercepted;
- The warrant reference number; and
- Details of the persons who may subsequently modify the certificate applicable to the warrant in an urgent case (if authorised in accordance with section 10(7) of RIPA).

**Modification of a section 8(4) warrant and/or certificate**

6.19. Interception warrants and certificates may be modified under the provisions of section 10 of RIPA. A warrant may only be modified by the Secretary of State or, in an urgent case, by a senior official with the express authorisation of the Secretary of State. In these cases a statement of that fact must be endorsed on the modifying instrument, and the modification ceases to have effect after five working days following the date of issue unless it is endorsed by the Secretary of State.

6.20. A certificate must be modified by the Secretary of State, except in an urgent case where a certificate may be modified by a senior official provided that the official holds a position in which he or she is expressly authorised by provisions contained in the certificate to modify the certificate on the Secretary of State's behalf, or the Secretary of State has expressly authorised the modification and a statement of that fact is endorsed on the modifying instrument. In the latter case, the modification ceases to have effect after five working days following the date of issue unless it is endorsed by the Secretary of State.

6.21. Where the Secretary of State is satisfied that it is necessary, a certificate may be modified to authorise the selection of communications of an individual in the British Islands. An individual's location should be assessed using all available information. If it is not possible, to determine definitively where the individual is located using that information, an informed assessment should be made, in good faith, as to the individual's location. If an individual is strongly suspected to be in the UK, the arrangements set out in this paragraph will apply.

**Renewal of a section 8(4) warrant**

6.22. The Secretary of State may renew a warrant at any point before its expiry date. Applications for renewals are made to the Secretary of State and contain an update of the matters outlined in paragraph 6.10 above. In particular, 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 purposes in section 5(3), and why it is considered that interception continues to be proportionate.

6.23. Where the Secretary of State is satisfied that the interception continues to meet the requirements of RIPA, the Secretary of State may renew the warrant. Where the warrant is issued on serious crime grounds, the renewed warrant is valid for a further three months. Where it is issued on national security/economic well-being grounds the renewed warrant is valid for six months. These dates run from the date of signature on the renewal instrument.

6.24. In those circumstances where the assistance of CSPs has been sought, a copy of the warrant renewal instrument will be forwarded to all those on whom a copy of the original warrant instrument has been served, providing they are still actively assisting. A renewal instrument will include the reference number of the warrant or warrants being renewed under this single instrument.

**Warrant cancellation**

6.25. The Secretary of State must cancel an interception warrant if, at any time before its expiry date, he or she is satisfied that the warrant is no longer necessary on grounds falling within section 5(3) of RIPA. Intercepting agencies will therefore need to keep their warrants under continuous review and must notify the Secretary of State if they assess that the interception is no longer necessary. In practice, the responsibility to cancel a warrant will be exercised by a senior official in the warrant issuing department on behalf of the Secretary of State.

6.26. The cancellation instrument will be addressed to the person to whom the warrant was issued (the intercepting agency). A copy of the cancellation instrument should be sent to those CSPs, if any, who have given effect to the warrant during the preceding twelve months.

**Records**

6.27. The oversight regime allows the Interception of Communications Commissioner to inspect the warrant application upon which the Secretary of State's decision is based, and the interception agency may be required to justify the content. Each intercepting agency should keep the following to be made available for scrutiny by the Commissioner as he or she may require:

- All applications made for warrants complying with section 8(4), and applications made for the renewal of such warrants;

- All warrants and certificates, and copies of renewal and modification instruments (if any);

- Where any application is refused, the grounds for refusal as given by the Secretary of State;

- The dates on which interception started and stopped.

6.28. Records should also be kept of the arrangements for securing that only material which has been certified for examination for a purpose under section 5(3) and

which meets the conditions set out in section 16(2) – 16(6) of RIPA in accordance with section 15 of RIPA is, in fact, read, looked at or listened to. Records should be kept of the arrangements by which the requirements of section 15(2) (minimisation of copying and distribution of intercepted material) and section 15(3) (destruction of intercepted material) are to be met. For further details see the chapter on 'Safeguards'.

7. SAFEGUARDS

7.1. All material intercepted under the authority of a warrant complying with section 8(1) or section 8(4) of RIPA and any related communications data must be handled in accordance with safeguards which the Secretary of State has approved in conformity with the duty imposed on him or her by RIPA. These safeguards are made available to the Interception of Communications Commissioner, and they must meet the requirements of section 15 of RIPA which are set out below. In addition, the safeguards in section 16 of RIPA apply to warrants complying with section 8(4). Any breach of these safeguards must be reported to the Interception of Communications Commissioner. The intercepting agencies must keep their internal safeguards under periodic review to ensure that they remain up-to-date and effective. During the course of such periodic reviews, the agencies must consider whether more of their internal arrangements might safely and usefully be put into the public domain.

**The section 15 safeguards**

7.2. Section 15 of RIPA requires that disclosure, copying and retention of intercepted material is limited to the minimum necessary for the authorised purposes. Section 15(4) of RIPA provides that something is necessary for the authorised purposes if the intercepted material:

- Continues to be, or is likely to become, necessary for any of the purposes set out in section 5(3) – namely, in the interests of national security, for the purpose of preventing or detecting serious crime, or for the purpose, in circumstances appearing to the Secretary of State to be relevant to the interests of national security, of safeguarding the economic well-being of the UK;

- Is necessary for facilitating the carrying out of the functions of the Secretary of State under Chapter I of Part I of RIPA;

- Is necessary for facilitating the carrying out of any functions of the Interception of Communications Commissioner or the Tribunal;

- Is necessary to ensure that a person conducting a criminal prosecution has the information needed to determine what is required of him or her by his or her duty to secure the fairness of the prosecution; or

- Is necessary for the performance of any duty imposed by the Public Record Acts.

**Dissemination of intercepted material**

7.3. The number of persons to whom any of the intercepted material is disclosed, and the extent of disclosure, is limited to the minimum that is necessary for the authorised purposes set out in section 15(4) of RIPA. This obligation applies equally to disclosure to additional persons within an agency, and to disclosure outside the agency. It is enforced by prohibiting disclosure to persons who have not been appropriately vetted and also by the need-to-know principle: intercepted material must not be disclosed to any person unless that person's duties, which must relate to one of the authorised purposes, are such that he or she needs to know about the intercepted material to carry out those duties. In the same way, only so much of the intercepted

material may be disclosed as the recipient needs. For example, if a summary of the intercepted material will suffice, no more than that should be disclosed.

7.4. The obligations apply not just to the original interceptor, but also to anyone to whom the intercepted material is subsequently disclosed. In some cases this will be achieved by requiring the latter to obtain the originator's permission before disclosing the intercepted material further. In others, explicit safeguards are applied to secondary recipients.

7.5. Where intercepted material is disclosed to the authorities of a country or territory outside the UK, the agency must take reasonable steps to ensure that the authorities in question have and will maintain the necessary procedures to safeguard the intercepted material, and to ensure that it is disclosed, copied, distributed and retained only to the minimum extent necessary. In particular, the intercepted material must not be further disclosed to the authorities of a third country or territory unless explicitly agreed with the issuing agency, and must be returned to the issuing agency or securely destroyed when no longer needed.

**Copying**

7.6. Intercepted material may only be copied to the extent necessary for the authorised purposes set out in section 15(4) of RIPA. Copies include not only direct copies of the whole of the intercepted material, but also extracts and summaries which identify themselves as the product of an interception, and any record referring to an interception which includes the identities of the persons to or by whom the intercepted material was sent. The restrictions are implemented by requiring special treatment of such copies, extracts and summaries that are made by recording their making, distribution and destruction.

**Storage**

7.7. Intercepted material and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of vetting. This requirement to store intercept product securely applies to all those who are responsible for handling it, including CSPs. The details of what such a requirement will mean in practice for CSPs will be set out in the discussions they have with the Government before a Section 12 Notice is served (see paragraph 3.13).

**Destruction**

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

7.9. Where an intercepting agency undertakes interception under a section 8(4) warrant and receives unanalysed intercepted material and related communications data from interception under that warrant, the agency must specify (or must determine on a system by system basis) maximum retention periods for different categories of the data which reflect its nature and intrusiveness. The specified periods should normally be no longer than two years, and should be agreed with the Interception of Communications Commissioner. Data may only be retained for longer than the applicable maximum retention periods if prior authorisation is obtained from a senior official within the particular intercepting agency on the basis that continued retention

of the data has been assessed to be necessary and proportionate. If continued retention of any such data is thereafter assessed to no longer meet the tests of necessity and proportionality, it must be deleted. So far as possible, all retention periods should be implemented by a process of automated deletion, which is triggered once the applicable maximum retention period has been reached for the data at issue.

**Personnel security**

7.10. All persons who may have access to intercepted material or need to see any reporting in relation to it must be appropriately vetted. On an annual basis, managers must identify any concerns that may lead to the vetting of individual members of staff being reconsidered. The vetting of each individual member of staff must also be periodically reviewed. Where it is necessary for an officer of one agency to disclose intercepted material to another, it is the former's responsibility to ensure that the recipient has the necessary clearance.

**The section 16 safeguards**

7.11. Section 16 provides for additional safeguards in relation to intercepted material gathered under section 8(4) warrants, requiring that the safeguards:

• Ensure that intercepted material is read, looked at or listened to by any person only to the extent that the intercepted material is certified; and

• Regulate the use of selection factors that refer to the communications of individuals known to be currently in the British Islands.

7.12. In addition, any individual selection of intercepted material must be proportionate in the particular circumstances (given section 6(1) of the Human Rights Act 1998).

7.13. The certificate ensures that a selection process is applied to material intercepted under section 8(4) warrants so that only material described in the certificate is made available for human examination (in the sense of being read, looked at or listened to). No official is permitted to gain access to the data other than as permitted by the certificate.

7.14. In general, automated systems must, where technically possible, be used to effect the selection in accordance with section 16(1) of RIPA. As an exception, a certificate may permit intercepted material to be accessed by a limited number of specifically authorised staff without having been processed or filtered by the automated systems. Such access may only be permitted to the extent necessary to determine whether the material falls within the main categories to be selected under the certificate, or to ensure that the methodology being used remains up to date and effective. Such checking must itself be necessary on the grounds specified in section 5(3) of RIPA. Once those functions have been fulfilled, any copies made of the material for those purposes must be destroyed in accordance with section 15(3) of RIPA. Such checking by officials should be kept to an absolute minimum; whenever possible, automated selection techniques should be used instead. Checking will be kept under review by the Interception of Communications Commissioner during his or her inspections.

7.15. Material gathered under a section 8(4) warrant should be read, looked at or listened to only by authorised persons who receive regular mandatory training regarding the provisions of RIPA and specifically the operation of section 16 and the requirements of necessity and proportionality. These requirements and procedures must be set out in internal guidance provided to all authorised persons and the attention of all authorised persons must be specifically directed to the statutory

safeguards. All authorised persons must be appropriately vetted (see paragraph 7.10 for further information).

7.16. Prior to an authorised person being able to read, look at or listen to material, a record should be created setting out why access to the material is required consistent with, and pursuant to, section 16 and the applicable certificate, and why such access is proportionate. Save where the material or automated systems are being checked as described in paragraph 7.14, the record must indicate, by reference to specific factors, the material to which access is being sought and systems should, to the extent possible, prevent access to the material unless such a record has been created. The record should include any circumstances that are likely to give rise to a degree of collateral infringement of privacy, and any measures taken to reduce the extent of the collateral intrusion. All records must be retained for the purposes of subsequent examination or audit.

7.17. Access to the material as described in paragraph 7.15 must be limited to a defined period of time, although access may be renewed. If access is renewed, the record must be updated with the reason for the renewal. Systems must be in place to ensure that if a request for renewal is not made within that period, then no further access will be granted. When access to the material is no longer sought, the reason for this must also be explained in the record.

7.18. Periodic audits should be carried out to ensure that the requirements set out in section 16 of RIPA and Chapter 3 of this code are being met. These audits must include checks to ensure that the records requesting access to material to be read, looked at, or listened to have been correctly compiled, and specifically, that the material requested falls within matters certified by the Secretary of State. Any mistakes or procedural deficiencies should be notified to management, and remedial measures undertaken. Any serious deficiencies should be brought to the attention of senior management and any breaches of safeguards (as noted in paragraph 7.1) must be reported to the Interception of Communications Commissioner. All intelligence reports generated by the authorised persons must be subject to a quality control audit.

7.19. In order to meet the requirements of RIPA described in paragraph 6.3 above, where a selection factor refers to an individual known to be for the time being in the British Islands, and has as its purpose or one of its purposes, the identification of material contained in communications sent by or intended for him or her, a submission must be made to the Secretary of State, or to a senior official in an urgent case, giving an explanation of why an amendment to the section 8(4) certificate in relation to such an individual is necessary for a purpose falling within section 5(3) of RIPA and is proportionate in relation to any conduct authorised under section 8(4) of RIPA.

7.20. The Secretary of State must ensure that the safeguards are in force before any interception under section 8(4) warrants can begin. The Interception of Communications Commissioner is under a duty to review the adequacy of the safeguards.

...

8. DISCLOSURE TO ENSURE FAIRNESS IN CRIMINAL PROCEEDINGS

...

**Exclusion of matters from legal proceedings**

8.3. The general rule is that neither the possibility of interception, nor intercepted material itself, plays any part in legal proceedings. This rule is set out in section 17 of

RIPA, which excludes evidence, questioning, assertion or disclosure in legal proceedings likely to reveal the existence (or the absence) of a warrant issued under this Act (or the Interception of Communications Act 1985). This rule means that the intercepted material cannot be used either by the prosecution or the defence. This preserves 'equality of arms' which is a requirement under Article 6 of the ECHR.

...

10. OVERSIGHT

10.1. RIPA provides for an Interception of Communications Commissioner, whose remit is to provide independent oversight of the use of the powers contained within the warranted interception regime under Chapter I of Part I of RIPA.

10.2. The Commissioner carries out biannual inspections of each of the nine interception agencies. The primary objectives of the inspections are to ensure that the Commissioner has the information he or she requires to carry out his or her functions under section 57 of RIPA and produce his or her report under section 58 of RIPA. This may include inspection or consideration of:

- The systems in place for the interception of communications;
- The relevant records kept by the intercepting agency;
- The lawfulness of the interception carried out; and
- Any errors and the systems designed to prevent such errors.

10.3. Any person who exercises the powers in RIPA Part I Chapter I must report to the Commissioner any action that is believed to be contrary to the provisions of RIPA or any inadequate discharge of section 15 safeguards. He or she must also comply with any request made by the Commissioner to provide any such information as the Commissioner requires for the purpose of enabling him or her to discharge his or her functions."

### *5. Statement of Charles Farr*

97. In his witness statement prepared for the *Liberty* proceedings (see paragraph 40 above), Charles Farr indicated that, beyond the details set out in RIPA, the 2010 IC Code, and the draft 2016 IC Code (which had at that stage been published for consultation), the full details of the sections 15 and 16 safeguards were kept confidential. He had personally reviewed the arrangements and was satisfied that they could not safely be put in the public domain without undermining the effectiveness of the interception methods. However, the arrangements were made available to the IC Commissioner who was required by RIPA to keep them under review. Furthermore, each intercepting agency was required to keep a record of the arrangements in question and any breach had to be reported to the IC Commissioner.

*6. National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*

98. In this review the National Security Council stated that its priorities over the next five years would be as follows:

> "Tackle terrorism head-on at home and abroad in a tough and comprehensive way, counter extremism and challenge the poisonous ideologies that feed it. We will remain a world leader in cyber security. We will deter state-based threats. We will respond to crises rapidly and effectively and build resilience at home and abroad.
>
> Help strengthen the rules-based international order and its institutions, encouraging reform to enable further participation of growing powers. We will work with our partners to reduce conflict, and to promote stability, good governance and human rights.
>
> Promote our prosperity, expanding our economic relationship with growing powers such as India and China, helping to build global prosperity, investing in innovation and skills, and supporting UK defence and security exports."

*7. Judgment of the Investigatory Powers Tribunal of 29 March 2015 in* Belhadj and Others v. Security Service, Secret Intelligence Service, Government Communications Headquarters, the Secretary of State for the Home Department, and the Secretary of State for the Foreign and Commonwealth Office*, IPT/13/132-9/H and IPT/14/86/CH*

99. The applicants in this case complained of breaches of Articles 6, 8 and 14 of the Convention arising from the alleged interception of their legally privileged communications. In so far as Amnesty International, in the course of the *Liberty* proceedings, complained about the adequacy of the arrangements for the protection of material subject to legal professional privilege (LPP), those complaints were "hived off" to be dealt with in this case, and Amnesty International was joined as a claimant (see paragraph 52 above).

100. In the course of the proceedings, the respondents conceded that by virtue of there not being in place a lawful system for dealing with LPP, from January 2010 the regime for the interception/obtaining, analysis, use, disclosure and destruction of legally privileged material had not been in accordance with the law for the purposes of Article 8 § 2 of the Convention and was accordingly unlawful. The Security Service and GCHQ confirmed that they would work in the forthcoming weeks to review their policies and procedures in the light of the draft IC Code and otherwise.

101. The IPT subsequently held a closed hearing, with the assistance of Counsel to the Tribunal (see paragraph 132 below), to consider whether any documents or information relating to any legally privileged material had been intercepted or obtained by the respondents. In a determination of 29 March 2015, it found that the intelligence services had only held two documents belonging to any of the claimants which contained material subject to LPP, and they neither disclosed nor referred to legal advice. It

therefore found that the claimant concerned had not suffered any detriment or damage, and that the determination provided adequate just satisfaction. It nevertheless required that GCHQ provide an undertaking that those parts of the documents containing legally privileged material would be destroyed or deleted; that a copy of the documents would be delivered to the IC Commissioner to be retained for five years; and that a closed report would be provided within fourteen days confirming the destruction and deletion of the documents.

102. Draft amendments to both the IC Code and the Acquisition and Disclosure of Communications Data Code of Practice were subsequently put out for consultation and the Codes which were adopted as a result in 2018 contained expanded sections concerning access to privileged information.

## B. Intelligence sharing

### *1. British-US Communication Intelligence Agreement*

103. A British-US Communication Intelligence Agreement of 5 March 1946 governed the arrangements between the British and United States authorities in relation to the exchange of intelligence information relating to "foreign" communications, defined by reference to countries other than the United States, the United Kingdom and the Commonwealth. Under the agreement, the parties undertook to exchange the products of a number of interception operations relating to foreign communications.

### *2. Relevant statutory framework for the operation of the intelligence services*

104. There are three intelligence services in the United Kingdom: the security service (MI5), the secret intelligence service (MI6) and GCHQ.

#### (a) MI5

105. Pursuant to section 2 of the Security Service Act 1989, it was the duty of the Director-General of MI5, who was appointed by the Secretary of State for the Home Department, to ensure that there were arrangements for securing that no information was obtained by MI5 except in so far as necessary for the proper discharge of its functions or disclosed by it except so far as necessary for that purpose or for the purpose of the prevention or detection of serious crime or for the purpose of any criminal proceedings.

106. Under section 1 of the Act, the functions of MI5 were the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means; to

safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands; and to act in support of the activities of police forces, the National Crime Agency and other law enforcement agencies in the prevention and detection of serious crime.

**(b) MI6**

107. Section 2 of the Intelligence Services Act 1994 ("ISA") provided that the duties of the Chief of Service of MI6, who was appointed by the Secretary of State for Foreign and Commonwealth Affairs (as he then was), included ensuring that there were arrangements for securing that no information was obtained by MI6 except so far as necessary for the proper discharge of its functions, and that no information was disclosed by it except so far as necessary for that purpose, in the interests of national security, for the purposes of the prevention or detection of serious crime or for the purpose of any criminal proceedings.

108. Under section 1 ISA, the functions of MI6 were to obtain and provide information relating to the actions or intentions of persons outside the British Islands; and to perform other tasks relating to the actions or intentions of such persons. Those functions could only be exercised in the interests of national security, with particular reference to the State's defence and foreign policies; in the interests of the economic well-being of the United Kingdom; or in support of the prevention or detection of serious crime.

**(c) GCHQ**

109. Section 4 ISA provided that it was the duty of the Director of GCHQ, who was appointed by the Secretary of State for Foreign and Commonwealth Affairs (as he then was), to ensure that there were arrangements for securing that it obtained no information except so far as necessary for the proper discharge of its functions and that no information was disclosed by it except so far as necessary.

110. Under section 3 ISA, one of the functions of GCHQ was to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material. This function was exercisable only in the interests of national security, with particular reference to the State's defence and foreign policies; in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or in support of the prevention or detection of serious crime.

**(d) Counter-Terrorism Act 2008**

111. Section 19 of the Counter-Terrorism Act 2008 allowed the disclosure of information to any of the intelligence services for the purpose of the exercise of any of their functions. Information obtained by an intelligence service in connection with the exercise of its functions could be used by that service in connection with the exercise of any of its other functions.

112. Information obtained by MI5 could be disclosed for the purpose of the proper discharge of its functions, for the purpose of the prevention or detection of serious crime, or for the purpose of any criminal proceedings. Information obtained by MI6 could be disclosed for the purpose of the proper discharge of its functions, in the interests of national security, for the purpose of the prevention or detection of serious crime, or for the purpose of any criminal proceedings. Information obtained by GCHQ could be disclosed by it for the purpose of the proper discharge of its functions or for the purpose of any criminal proceedings.

**(e) Data Protection Act 1998**

113. The Data Protection Act 1998 was the legislation transposing into United Kingdom law Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31). Each of the intelligence services was a "data controller" for the purposes of the Act and, as such, they were required to comply – subject to exemption by Ministerial certificate – with the data protection principles in Part 1 of Schedule 1, which included as follows:

> "(5) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes ..."

and

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

**(f) Official Secrets Act 1989**

114. A member of the intelligence services would commit an offence under section 1(1) of the Official Secrets Act 1989 if he or she disclosed, without lawful authority, any information, document or other article relating to security or intelligence which was in his or her possession by virtue of his or her position as a member of those services.

**(g) Human Rights Act 1998**

115. Under section 6 of the Human Rights Act 1998, it is unlawful for a public authority to act in a way which is incompatible with a Convention right.

*3. Interception of Communications Code of Practice*

116. Following the *Liberty* proceedings, the information contained in the 9 October disclosure (see paragraphs 33 and 36 above) was incorporated into the IC Code:

"12. RULES FOR REQUESTING AND HANDLING UNANALYSED INTERCEPTED COMMUNICATIONS FROM A FOREIGN GOVERNMENT

**Application of this chapter**

12.1. This chapter applies to those intercepting agencies that undertake interception under a section 8(4) warrant.

**Requests for assistance other than in accordance with an international mutual assistance agreement**

12.2. A request may only be made by an intercepting agency to the government of a country or territory outside the UK for unanalysed intercepted communications (and associated communications data), otherwise than in accordance with an international mutual assistance agreement, if either:

• A relevant interception warrant under RIPA has already been issued by the Secretary of State, the assistance of the foreign government is necessary to obtain the particular communications because they cannot be obtained under the relevant RIPA interception warrant and it is necessary and proportionate for the intercepting agency to obtain those communications; or

• Making the request for the particular communications in the absence of a relevant RIPA interception warrant does not amount to a deliberate circumvention of RIPA or otherwise frustrate the objectives of RIPA (for example, because it is not technically feasible to obtain the communications via RIPA interception), and it is necessary and proportionate for the intercepting agency to obtain those communications.

12.3. A request falling within the second bullet of paragraph 12.2 may only be made in exceptional circumstances and must be considered and decided upon by the Secretary of State personally.

12.4. For these purposes, a 'relevant RIPA interception warrant' means one of the following: (i) a section 8(1) warrant in relation to the subject at issue; (ii) a section 8(4) warrant and an accompanying certificate which includes one or more 'descriptions of intercepted material' (within the meaning of section 8(4)(b) of RIPA) covering the subject's communications, together with an appropriate section 16(3) modification (for individuals known to be within the British Islands); or (iii) a section 8(4) warrant and an accompanying certificate which includes one or more 'descriptions of intercepted material' covering the subject's communications (for other individuals).

**Safeguards applicable to the handling of unanalysed intercepted communications from a foreign government**

12.5. If a request falling within the second bullet of paragraph 12.2 is approved by the Secretary of State other than in relation to specific selectors, any communications obtained must not be examined by the intercepting agency according to any factors as are mentioned in section 16(2)(a) and (b) of RIPA unless the Secretary of State has personally considered and approved the examination of those communications by reference to such factors.[1]

[Footnote 1: All other requests within paragraph 12.2 (whether with or without a relevant RIPA interception warrant) will be made for material to, from or about specific selectors (relating therefore to a specific individual or individuals). In these circumstances the Secretary of State will already therefore have approved the request for the specific individual(s) as set out in paragraphs [*sic*] 12.2.]

12.6. Where intercepted communications content or communications data are obtained by the intercepting agencies as set out in paragraph 12.2, or are otherwise received by them from the government of a country or territory outside the UK in circumstances where the material identifies itself as the product of an interception, (except in accordance with an international mutual assistance agreement), the communications content and communications data 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.

12.7. All requests in the absence of a relevant RIPA interception warrant to the government of a country or territory outside the UK for unanalysed intercepted communications (and associated communications data) will be notified to the Interception of Communications Commissioner."

## C. Acquisition of communications data

117. Chapter II of Part 1 of RIPA set out the framework under which public authorities could acquire communications data from CSPs.

118. Under section 22, authorisation for the acquisition of communications data from CSPs was granted by a "designated person", being a person holding such office, rank or position with relevant public authorities as prescribed by an order made by the Secretary of State. The designated person could either grant authorisation for persons within the same "relevant public authority" as himself or herself to "engage in conduct to which this Chapter applies" (authorisation under section 22(3)), or he or she could, by notice to the CSP, require it either to disclose data already in its possession, or to obtain and disclose data (notice under section 22(4)). For the purposes of section 22(3), "relevant public authorities" included a police force, the National Crime Agency, Her Majesty's Revenue and Customs, any of the intelligence services and any such public authority as could be specified by an order made by the Secretary of State.

119. Section 22(2) further provided that the designated person could only grant an authorisation under section 22(3) or give a notice under

section 22(4) if he or she believed it was necessary for one of the following grounds:

> "(a) in the interests of national security;
>
> (b) for the purpose of preventing or detecting crime or of preventing disorder;
>
> (c) in the interests of the economic well-being of the United Kingdom;
>
> (d) in the interests of public safety;
>
> (e) for the purpose of protecting public health;
>
> (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
>
> (g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or
>
> (h) for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State."

120. He or she also had to believe that obtaining the data was proportionate to what was sought to be achieved.

121. Chapter II of RIPA was supplemented by the Acquisition and Disclosure of Communications Data Code of Practice, issued pursuant to section 71 RIPA.

## D. Practice and procedure of the Investigatory Powers Tribunal

### *1. Regulation of Investigatory Powers Act 2000*

122. The IPT was established under section 65(1) RIPA to hear allegations by citizens of wrongful interference with their communications as a result of conduct covered by that Act. It had jurisdiction to investigate any complaint that a person's communications had been intercepted and, where interception had occurred, to examine the authority for such interception.

123. Appointments to the IPT were essentially judicial in nature but varied depending on whether the proposed candidate was a serving member of the senior judiciary of England and Wales, Scotland or Northern Ireland (referred to as a "judicial member") or if they were a "non-judicial member". A non-judicial member could be a former member of the judiciary who was no longer serving or a senior member of the legal profession of at least ten years' standing who was not a full-time judge. Where judicial members were selected from the judiciary in England and Wales, the Judicial Office, on behalf of the Lord Chief Justice, managed the selection process. The Judicial Office invited expressions of interest from serving High Court judges in England and Wales and applicants were interviewed by a panel, which consisted of the President of the IPT, a non-judicial member of the IPT and a lay commissioner from the Judicial

Appointments Commission. The panel then reported to the Lord Chief Justice who wrote to the Home Secretary making formal recommendations for appointments. The Home Secretary then wrote to the Prime Minister asking him to seek permission for letters patent from Her Majesty the Queen for the recommended appointment(s). The Prime Minister recommended the chosen candidate(s) to Her Majesty the Queen, who formalised the appointment through letters patent. Non-judicial members were recruited through open competition. The IPT placed advertisements for non-judicial members in a selection of national newspapers and recruitment sites, asking for expressions of interest from suitably qualified individuals. The process differed from that of judicial members in that it did not involve the Lord Chief Justice, but was the same in all other respects. There are currently five judicial members (two members of the English Court of Appeal (one of whom is the President), one member of the English High Court and two members of the Outer House of the Court of Session in Scotland (one of whom is the Vice-President)) and five non-judicial members (of whom one is a retired High Court judge from Northern Ireland).

124. Pursuant to sections 67(2) and 67(3)(c) RIPA, the IPT was to apply the principles applicable by a court on an application for judicial review. It did not, however, have power to make a Declaration of Incompatibility if it found primary legislation to be incompatible with the European Convention on Human Rights as it was not a "court" for the purposes of section 4 of the Human Rights Act 1998.

125. Section 68(6) and (7) RIPA required those involved in the authorisation and execution of an interception warrant to disclose or provide to the IPT all documents and information it required.

126. Section 68(4) RIPA provided that where the IPT determined any complaint it had the power to award compensation and to make such other orders as it thought fit, including orders quashing or cancelling any warrant and orders requiring the destruction of any records obtained thereunder (section 67(7)). In the event that a claim before the IPT was successful, the IPT was generally required to make a report to the Prime Minister (section 68(5)).

127. Section 68(1) RIPA entitled the IPT to determine its own procedure, although section 69(1) provided that the Secretary of State could also make procedural rules.

### *2. Investigatory Powers Tribunal Rules 2000*

128. The IPT's Rules of Procedure were adopted by the Secretary of State to govern various aspects of the procedure before the IPT.

129. Rule 9 allowed the IPT to hold, at any stage of consideration, oral hearings at which the complainant could make representations, give evidence and call witnesses. Although Rule 9 provided that the IPT's

proceedings, including any oral hearings, were to be conducted in private, in cases IPT/01/62 and IPT/01/77 the IPT itself decided that, subject to the general duty imposed by Rule 6 (1) to prevent the disclosure of sensitive information, it could exercise its discretion in favour of holding an open hearing. Following this commitment to hold hearings in open when possible, the IPT has also published its significant rulings on its website, provided that there is no risk of disclosure of any prejudicial information.

130. Rule 11 allowed the IPT to receive evidence in any form, even where it would not be admissible in a court of law.

131. Rule 6 required the IPT to carry out its functions in such a way as to ensure that information was not disclosed that was contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of the United Kingdom or the continued discharge of the functions of any of the intelligence services.

#### *3. Counsel to the Tribunal*

132. The IPT could appoint Counsel to the Tribunal to make submissions on behalf of applicants in hearings at which they could not be represented. In the *Liberty* proceedings, Counsel to the Tribunal described his role as follows:

> "Counsel to the Tribunal performs a different function [from special advocates in closed proceedings conducted before certain tribunals], akin to that of *amicus curiae*. His or her function is to assist the Tribunal in whatever way the Tribunal directs. Sometimes (e.g. in relation to issues on which all parties are represented), the Tribunal will not specify from what perspective submissions are to be made. In these circumstances, counsel will make submissions according to his or her own analysis of the relevant legal or factual issues, seeking to give particular emphasis to points not fully developed by the parties. At other times (in particular where one or more interests are not represented), the Tribunal may invite its counsel to make submissions from a particular perspective (normally the perspective of the party or parties whose interests are not otherwise represented)."

133. This description was accepted and endorsed by the IPT.

#### *4.* R (on the application of Privacy International) v. Investigatory Powers Tribunal and others *[2019] UKSC 22*

134. In this judgment, which was handed down on 15 May 2019, the Supreme Court held that section 67(8) RIPA did not preclude judicial review of a decision of the IPT.

### E. Oversight

135. Part IV of RIPA provided for the appointment by the Prime Minister of an Interception of Communications Commissioner ("the IC

Commissioner") and an Intelligence Services Commissioner charged with supervising the activities of the intelligence services.

136. The IC Commissioner was responsible for keeping under review the interception of communications and the acquisition and disclosure of communications data by intelligence services, police forces and other public authorities. In undertaking his review of surveillance practices, the IC Commissioner and his inspectors had access to all relevant documents, including closed materials, and all those involved in interception activities had a duty to disclose to him any material he required. The obligation on intercepting agencies to keep records ensured that the IC Commissioner had effective access to details of surveillance activities undertaken. After each inspection a report was sent to the head of the public authority which contained formal recommendations and which required the public authority to report back within two months to confirm whether the recommendations had been implemented or what progress had been made. The Commissioner reported to the Prime Minister on a half-yearly basis with respect to the carrying out of his functions and prepared an annual report. This report was a public document (subject to the non-disclosure of confidential annexes) which was laid before Parliament.

137. The Intelligence Services Commissioner provided further independent external oversight of the use of the intrusive powers of the intelligence services and parts of the Ministry of Defence. He also submitted annual reports to the Prime Minister, which were laid before Parliament.

138. The Investigatory Powers Act 2016 (see paragraphs 183-190 below) repealed these provisions, in so far as they related to England, Scotland and Wales, and in September 2017 the Investigatory Powers Commissioner's Office (IPCO) took over responsibility for the oversight of investigatory powers. IPCO consists of around fifteen Judicial Commissioners, made up of current and recently retired High Court, Court of Appeal and Supreme Court Judges; a technical advisory panel, made up of scientific experts; and almost fifty official staff, including inspectors, lawyers and communications experts.

## F. Reviews of interception operations by the intelligence service

### *1. Intelligence and Security Committee of Parliament: July 2013 Statement on GCHQ's alleged interception of communications under the US PRISM programme*

139. The ISC was originally established by the ISA to examine the policy, administration and expenditure of MI5, MI6 and GCHQ. Since the introduction of the Justice and Security Act 2013, however, the ISC was expressly given the status of a Committee of Parliament; it was provided with greater powers; and its remit was increased to include oversight of operational activity and the wider intelligence and security activities of

government. Under sections 1-4 of the Justice and Security Act 2013, it consisted of nine members drawn from both Houses of Parliament, and, in the exercise of their functions, those members were routinely given access to highly classified material.

140. Following the Edward Snowden revelations, the ISC conducted an investigation into GCHQ's access to the content of communications intercepted under the United States PRISM programme, the legal framework governing access, and the arrangements GCHQ had with its overseas counterpart for sharing information. In the course of the investigation, the ISC took detailed evidence from GCHQ and discussed the programme with the NSA.

141. The ISC concluded that allegations that GCHQ had circumvented United Kingdom law by using the PRISM programme to access the content of private communications were unfounded as GCHQ had complied with its statutory duties contained in the ISA. It further found that in each case in which GCHQ had sought information from the United States, a warrant for interception, signed by a government minister, had already been in place.

*2. Privacy and security: a modern and transparent legal framework*

142. Following its statement in July 2013, the ISC conducted a more in-depth inquiry into the full range of the intelligence services' capabilities. Its report, which contained an unprecedented amount of information about the intelligence services' intrusive capabilities, was published on 12 March 2015.

143. The ISC was satisfied that the United Kingdom's intelligence and security services did not seek to circumvent the law, including the requirements of the Human Rights Act 1998, which governed everything that they did. However, it considered that as the legal framework had developed piecemeal, it was unnecessarily complicated. The ISC therefore had serious concerns about the resulting lack of transparency, which was not in the public interest. Consequently, its key recommendation was that the existing legal framework be replaced by a new Act of Parliament which clearly set out the intrusive powers available to the intelligence services, the purposes for which they could use them, and the authorisation required before they could do so.

144. With regard to GCHQ's bulk interception capability, the inquiry showed that the intelligence services did not have the legal authority, the resources, the technical capability, or the desire to intercept every communication of British citizens, or of the Internet as a whole. GCHQ were not, therefore, reading the emails of everyone in the United Kingdom. On the contrary, GCHQ's bulk interception systems operated on a very small percentage of the bearers that made up the Internet and the ISC was satisfied that GCHQ applied levels of filtering and selection such that only a certain amount of the material on those bearers was collected. Further

targeted searches ensured that only those items believed to be of the highest intelligence value were ever presented for analysts to examine, with the consequence that only a tiny fraction of those collected were ever seen by human eyes.

145. In respect of Internet communications, the ISC considered that the distinction between "internal" and "external" communications was confusing and lacked transparency. It therefore suggested that the government publish an explanation of which Internet communications fell under which category. Nevertheless, the inquiry had established that bulk interception could not be used to target the communications of an individual in the United Kingdom without a specific authorisation, signed by a Secretary of State, naming that individual.

146. The ISC observed that the section 8(4) warrant was very brief. In so far as the accompanying certificate set out the categories of communications which might be examined, those categories were expressed in very general terms (for example, "material providing intelligence on terrorism (as defined by the Terrorism Act 2000 (as amended)), including, but not limited to, terrorist organisations, terrorists, active sympathisers, attack planning, fund-raising"). Given that the certificate was so generic, the ISC questioned whether it needed to be secret or whether, in the interests of transparency, it could be published.

147. Although the section 8(4) certificate set out the general categories of information which could be examined, the ISC found that in practice it was the selection of the bearers and the application of simple selectors and search criteria which determined what communications were examined. The ISC had therefore sought assurances that these were subject to scrutiny and review by Ministers and/or the Commissioners. However, the evidence before the ISC indicated that neither Ministers nor the Commissioners had any significant visibility of these issues. The ISC therefore recommended that the IC Commissioner should be given statutory responsibility to review the various selection criteria used in bulk interception to ensure that they followed directly from the certificate and valid national security requirements.

148. The ISC noted that communications data were central to most intelligence services' investigations: they could be analysed to find patterns that reflected particular online behaviours associated with activities such as attack planning, to establish links, to help focus on individuals who might pose a threat, to ensure that interception was properly targeted, and to illuminate networks and associations relatively quickly. They were particularly useful in the early stages of an investigation, when the intelligence services had to be able to determine whether those associating with a target were connected to the plot (and therefore required further investigation) or were innocent bystanders. According to the Secretary of State for the Home Department, they had "played a significant role in every

Security Service counter-terrorism operation over the last decade". Nevertheless, the ISC expressed concern about the definition of "communications data". While it accepted that there was a category of communications data which was less intrusive than content, and therefore did not require the same degree of protection, it considered that there existed certain categories of communications data which had the potential to reveal more intrusive details about a person's private life and, therefore, required greater safeguards.

149. Lastly, with regard to the IPT, the ISC expressly recognised the importance of a domestic right of appeal.

### 3. *"A Question of Trust": Report of the Investigatory Powers Review by the Independent Reviewer of Terrorism Legislation ("the Anderson Report")*

150. The Independent Reviewer of Terrorism Legislation is a person wholly independent of government, appointed by the Home Secretary and by the Treasury for a renewable three-year term. He is tasked with reporting to the Home Secretary and to Parliament on the operation of counter-terrorism law in the United Kingdom. These reports are laid before Parliament to inform the public and political debate.

151. The purpose of the Anderson Report, which was both laid before Parliament and published on 11 June 2015, and which was named after David Anderson QC, the then Independent Reviewer of Terrorism Legislation, was to inform the public and political debate on the threats to the United Kingdom, the capabilities required to combat those threats, the safeguards in place to protect privacy, the challenges of changing technology, issues relating to transparency and oversight, and the case for new or amended legislation. In conducting the review the Independent Reviewer had unrestricted access, at the highest level of security clearance, to the responsible government departments and public authorities. He also engaged with service providers, independent technical experts, NGOs, academics, lawyers, judges and regulators.

152. The Independent Reviewer had noted that the statutory framework governing investigatory powers had "developed in a piecemeal fashion", with the consequence that there were "few [laws] more impenetrable than RIPA and its satellites".

153. With regard to the importance of communications data, he observed that they enabled the intelligence services to build a picture of a subject of interest's activities and were extremely important in providing information about criminal and terrorist activity. They identified targets for further work and also helped to determine if someone was completely innocent. Of central importance was the ability to use communications data (subject to necessity and proportionality) for:

(a) linking an individual to an account or action (for example, visiting a website or sending an email) through IP resolution;

(b) establishing a person's whereabouts, traditionally via cell site or GPRS data;

(c) establishing how suspects or victims were communicating (that is, via which applications or services);

(d) observing online criminality (for example, which websites were being visited for the purposes of terrorism, child sexual exploitation or purchases of firearms or illegal drugs); and

(e) exploiting data (for example, to identify where, when and with whom or what someone was communicating, how malware or a denial of service attack was delivered, and to corroborate other evidence).

154. Moreover, analysis of communications data could be performed speedily, making them extremely useful in fast-moving operations, and use of communications data could either build a case for using a more intrusive measure, or deliver the information that would make other measures unnecessary.

155. The Independent Reviewer's proposals for reform can be summarised as follows:

(a) the drafting of a comprehensive and comprehensible new law, replacing "the multitude of current powers" and providing clear limits and safeguards on any intrusive power it might be necessary for public authorities to use;

(b) the review and clarification of the definitions of "content" and "communications data";

(c) the retention of the capability of the security and intelligence services to practice bulk collection of intercepted material and associated communications data, but only subject to strict additional safeguards including the authorisation of all warrants by a Judicial Commissioner at a new Independent Surveillance and Intelligence Commission;

(d) the spelling out in the accompanying certificate of the purposes for which material or data were sought by reference to specific operations or mission purposes (for example, "attack planning by ISIL in Iraq/Syria against the UK");

(e) the creation of a new form of bulk warrant limited to the acquisition of communications data which could be a proportionate option in certain cases;

(f) the Independent Surveillance and Intelligence Commission should take over intelligence oversight functions and should be public-facing, transparent and accessible to the media; and

(g) the IPT should have the capacity to make declarations of incompatibility and its rulings should be subject to appeals on points of law.

*4. "A Democratic Licence to Operate": report of the Independent Surveillance Review*

156. The Independent Surveillance Review (ISR) was carried out by a panel supervised by the Royal United Services Institute, an independent think-tank. The ISR was established at the request of the then deputy Prime Minister, partly in response to the revelations by Edward Snowden. Its terms of reference were to look at the legality of United Kingdom surveillance programmes and the effectiveness of the regimes that governed them, and to suggest reforms which might be necessary to protect both individual privacy and the necessary capabilities of the police and security and intelligence services.

157. Having completed its review, the ISR panel found no evidence that the British government was knowingly acting illegally in intercepting private communications, or that the ability to collect data in bulk was being used by the government to provide it with a perpetual window into the private lives of British citizens. On the other hand, the panel found evidence that the existing legal framework authorising the interception of communications was unclear, had not kept pace with developments in communications technology, and did not serve either the government or members of the public satisfactorily. It therefore concluded that a new, comprehensive and clearer legal framework was required.

158. In particular, the ISR panel supported the view set out in both the ISC and the Anderson Report that while the current surveillance powers were needed, both a new legislative framework and oversight regime were required. The panel further considered that the definitions of "content" and "communications data" should be reviewed as part of the drafting of the new legislation so that they could be delineated clearly in law.

159. With regard to communications data, it was noted in the report that greater volumes were available on an individual relative to content, because every piece of content was surrounded by multiple pieces of communications data. Furthermore, aggregating data sets could create an extremely accurate picture of an individual's life since, given enough raw data, algorithms and powerful computers could generate a substantial picture of the individual and his or her patterns of behaviour without ever accessing content. In addition, the use of increasingly sophisticated encryption methods had made content increasingly difficult to access.

160. The ISR panel further considered that the capability of the security and intelligence services to collect and analyse intercepted material in bulk should be maintained, but with the stronger safeguards recommended in the Anderson Report. In particular, the panel agreed that warrants for bulk interception should include much more detail and should be the subject of a judicial authorisation process, save for when there was an urgent requirement.

161. In addition, the ISR panel agreed with both the ISC and the Anderson Report that there should be different types of warrant for the interception and acquisition of communications and related data. It was proposed that warrants for a purpose relating to the detection or prevention of serious and organised crime should always be authorised by a Judicial Commissioner, while warrants for purposes relating to national security should be authorised by the Secretary of State subject to judicial review by a Judicial Commissioner.

162. With regard to the IPT, the panel recommended open public hearings, except where it was satisfied private or closed hearings were necessary in the interests of justice or other identifiable public interest. Furthermore, the IPT should have the ability to test secret evidence put before it, possibly through the appointment of Special Counsel. Lastly, the ISR panel agreed with the ISC and the Anderson Report that a domestic right of appeal was important and should be considered in future legislation.

*5. Report of the Bulk Powers Review*

163. The bulk powers review was set up in May 2016 to evaluate the operational case for the four bulk powers contained in what was then the Investigatory Powers Bill (now the Investigatory Powers Act 2016 – see paragraphs 183-190 below). Those powers related to bulk interception and the bulk acquisition of communications data, bulk equipment interference and the acquisition of bulk personal datasets.

164. The review was again carried out by the Independent Reviewer of Terrorism Legislation. To conduct the review he recruited three team members, all of whom had the necessary security clearance to access very highly classified material, including a person with the necessary technical background to understand the systems and techniques used by GCHQ, and the uses to which they could be put; an investigator with experience as a user of secret intelligence, including intelligence generated by GCHQ; and senior independent counsel with the skills and experience to challenge forensically the evidence and the case studies presented by the security and intelligence services.

165. In conducting their review, the team had significant and detailed contact with the intelligence services at all levels of seniority as well as the relevant oversight bodies (including the IPT and Counsel to the Tribunal), NGOs and independent technical experts.

166. Although the review was of the Investigatory Powers Bill, a number of its findings in respect of bulk interception were relevant to the case at hand. In particular, having examined a great deal of closed material, the review concluded that bulk interception was an essential capability: first, because terrorists, criminal and hostile foreign intelligence services had become increasingly sophisticated at evading detection by traditional means; and secondly, because the nature of the global Internet meant that

the route a particular communication would travel had become hugely unpredictable. The review team looked at alternatives to bulk interception (including targeted interception, the use of human sources and commercial cyberdefence products) but concluded that no alternative or combination of alternatives would be sufficient to substitute for the bulk interception power as a method of obtaining the necessary intelligence.

*6. Attacks in London and Manchester March-June 2017: independent assessment of MI5 and police internal reviews*

167. Following a series of four terrorist attacks in the short period between March and June 2017, in the course of which some thirty-six innocent people were killed and almost 200 more were injured, the Home Secretary asked the recently retired Independent Reviewer of Terrorism Legislation, David Anderson QC, to assess the classified internal reviews of the police and intelligence services involved. In placing the attacks in context, the Report made the following observations:

> "1.4 First, the ***threat level*** in the UK from so-called 'international terrorism' (in practice, Islamist terrorism whether generated at home or abroad) has been assessed by the Joint Terrorism Analysis Centre (JTAC) as SEVERE since August 2014, indicating that Islamist terrorist attacks in the UK are 'highly likely'. Commentators with access to the relevant intelligence have always been clear that this assessment is realistic. They have pointed also to the smaller but still deadly threat from extreme right wing (XRW) terrorism, exemplified by the murder of Jo Cox MP in June 2016 and by the proscription of the neo-Nazi group National Action in December 2016.
>
> 1.5 Secondly, the ***growing scale*** of the threat from Islamist terrorism is striking. The Director General of MI5, Andrew Parker, spoke in October 2017 of 'a dramatic upshift in the threat this year' to 'the highest tempo I've seen in my 34 year career'. Though deaths from Islamist terrorism occur overwhelmingly in Africa, the Middle East and South Asia, the threat has grown recently across the western world, and has been described as 'especially diffuse and diverse in the UK'. It remains to be seen how this trend will be affected, for good or ill, by the physical collapse of the so-called Islamic State in Syria and Iraq.
>
> 1.6 Thirdly, the profiles of the ***attackers*** ... display many familiar features. ...
>
> 1.7 Fourthly, though the ***targets*** of the first three attacks did not extend to the whole of the current range, they had strong similarities to the targets of other recent western attacks: political centres (e.g. Oslo 2011, Ottawa 2014, Brussels 2016); concert-goers, revellers and crowds (e.g. Orlando 2016, Paris 2016, Barcelona 2017); and police officers (e.g. Melbourne 2014, Berlin 2015, Charleroi 2016). There are precedents also for attacks on observant Muslims which have crossed the boundary from hate crime to terrorism, including the killing of Mohammed Saleem in the West Midlands in 2013.
>
> 1.8 Fifthly, the ***modus operandi*** (MO) of terrorist attacks has diversified and simplified over the years, as Daesh has employed its formidable propaganda effort to inspire rather than to direct acts of terrorism in the west. The attacks under review were typical in style for their time and place:

(a) Unlike the large, directed Islamist plots characteristic of the last decade, all four attacks were committed by ***lone actors*** or ***small groups***, with little evidence of detailed planning or precise targeting.

(b) Strong gun controls in the UK mean that ***bladed weapons*** are more commonly used than firearms in gang-related and terrorist crime.

(c) Since a truck killed 86 innocent people in Nice (July 2016), ***vehicles*** – which featured in three of the four attacks under review – have been increasingly used as weapons.

(d) The ***combination*** of a vehicle and bladed weapons, seen at Westminster and London Bridge, had previously been used to kill the soldier Lee Rigby (Woolwich, 2013).

(e) ***Explosives***, used in Manchester, were the most popular weapon for Islamist terrorists targeting Europe between 2014 and 2017. The explosive TATP has proved to be capable of manufacture (aided by on-line purchases and assembly instructions) more easily than was once assumed."

### *7. Annual Report of the Interception of Communications Commissioner for 2016*

168. The IC Commissioner observed that when conducting interception under a section 8(4) warrant, an intercepting agency had to use its knowledge of the way in which international communications were routed, combined with regular surveys of relevant communications links, to identify those individual communications bearers that were most likely to contain external communications that would meet the descriptions of material certified by the Secretary of State under section 8(4). It also had to conduct the interception in ways that limited the collection of non-external communications to the minimum level compatible with the objective of intercepting the wanted external communications.

169. He further observed that prior to analysts being able to read, look at or listen to material, they had to provide a justification, which included why access to the material was required, consistent with, and pursuant to section 16 and the applicable certificate, and why such access was proportionate. Inspections and audits showed that although the selection procedure was carefully and conscientiously undertaken, it relied on the professional judgment of analysts, their training and management oversight.

170. According to the report, 3,007 interception warrants were issued in 2016 and five applications were refused by a Secretary of State. In the view of the IC Commissioner, these figures did not capture the critical quality assurance function initially carried out by the staff and lawyers within the intercepting agency or the warrant-granting department (the warrant-granting departments were a source of independent advice to the Secretary of State and performed pre-authorisation scrutiny of warrant applications and renewals to ensure that they were (and remained) necessary and proportionate). Based on his inspections, he was confident that the low

number of rejections reflected the careful consideration given to the use of these powers.

171. A typical inspection of an interception agency included the following:

(a) a review of the action points or recommendations from the previous inspection and their implementation;

(b) an evaluation of the systems in place for the interception of communications to ensure they were sufficient for the purposes of Chapter 1 of Part 1 of RIPA and that all relevant records had been kept;

(c) the examination of selected interception applications to assess whether they were necessary in the first instance and whether the requests met the necessity and proportionality requirements;

(d) interviews with case officers, analysts and/or linguists from selected investigations or operations to assess whether the interception and the justifications for acquiring all of the material were proportionate;

(e) the examination of any urgent oral approvals to check that the process was justified and used appropriately;

(f) a review of those cases where communications subject to legal privilege or otherwise confidential information had been intercepted and retained, and any cases where a lawyer was the subject of an investigation;

(g) a review of the adequacy of the safeguards and arrangements under sections 15 and 16 RIPA;

(h) an investigation of the procedures in place for the retention, storage and destruction of intercepted material and related communications data; and

(i) a review of the errors reported, including checking that the measures put in place to prevent recurrence were sufficient.

172. After each inspection, inspectors produced a report, including:

(a) an assessment of how far the recommendations from the previous inspection had been achieved;

(b) a summary of the number and type of interception documents selected for inspection, including a detailed list of those warrants;

(c) detailed comments on all warrants selected for further examination and discussion during the inspection;

(d) an assessment of the errors reported to the IC Commissioner's office during the inspection period;

(e) an account of the examination of the retention, storage and destruction procedures;

(f) an account of other policy or operational issues which the agency or warrant-granting departments raised during the inspection;

(g) an assessment of how any material subject to legal professional privilege (or otherwise confidential material) had been handled; and

(h) a number of recommendations aimed at improving compliance and performance.

173. During 2016, the IC Commissioner's office inspected all nine interception agencies once and the four main warrant-granting departments twice. This, together with extra visits to GCHQ, made a total of twenty-two inspection visits. In addition, he and his inspectors arranged other *ad hoc* visits to agencies.

174. Inspection of the systems in place for applying for and authorising interception warrants usually involved a three-stage process. First, to achieve a representative sample of warrants, inspectors selected them across different crime types and national security threats. In addition, inspectors focussed on those of particular interest or sensitivity (such as those which gave rise to an unusual degree of collateral intrusion, those which had been extant for a considerable period, those which were approved orally, those which resulted in the interception of legal or otherwise confidential communications, and so-called "thematic" warrants). Secondly, inspectors scrutinised the selected warrants and associated documentation in detail during reading days which preceded the inspections. At this stage, inspectors were able to examine the necessity and proportionality statements made by analysts when adding a selector to the collection system for examination. Each statement had to stand on its own and had to refer to the overall requirement of priorities for intelligence collection. Thirdly, they identified those warrants, operations or areas of the process which required further information or clarification and arranged to interview relevant operational, legal or technical staff. Where necessary, they examined further documentation or systems relating to those warrants.

175. A total of 970 warrants were examined during the twenty-two interception inspections (61% of the number of warrants in force at the end of the year and 32% of the total of new warrants issued in 2016).

176. Retention periods were not prescribed by legislation, but the agencies had to consider section 15(3) RIPA, which provided that the material or data had to be destroyed as soon as retaining them was no longer necessary for any of the authorised purposes in section 15(4). According to the report, every interception agency had a different view on what constituted an appropriate retention period for intercepted material and related communications data. The retention periods therefore differed within the interception agencies; for content, they ranged between thirty days and one year, and for related communications data, they ranged between six months and one year. In practice, however, the vast majority of content was reviewed and automatically deleted after a very short period of time unless specific action was taken to retain the content for longer because it was necessary to do so.

177. The IC Commissioner expressly noted that he "was impressed by the quality" of the necessity and proportionality statements made by analysts when adding a selector to the collection system for examination.

178. Inspectors made a total of twenty-eight recommendations in their inspection reports, eighteen of which were made in relation to the application process. The majority of the recommendations in this category related to the necessity, proportionality and/or collateral intrusion justifications in the applications, or to the handling of legally privileged or otherwise confidential material relating to sensitive professions.

179. The total number of interception errors reported to the IC Commissioner during 2016 was 108. Key causes of interception errors were over-collection (generally technical software or hardware errors that caused over-collection of intercepted material and related communications data), unauthorised selection/examination, incorrect dissemination, the failure to cancel interception, and the interception of either an incorrect communications address or person.

180. Lastly, with regard to intelligence sharing, the IC Commissioner noted that:

> "GCHQ provided comprehensive details of the sharing arrangements whereby Five Eyes partners can access elements of the product of GCHQ's interception warrants on their own systems. My inspectors also met representatives of the Five Eyes community and received a demonstration of how other Five Eyes members can request access to GCHQ's data. Access to GCHQ systems is tightly controlled and has to be justified in accordance with the laws of the host country and handling instructions of section 15/16 safeguards. Before getting any access to GCHQ data, Five Eyes analysts must complete the same legalities training as GCHQ staff."

### *8. Annual report of the Intelligence Services Commissioner for 2016*

181. The Intelligence Services Commissioner, in his report on compliance with the "Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the Passing and Receipt of Intelligence Relating to Detainees", observed that

> "In the course of their work, each of the agencies works closely with foreign liaison partners. This involves routine intelligence sharing and at times collaborative operations. I am satisfied that the agencies are sensitive to the implications of working with partners acting under different legal systems and note that [the United Kingdom Intelligence Community] working overseas are careful to apply the principles of UK law as far as possible.
>
> ...
>
> GCHQ works closely with liaison partners and is involved in regular intelligence sharing and at times collaborative work. This is a complex area for both GCHQ and SIS, where agency staff work with partners who are applying different and sometimes incompatible legal frameworks. I have been impressed by the efforts of GCHQ's staff to gain assurances from partners, particularly with regard to the consolidated guidance. I have recommended that GCHQ should consider making reference in relevant submissions to the fact of local laws which will affect any partner's activity.

> I was satisfied that GCHQ is applying the principles of the consolidated guidance sensitively, and am pleased that changes made to the training for 24/7 staff are raising the already high standard of the referrals process. I noted that on occasion GCHQ officers updated the consolidated guidance log after the fact to clarify judgements or details. While it is important to represent the fullest available facts, I recommended that GCHQ should set out points of clarification in addition to and not amendment to the original log entry. GCHQ subsequently confirmed that this has been implemented.
>
> ...
>
> The Foreign Secretary is also responsible for providing ministerial oversight on occasions where the consolidated guidance has been engaged and the agencies intend to proceed, either with intelligence sharing or a live operation. I have recommended that the [Foreign and Commonwealth Office] should obtain a copy of any assurances that SIS have obtained from a liaison partner. I would advise that these should be made available for the Foreign Secretary to scrutinise while considering any consolidated guidance-related submissions."

182. Oversight of compliance with the Consolidated Guidance now falls under the remit of the new Investigatory Powers Commissioner. The Guidance is currently being reviewed since the Intelligence Services Commissioner, in his 2015 report, indicated that while he did "not think that the Consolidated Guidance was fundamentally defective or not fit for purpose", he nevertheless expressed the view that it had been "in operation in its current form for some years and that there was room for improvement".

## G. Investigatory Powers Act 2016

183. The Investigatory Powers Act 2016 ("the IPA") received Royal Assent on 29 November 2016. The new regime which it introduced is now largely operational, with the majority of the powers under the Act having been brought into force in the course of 2018.

184. Under the IPA a bulk interception warrant, which may cover both the "content" of communications and "secondary data", has to be necessary at least in the interests of national security (but may also be for the purpose of preventing or detecting serious crime or in the interests of the economic well-being of the United Kingdom in so far as those interests are also relevant to national security). The warrant must specify the "operational purposes" for which any material obtained under that warrant may be selected for examination. There are detailed provisions about the making of the list of "operational purposes" by the heads of the intelligence services. An operational purpose may be specified in that list only with the approval of the Secretary of State. The list of operational purposes must be provided to the ISC every three months and must be reviewed by the Prime Minister at least once a year.

185. An application for a bulk warrant must be made by or on behalf of the head of an intelligence service. The power to issue a warrant must be

exercised by the Secretary of State personally and in deciding whether to issue a bulk warrant he or she must apply the principles of necessity and proportionality. The issuing of the warrant is subject to prior approval by a Judicial Commissioner, who must apply the principles of judicial review (the so-called "double-lock"). The Judicial Commissioner must therefore consider for himself or herself questions such as whether an interference is justified as being proportionate under Article 8 § 2 of the Convention.

186. The warrant lasts for six months unless it has already been cancelled or renewed. Renewal is subject to approval by a Judicial Commissioner.

187. The "main purpose" of the warrant must be to obtain "overseas-related communications", being communications sent to or received by individuals outside the British Islands. Selection for examination of intercepted content or "protected material" is subject to the "British Islands safeguard", meaning that it may not at any time be selected for examination if any criteria used for the selection of the intercepted content for examination are referable to an individual known to be in the British Islands at that time, and the purpose of using those criteria is to identify the content of communications sent by, or intended for, that individual.

188. The IPA also created a right of appeal from the IPT and replaced the Interception of Communications Commissioner with a new Investigatory Powers Commissioner (see paragraph 138 above).

189. A series of new Codes of Practice, including a new IC Code, entered into force on 8 March 2018 (see paragraph 102 above).

190. Part 4 of the IPA, which came into force on 30 December 2016, included a power to issue "retention notices" to telecommunications operators requiring the retention of data. Following a legal challenge by Liberty, the Government conceded that Part 4 of the IPA was, in its existing form, inconsistent with the requirements of EU law. Part 4 was not amended and on 27 April 2018 the High Court found Part 4 to be incompatible with fundamental rights in EU law since, in the area of criminal justice, access to retained data was not limited to the purpose of combating "serious crime"; and access to retained data was not subject to prior review by a court or an independent administrative body.

## II. RELEVANT INTERNATIONAL LAW

### A. United Nations

191. Resolution no. 68/167, adopted by the General Assembly on 18 December 2013, reads as follows:

> "The General Assembly,
>
> ...

4. *Calls upon* all States:

...

(*c*) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law;

(*d*) To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data ..."

## B. Council of Europe

### *1. Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981*

192. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, which entered into force in respect of the United Kingdom on 1 December 1987, sets out standards for data protection in the sphere of automatic processing of personal data in the public and private sectors. It provides in its relevant parts as follows:

**Preamble**

"The member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms;

Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing;

Reaffirming at the same time their commitment to freedom of information regardless of frontiers;

Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows:"

**Article 1 – Object and purpose**

"The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ('data protection')."

...

**Article 8 – Additional safeguards for the data subject**

"Any person shall be enabled:

a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;

b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention;

d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with."

**Article 9 – Exceptions and restrictions**

"1. No exception to the provisions of Articles 5, 6 and 8 of this Convention shall be allowed except within the limits defined in this article.

2. Derogation from the provisions of Articles 5, 6 and 8 of this Convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of:

a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences;

b. protecting the data subject or the rights and freedoms of others.

..."

**Article 10 – Sanctions and remedies**

"Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter."

193. The Explanatory Report to the above-mentioned Convention explains that:

**Article 9 – Exceptions and restrictions**

"55. Exceptions to the basic principles for data protection are limited to those which are necessary for the protection of fundamental values in a democratic society. The text of the second paragraph of this article has been modelled after that of the second paragraphs of Articles 6, 8, 10 and 11 of the European Human Rights Convention. It is clear from the decisions of the Commission and the Court of Human Rights relating to the concept of 'necessary measures' that the criteria for this concept cannot be laid down for all countries and all times, but should be considered in the light of the given situation in each country.

56. Littera a in paragraph 2 lists the major interests of the State which may require exceptions. These exceptions are very specific in order to avoid that, with regard to the general application of the convention, States would have an unduly wide leeway.

States retain, under Article 16, the possibility to refuse application of the convention in individual cases for important reasons, which include those enumerated in Article 9.

The notion of 'State security' should be understood in the traditional sense of protecting national sovereignty against internal or external threats, including the protection of the international relations of the State."

### 2. *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows of 8 November 2001 (ETS 181)*

194. The Protocol, which has not been ratified by the United Kingdom, provides in its relevant parts as follows:

**Article 1 – Supervisory authorities**

"1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol.

2. a. To this end, the said authorities shall have, in particular, powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.

b. Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.

3. The supervisory authorities shall exercise their functions in complete independence.

4. Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts.

..."

**Article 2 – Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention**

"1. Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer.

2. By way of derogation from paragraph 1 of Article 2 of this Protocol, each Party may allow for the transfer of personal data:

a. if domestic law provides for it because of:

– specific interests of the data subject, or

– legitimate prevailing interests, especially important public interests, or

b. if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law."

### *3. Recommendation of the Committee of Ministers on the protection of personal data in the area of telecommunication services*

195. Recommendation (No. R (95) 4 of the Committee of Ministers), which was adopted on 7 February 1995, reads, in so far as relevant, as follows:

> "2.4. Interference by public authorities with the content of a communication, including the use of listening or tapping devices or other means of surveillance or interception of communications, must be carried out only when this is provided for by law and constitutes a necessary measure in a democratic society in the interests of:
>
> a. protecting state security, public safety, the monetary interests of the state or the suppression of criminal offences;
>
> b. protecting the data subject or the rights and freedoms of others.
>
> 2.5. In the case of interference by public authorities with the content of a communication, domestic law should regulate:
>
> a. the exercise of the data subject's rights of access and rectification;
>
> b. in what circumstances the responsible public authorities are entitled to refuse to provide information to the person concerned, or delay providing it;
>
> c. storage or destruction of such data.
>
> If a network operator or service provider is instructed by a public authority to effect an interference, the data so collected should be communicated only to the body designated in the authorisation for that interference."

### *4. 2015 Report of the Venice Commission on the Democratic Oversight of Signals Intelligence Agencies*

196. The European Commission for Democracy through Law (Venice Commission) in its 2015 Report noted, at the outset, the value that bulk interception could have for security operations, since it enabled the security services to adopt a proactive approach, looking for hitherto unknown dangers rather than investigating known ones. However, it also noted that intercepting bulk data in transmission, or requirements that telecommunications companies store and then provide telecommunications content data or metadata to law-enforcement or security agencies, involved an interference with the privacy and other human rights of a large proportion of the population of the world. In this regard, the Venice Commission considered that the main interference with privacy occurred when stored personal data were accessed and/or processed by the agencies. For this reason, the computer analysis (usually with the help of selectors) was one of the important stages for balancing personal integrity concerns against other interests.

197. According to the report, the two most significant safeguards were the authorisation (of collection and access) and the oversight of the process. It was clear from the Court's case-law that the latter had to be performed by

an independent, external body. While the Court had a preference for judicial authorisation, it had not found this to be a necessary requirement. Rather, the system had to be assessed as a whole, and where independent controls were absent at the authorisation stage, particularly strong safeguards had to exist at the oversight stage. In this regard, the Venice Commission considered the example of the system in the United States, where authorisation was given by the FISC. However, despite the existence of judicial authorisation, the lack of independent oversight of the conditions and limitations set by the court was problematic.

198. Similarly, the Commission observed that notification of the subject of surveillance was not an absolute requirement of Article 8 of the Convention, since a general complaints procedure to an independent oversight body could compensate for non-notification.

199. The report also considered internal controls to be a "primary safeguard". Recruitment and training were key issues; in addition, it was important for the agencies to build in respect for privacy and other human rights when promulgating internal rules.

200. The report acknowledged that journalists were a group which required special protection, since searching their contacts could reveal their sources (and the risk of discovery could be a powerful disincentive to whistle-blowers). Nevertheless, it considered there to be no absolute prohibition on searching the contacts of journalists, provided that there were very strong reasons for doing so. According to the report, the journalistic profession was not one which was easily identified, since NGOs were also engaged in building public opinion and even bloggers could claim to be entitled to equivalent protections.

201. Lastly, the report considered briefly the issue of intelligence sharing, and in particular the risk that States could thereby circumvent stronger domestic surveillance procedures and/or any legal limits which their agencies might be subject to as regards domestic intelligence operations. It considered that a suitable safeguard would be to provide that the bulk material transferred could only be searched if all the material requirements of a national search were fulfilled and this was duly authorised in the same way as a search of bulk material obtained by the signals intelligence agency using its own techniques.

## III. EUROPEAN UNION LAW

### A. Charter of Fundamental Rights

202. Articles 7, 8 and 11 of the Charter of Fundamental Rights of the European Union (OJ 2016/C 202/02, p. 389) provide as follows:

**Article 7 – Respect for private and family life**

"Everyone has the right to respect for his or her private and family life, home and communications."

**Article 8 – Protection of personal data**

"1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which have been collected concerning him or her, and the right to have them rectified.

3. Compliance with these rules shall be subject to control by an independent authority."

**Article 11 – Freedom of expression and information**

"1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

2. The freedom and pluralism of the media shall be respected."

## B. EU directives and regulations relating to protection and processing of personal data

203. Directive 95/46/EC on data protection (see paragraph 113 above) regulated for many years the protection and processing of personal data within the European Union. As the activities of member States regarding public safety, defence and State security fell outside the scope of Community law, the Directive did not apply to these activities (Article 3(2)).

204. The General Data Protection Regulation ("GDPR"), adopted in April 2016, superseded the Data Protection Directive and became enforceable on 25 May 2018. The Regulation, which is directly applicable in member States[1], contains provisions and requirements pertaining to the processing of personally identifiable information of data subjects inside the European Union, and applies to all enterprises, regardless of location, doing business with the European Economic Area. Business processes that handle personal data must be built with data protection by design and by default, meaning that personal data must be stored using pseudonymisation or full anonymisation, and use the highest possible privacy settings by default, so that the data are not available publicly without explicit consent, and cannot be used to identify a subject without additional information stored separately. No personal data may be processed unless it is done under a lawful basis specified by the Regulation, or if the data controller or

[1] Before the United Kingdom left the European Union, royal assent was granted to the Data Protection Act 2018 on 23 May 2018, which contains equivalent regulations and protections.

processor has received explicit, opt-in consent from the data's owner. The data owner has the right to revoke this permission at any time.

205. A processor of personal data must clearly disclose any data collection, declare the lawful basis and purpose for data processing, how long data are being retained, and if they are being shared with any third-parties or outside of the European Union. Users have the right to request a portable copy of the data collected by a processor in a common format, and the right to have their data erased under certain circumstances. Public authorities, and businesses whose core activities centre around regular or systematic processing of personal data, are required to employ a data protection officer, who is responsible for managing compliance with the GDPR. Businesses must report any data breaches within seventy-two hours if they have an adverse effect on user privacy.

206. The Privacy and Electronic Communications Directive (Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ 2002 L 201, p. 37), adopted on 12 July 2002, states in its recitals as follows:

> "(2) This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.
>
> ...
>
> (11) Like Directive 95/46/EC, this Directive does not address issues of protection of fundamental rights and freedoms related to activities which are not governed by Community law. Therefore it does not alter the existing balance between the individual's right to privacy and the possibility for Member States to take the measures referred to in Article 15(1) of this Directive, necessary for the protection of public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the enforcement of criminal law. Consequently, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the rulings of the European Court of Human Rights. Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the European Convention for the Protection of Human Rights and Fundamental Freedoms."

207. The Directive further provides in its relevant parts as follows:

**Article 1 – Scope and aim**

> "1. This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law."

**Article 15 – Application of certain provisions of Directive 95/46/EC**

"1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union."

208. On 15 March 2006 the Data Retention Directive (Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ 2006 L 105, p. 54) was adopted. Prior to the judgment of 2014 declaring it invalid (see paragraph 209 below), it had provided in its relevant parts as follows:

**Article 1 – Subject matter and scope**

"1. This Directive aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.

2. This Directive shall apply to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It shall not apply to the content of electronic communications, including information consulted using an electronic communications network."

**Article 3 – Obligation to retain data**

"1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned."

## C. Relevant case-law of the Court of Justice of the European Union

### 1. *Judgment of 8 April 2014 in* Digital Rights Ireland and Others *(C-293/12 and C-594/12, EU:C:2014:238)*

209. In a judgment of 8 April 2014, the Court of Justice of the European Union ("the CJEU") declared invalid the Data Retention Directive laying down the obligation on the providers of publicly available electronic communication services or of public communications networks to retain all traffic and location data for periods from six months to two years, in order to ensure that the data were available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each member State in its national law. The CJEU noted that, even though the directive did not permit the retention of the content of the communication, the traffic and location data covered by it might allow very precise conclusions to be drawn concerning the private lives of the persons whose data had been retained. Accordingly, the obligation to retain the data constituted in itself an interference with the right to respect for private life and communications guaranteed by Article 7 of the Charter of Fundamental Rights of the European Union and the right to protection of personal data under Article 8 of the Charter.

210. The access of the competent national authorities to the data constituted a further interference with those fundamental rights, which the CJEU considered to be "particularly serious". The fact that data were retained and subsequently used without the subscriber or registered user being informed was, according to the CJEU, likely to generate in the minds of the persons concerned the feeling that their private lives were the subject of constant surveillance. The interference satisfied an objective of general interest, namely to contribute to the fight against serious crime and terrorism and thus, ultimately, to public security. However, it failed to satisfy the requirement of proportionality.

211. Firstly, the Directive covered, in a generalised manner, all persons and all means of electronic communication, as well as all traffic data, without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime. It therefore entailed an interference with the fundamental rights of practically the entire European population, according to the CJEU. It applied even to persons for whom there was no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime.

212. Secondly, the Directive did not contain substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use. By simply referring, in a general manner, to serious crime, as defined by each member State in its national law, the directive failed to lay down any objective criterion by which to determine which offences might be considered to be sufficiently serious to justify such

an extensive interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. Above all, the access by the competent national authorities to the data retained was not made dependent on a prior review carried out by a court or by an independent administrative body whose decision sought to limit access to the data and their use to what was strictly necessary for the purpose of attaining the objective pursued.

213. Thirdly, the directive required that all data be retained for a period of at least six months, without any distinction being made between the categories of data on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned. The CJEU concluded that the directive entailed a wide-ranging and particularly serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, without such an interference being precisely circumscribed by provisions to ensure that it was actually limited to what was strictly necessary. The CJEU also noted that the directive did not provide for sufficient safeguards, by means of technical and organisational measures, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of those data.

### 2. *Judgment of 21 December 2016 in* Tele2 Sverige and Watson and Others *(C-203/15 and C-698/15, EU:C:2016:970)*

214. In *Watson and Others*, the applicants had sought judicial review of the legality of section 1 of the Data Retention and Investigatory Powers Act 2014 ("DRIPA"), pursuant to which the Secretary of State could require a public telecommunications operator to retain relevant communications data if he or she considered it necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (h) of section 22(2) RIPA. The applicants claimed, *inter alia*, that section 1 DRIPA was incompatible with Articles 7 and 8 of the Charter and Article 8 of the Convention.

215. On 17 July 2015, the High Court held that the *Digital Rights Ireland and Others* judgment laid down "mandatory requirements of EU law" applicable to the legislation of member States on the retention of communications data and access to such data. Since the CJEU, in that judgment, held that the Data Retention Directive was incompatible with the principle of proportionality, national legislation containing the same provisions as that directive could, equally, not be compatible with that principle. In fact, it followed from the underlying logic of the *Digital Rights Ireland and Others* judgment that legislation that established a general body of rules for the retention of communications data was in breach of the rights guaranteed in Articles 7 and 8 of the Charter, unless that legislation was complemented by a body of rules for access to the data, defined by national law, which provided sufficient safeguards to protect those rights. Accordingly, section 1 DRIPA was not compatible with Articles 7 and 8 of the Charter as it did not lay down clear and precise rules providing for

access to and use of retained data, and access to those data was not made dependent on prior review by a court or an independent administrative body.

216. On appeal by the Secretary of State, the Court of Appeal sought a preliminary ruling from the CJEU.

217. Before the CJEU this case was joined with the request for a preliminary ruling from the Kammarrätten i Stockholm in Case C-203/15 (*Tele2 Sverige*). Following an oral hearing in which some fifteen EU member States intervened, the CJEU gave judgment on 21 December 2016. It held that Article 15(1) of the Privacy and Electronic Communications Directive, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, had to be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, was not restricted solely to fighting serious crime, where access was not subject to prior review by a court or an independent administrative authority, and where there was no requirement that the data concerned should be retained within the European Union.

218. The CJEU declared the Court of Appeal's question whether the protection afforded by Articles 7 and 8 of the Charter was wider than that guaranteed by Article 8 of the Convention inadmissible.

219. Following the handing down of the CJEU's judgment, the case was relisted before the Court of Appeal, which on 31 January 2018 granted declaratory relief in the following terms: that section 1 DRIPA was inconsistent with EU law to the extent that it permitted access to retained data where the object pursued by access was not restricted solely to fighting serious crime; or where access was not subject to prior review by a court or independent administrative authority.

### 3. *Judgment of 2 October 2018 in* Ministerio Fiscal *(C-207/16, EU:C:2018:788)*

220. This request for a preliminary ruling arose after Spanish police, in the course of investigating the theft of a wallet and mobile phone, asked the investigating magistrate to grant them access to data identifying the users of telephone numbers activated with the stolen telephone during a period of twelve days prior to the theft. The investigating magistrate rejected the request on the ground, *inter alia*, that the acts giving rise to the criminal investigation did not constitute a "serious" offence. The referring court subsequently sought guidance from the CJEU on fixing the threshold of seriousness of offences above which an interference with fundamental rights, such as competent national authorities' access to personal data retained by providers of electronic communications services, may be justified.

221. On 2 October 2018 the Grand Chamber of the CJEU ruled that Article 15(1) of the Privacy and Electronic Communications Directive, read in the light of Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, had to be interpreted as meaning that the access of public authorities to data for the purpose of identifying the owners of SIM cards activated with a stolen mobile phone, such as the surnames, forenames and, if need be, addresses of the owners, entailed an interference with their fundamental rights which was not sufficiently serious to entail that access being limited, in the area of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime. In particular, it indicated that:

> "In accordance with the principle of proportionality, serious interference can be justified, in areas of prevention, investigation, detection and prosecution of criminal offences, only by the objective of fighting crime which must also be defined as 'serious'.
>
> By contrast, when the interference that such access entails is not serious, that access is capable of being justified by the objective of preventing, investigating, detecting and prosecuting 'criminal offences' generally."

222. It did not consider access to the data which were the subject of the request to be a particularly serious interference because it

> "only enables the SIM card or cards activated with the stolen mobile telephone to be linked, during a specific period, with the identity of the owners of those SIM cards. Without those data being cross-referenced with the data pertaining to the communications with those SIM cards and the location data, those data do not make it possible to ascertain the date, time, duration and recipients of the communications made with the SIM card or cards in question, nor the locations where those communications took place or the frequency of those communications with specific people during a given period. Those data do not therefore allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned".

#### 4. *Judgment of 6 October 2015 in* Schrems *(C-362/14, EU:C:2015:650)*

223. This request for a preliminary ruling arose from a complaint against Facebook Ireland Ltd which was made to the Irish Data Protection Commissioner by Mr Schrems, an Austrian privacy advocate. Mr Schrems challenged the transfer of his data by Facebook Ireland to the United States and the retention of his data on servers located in that country. The Data Protection Commissioner rejected the complaint since, in a decision of 26 July 2000, the European Commission had considered that the United States ensured an adequate level of protection of the personal data transferred ("the Safe Harbour Decision").

224. In its ruling of 6 October 2015, the CJEU held that the existence of a Commission decision finding that a third country ensured an adequate level of protection of the personal data transferred could not eliminate or even reduce the powers available to the national supervisory authorities

under the Charter or Directive 95/46/EC on data protection. Therefore, even if the Commission had adopted a decision, the national supervisory authorities had to be able to examine, with complete independence, whether the transfer of a person's data to a third country complied with the requirements laid down by the Directive.

225. However, only the CJEU could declare a decision of the Commission invalid. In this regard, it noted that the safe harbour scheme was applicable solely to the United States' undertakings which adhered to it, and United States public authorities were not themselves subject to it. Furthermore, national security, public interest and law enforcement requirements of the United States prevailed over the safe harbour scheme, so that the United States' undertakings were bound to disregard, without limitation, the protective rules laid down by the scheme where they conflicted with such requirements. The safe harbour scheme therefore enabled interference by United States public authorities with the fundamental rights of individuals, and the Commission had not, in the Safe Harbour Decision, referred either to the existence, in the United States, of rules intended to limit any such interference, or to the existence of effective legal protection against the interference.

226. As to whether the level of protection in the United States was essentially equivalent to the fundamental rights and freedoms guaranteed within the European Union, the CJEU found that legislation was not limited to what was strictly necessary where it authorised, on a generalised basis, storage of all the personal data of all the persons whose data were transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down for determining the limits of the access of the public authorities to the data and of their subsequent use. Therefore, under EU law legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications had to be regarded as compromising the essence of the fundamental right to respect for private life. Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, compromised the essence of the fundamental right to effective judicial protection.

227. Lastly, the Court found that the Safe Harbour Decision denied the national supervisory authorities their powers where a person called into question whether the decision was compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals. The Commission had not had competence to restrict the national supervisory authorities' powers in that way and, consequently, the CJEU held the Safe Harbour Decision to be invalid.

*5. Judgment of 16 July 2020 in* Facebook Ireland and Schrems *(C-311/18, EU:C:2020:559)*

228. Following the judgment of the CJEU of 6 October 2015, the referring court annulled the rejection of Mr Schrems' complaint and referred that decision back to the Commissioner. In the course of the Commissioner's investigation, Facebook Ireland explained that a large part of personal data were transferred to Facebook Inc. pursuant to the standard data protection clauses set out in the annex to Commission Decision 2010/87/EU, as amended (Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, OJ 2010 L 39, p. 5).

229. Mr Schrems reformulated his complaint, claiming, *inter alia*, that United States law required Facebook Inc. to make the personal data transferred to it available to certain United States authorities, such as the NSA and the Federal Bureau of Investigation. Since those data were used in the context of various monitoring programmes in a manner incompatible with Articles 7, 8 and 47 of the Charter, Decision 2010/87/EU could not justify the transfer of those data to the United States. On this basis, he asked the Commissioner to prohibit or suspend the transfer of his personal data to Facebook Inc.

230. In a draft decision published on 24 May 2016, the Commissioner took the provisional view that the personal data of EU citizens transferred to the United States were likely to be consulted and processed by the United States authorities in a manner incompatible with Articles 7 and 8 of the Charter and that United States law did not provide those citizens with legal remedies compatible with Article 47 of the Charter. The Commissioner found that the standard data protection clauses in the annex to Decision 2010/87/EU were not capable of remedying that defect, since they did not bind the United States authorities.

231. Having considered the United States' intelligence activities under section 702 of the Foreign Intelligence Surveillance Act ("FISA") and Executive Order 12333, the High Court concluded that the United States carried out mass processing of personal data without ensuring a level of protection essentially equivalent to that guaranteed by Articles 7 and 8 of the Charter; and that EU citizens did not have available to them the same remedies as citizens of the United States, with the consequence that United States law did not afford EU citizens a level of protection essentially equivalent to that guaranteed by Article 47 of the Charter. It stayed the proceedings and referred a number of questions to the CJEU for a preliminary ruling. It asked, *inter alia*, whether EU law applied to the transfer of data from a private company in the European Union to a private company in a third country; if so, how the level of protection in the third country should be assessed; and whether the level of protection afforded by

the United States respected the essence of the rights guaranteed by Article 47 of the Charter.

232. In a judgment of 16 July 2020, the CJEU held that the GDPR applied to the transfer of personal data for commercial purposes by an economic operator established in a member State to another economic operator established in a third country, irrespective of whether, at the time of that transfer or thereafter, those data were liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security. Moreover, the appropriate safeguards, enforceable rights and effective legal remedies required by the GDPR had to ensure that data subjects whose personal data were transferred to a third country pursuant to standard data protection clauses were afforded a level of protection essentially equivalent to that guaranteed within the European Union. To that end, the assessment of the level of protection afforded in the context of such a transfer had to take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country.

233. Furthermore, unless there was a valid Commission adequacy decision, the competent supervisory authority was required to suspend or prohibit a transfer of data to a third country if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, the standard data protection clauses adopted by the Commission were not or could not be complied with in that third country and the protection of the data transferred (as required by EU law) could not be ensured by other means.

234. In order for the Commission to adopt an adequacy decision, it had to find, duly stating reasons, that the third country concerned ensured, by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order. In the CJEU's view, the Safe Harbour Decision was invalid. Section 702 FISA did not indicate any limitations on the power it conferred to implement surveillance programmes for the purposes of foreign intelligence or the existence of guarantees for non-US persons potentially targeted by those programmes. In those circumstances, it could not ensure a level of protection essentially equivalent to that guaranteed by the Charter. Furthermore, as regards the monitoring programmes based on Executive Order 12333, it was clear that that order also did not confer rights which were enforceable against the United States authorities in the courts.

*6. Judgments of 6 October 2020 in* Privacy International *(C-623/17, EU:C:2020:790) and in* La Quadrature du Net and Others *(C-511/18, C-512/18 and C-520/18, EU:C:2020:791)*

235. On 8 September 2017 the IPT gave judgment in the case of *Privacy International*, which concerned the acquisition by the intelligence services of bulk communications data under section 94 of the Telecommunications Act 1984 and bulk personal data. The IPT found that, following their avowal, the regimes were compliant with Article 8 of the Convention. However, it identified the following four requirements which appeared to flow from the CJEU judgment in *Watson and Others* (see paragraph 214 above) and which seemed to go beyond the requirements of Article 8 of the Convention: a restriction on non-targeted access to bulk data; a need for prior authorisation (save in cases of validly established emergency) before data could be accessed; provision for subsequent notification of those affected; and the retention of all data within the European Union.

236. On 30 October 2017 the IPT made a request to the CJEU for a preliminary ruling clarifying the extent to which the *Watson* requirements could apply where the bulk acquisition and automated processing techniques were necessary to protect national security. In doing so, it expressed serious concern that if the *Watson* requirements were to apply to measures taken to safeguard national security, they would frustrate them and put the national security of member States at risk. In particular, it noted the benefits of bulk acquisition in the context of national security; the risk that the need for prior authorisation could undermine the intelligence services' ability to tackle the threat to national security; the danger and impracticality of implementing a requirement to give notice in respect of the acquisition or use of a bulk database, especially where national security was at stake; and the impact that an absolute bar on the transfer of data outside the European Union could have on member States' treaty obligations.

237. A public hearing took place on 9 September 2019. The *Privacy International* case was heard together with case C-511/18 (*La Quadrature du Net and Others*), C-512/18 (*French Data Network and Others*) and C-520/18 (*Ordre des barreaux francophones et germanophone and Others*), which also concerned the application of the Privacy and Electronic Communications Directive to activities related to national security and the combating of terrorism. Thirteen States intervened in support of the States concerned.

238. Two separate judgments were handed down on 6 October 2020. In *Privacy International* the CJEU found that national legislation enabling a State authority to require providers of electronic communications services to forward traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security fell within the scope of the Privacy and Electronic Communications Directive. The interpretation of that Directive had to take account of the right to privacy,

guaranteed by Article 7 of the Charter, the right to protection of personal data, guaranteed by Article 8, and the right to freedom of expression, guaranteed by Article 11. Limitations on the exercise of those rights had to be provided for by law, respect the essence of the rights, and be proportionate, necessary, and genuinely meet the objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. Furthermore, limitations on the protection of personal data must apply only in so far as is strictly necessary; and in order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data are affected have sufficient guarantees that data will be protected effectively against the risk of abuse.

239. In the opinion of the CJEU, national legislation requiring providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission – which affected all persons using electronic communications services – exceeded the limits of what was strictly necessary and could not be considered to be justified as required by the Privacy and Electronic Communications Directive read in the light of the Charter.

240. However, in *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18) the CJEU confirmed that while the Privacy and Electronic Communications Directive, read in the light of the Charter, precluded legislative measures which provided for the general and indiscriminate retention of traffic and location data, where a member State was facing a serious threat to national security that proved to be genuine and present or foreseeable, it did not preclude legislative measures requiring service providers to retain, generally and indiscriminately, traffic and location data for a period limited to what was strictly necessary, but which could be extended if the threat persisted. For the purposes of combating serious crime and preventing serious threats to public security, a member State could also provide – if it was limited in time to what was strictly necessary – for the targeted retention of traffic and location data, on the basis of objective and non-discriminatory factors according to the categories of person concerned or using a geographical criterion, or of IP addresses assigned to the source of an Internet connection. It was also open to a member State to carry out a general and indiscriminate retention of data relating to the civil identity of users of means of electronic communication, without the retention being subject to a specific time limit.

241. Furthermore, the Privacy and Electronic Communications Directive, read in the light of the Charter, did not preclude national rules which required providers of electronic communications services to have recourse, first, to the automated analysis and real-time collection of traffic

and location data, and secondly, to the real-time collection of technical data concerning the location of the terminal equipment used, where it was limited to situations in which a member State was facing a serious threat to national security that was genuine and present or foreseeable, and where recourse to such analysis may be the subject of an effective review by a court or independent administrative body whose decision was binding; and where recourse to the real-time collection of traffic and location data was limited to persons in respect of whom there was a valid reason to suspect that they were involved in terrorist activities and was subject to a prior review carried out either by a court or by an independent administrative body whose decision was binding.

## IV. RELEVANT COMPARATIVE LAW AND PRACTICE

### A. Contracting States

242. At least seven Contracting States (Finland, France, Germany, the Netherlands, Sweden, Switzerland and the United Kingdom) officially operate bulk interception regimes over cables and/or the airways.

243. In one additional State (Norway), a draft law is being debated: if adopted, it will also authorise bulk interception.

244. Details of the Swedish system can be found in *Centrum för rättvisa v. Sweden* (no. 35252/08); and details of the German system are set out in paragraphs 247-252 below.

245. As regards intelligence sharing agreements, at least thirty-nine Contracting States have either concluded intelligence sharing agreements with other States, or have the possibility for such agreements. Two expressly prohibit and two expressly permit the State to ask a foreign power to intercept material on their behalf. In the remaining States, the position on this issue is not clear.

246. Finally, in most States the applicable safeguards are broadly the same as for domestic operations, with various restrictions on the use of the received data and in some cases an obligation to destroy them if they became irrelevant.

### B. Judgment of the German Federal Constitutional Court of 19 May 2020 (1 BvR 2835/17)

247. In this judgment, the Federal Constitutional Court considered whether the Federal Intelligence Service's powers to conduct strategic (or "signals") intelligence on foreign telecommunications were in breach of the fundamental rights contained in the Basic Law (*Grundgesetz*).

248. The regime in question involved the interception of both content and related communications data and was aimed only at monitoring foreign

telecommunications outside of German territory. Such surveillance could be carried out for the purpose of gaining information about topics determined by the Federal Government's mandate to be significant for the State's foreign and security policy. It could, however, also be used to target specific individuals. The admissibility and necessity of the orders to conduct such surveillance were controlled by an independent panel. According to the Constitutional Court's judgment, interception was followed by a multi-stage, fully automated filtering and evaluation process. For this purpose, the Federal Intelligence Service used a six-digit number of search terms which were subject to control by an internal sub-unit responsible for ensuring that the link between the search terms employed and the purpose of the data request was explained in a reasonable and comprehensive manner. After the application of the automated filtering process, intercepted material was either deleted or stored and sent for evaluation by an analyst.

249. The sharing of intercept material with foreign intelligence services was accompanied by a cooperation agreement which had to include usage restrictions and assurances to ensure that data were handled and deleted in accordance with the rule of law.

250. The Constitutional Court held that the regime in question was not compliant with the Basic Law. While the court acknowledged the overriding public interest in effective foreign intelligence gathering, it nevertheless considered, *inter alia*, that the regime was not restricted to sufficiently specific purposes; it was not structured in a way that allowed for adequate oversight and control; and various safeguards were lacking, particularly with respect to the protection of journalists, lawyers and other persons whose communications required special confidentiality protection.

251. Regarding the sharing of intelligence obtained through foreign surveillance, the court again found the safeguards to be lacking. In particular, it was not specified with sufficient clarity when weighty interests might justify data transfers. In addition, while the court did not consider it necessary for a recipient State to have comparable rules on the processing of personal data, it nevertheless considered that data could only be transferred abroad if there was an adequate level of data protection and there was no reason to fear that the information would be used to violate fundamental principles of the rule of law. More generally, in the context of intelligence sharing, the court considered that cooperation with foreign States should not be used to undermine domestic safeguards and if the Federal Intelligence Service wished to use search terms provided to it by a foreign intelligence service it should first confirm the existence of the necessary link between the search terms and the purpose of the data request and that the resulting data did not disclose a particular need for confidentiality (for example, because they concerned whistle-blowers or dissidents). Although the court did not exclude the possibility of the bulk transfer of data to foreign

intelligence services, it found that this could not be a continuous process based on a single purpose.

252. Lastly, the court found that the surveillance powers under review also lacked an extensive independent and continual oversight serving to ensure that the law was observed and compensating for the virtual absence of safeguards commonly guaranteed under the rule of law. The legislature had to provide for two different types of oversight, which had also to be reflected in the organisational framework: firstly, a body resembling a court, tasked with conducting oversight and deciding in a formal procedure providing *ex ante* or *ex post* legal protection; and secondly, an oversight that was administrative in nature and could, on its own initiative, randomly scrutinise the entire process of strategic surveillance as to its lawfulness. In the Constitutional Court's view, certain key procedural steps would, in principle, require *ex ante* authorisation by a body resembling a court, namely: the formal determination of the various surveillance measures (exemptions in cases of urgency were not ruled out); the use of search terms, in so far as these directly targeted individuals who might pose a danger and were thus of direct interest to the Federal Intelligence Service; the use of search terms that directly targeted individuals whose communications required special confidentiality protection; and the sharing of the data of journalists, lawyers and other professions meriting special confidentiality protection with foreign intelligence services.

### C. Judgment of the Court of Appeal of The Hague of 14 March 2017

253. A number of individuals and associations argued that the Dutch intelligence and security services were acting unlawfully by receiving data from foreign intelligence and security services, in particular the NSA and GCHQ, which in their view either had obtained or may have obtained the data in an "unauthorised" or "illegal" manner. The plaintiffs did not contend that the activities of the NSA and GCHQ were "unlawful" or "illegal" under domestic law, but rather that the NSA had acted in violation of the International Covenant on Civil and Political Rights (ICCPR) and GCHQ had acted in violation of the Convention. The plaintiffs relied, *inter alia*, on the "Snowden revelations" (see paragraph 12 above).

254. The plaintiffs' claims were dismissed by the District Court of The Hague on 23 July 2014 (ECLI:NL:RBDHA:2014:8966). Their appeal against this judgment was dismissed by the Court of Appeal of The Hague on 14 March 2017 (ECLI:NL:GHDHA:2017:535).

255. The Court of Appeal held that in principle one had to trust that the United States of America and the United Kingdom would comply with their obligations under these treaties. That trust only needed to give way if sufficiently concrete circumstances had come to light for it to be assumed that it was not justified.

256. With respect to the collection of telecommunications data by the NSA, there were no clear indications that the NSA had acted in violation of the ICCPR. In so far as the plaintiffs had sought to argue that the statutory powers underpinning the collection of data were broader than permissible under the ICCPR, they had insufficiently explained in what respect the relevant laws and regulations were inadequate.

257. With respect to the collection of data by GCHQ, the plaintiffs had not in any way substantiated their claim that GCHQ was acting in breach of the Convention.

258. The plaintiffs had therefore failed to demonstrate that the manner in which the NSA and GCHQ operated was, at least in principle, in conflict with the ICCPR and the Convention. While it could not be excluded that in a specific case the NSA or GCHQ, or any other foreign intelligence service, may have collected data in a way that violated the ICCPR or the Convention, the principle of trust prevented this mere possibility from implying that the Dutch intelligence services could not receive data from foreign intelligence services without verifying in each individual case that these data had been obtained without violating the relevant treaty obligations.

259. Lastly, the Court of Appeal admitted that, even if the foreign intelligence services acted within the limits of their statutory powers and treaty obligations, the fact that these statutory powers might be broader than those of the Dutch intelligence services could under certain circumstances raise concerns. For example, it was conceivable that the Dutch intelligence services would be acting contrary to the Intelligence and Security Services Act 2002 (or the spirit of it) if they were systematically or knowingly to receive data from foreign intelligence agencies about Dutch residents, while they could not have gathered these data by virtue of their own powers. In that case, the restrictions imposed on the intelligence services by the 2002 Act could become a dead letter. However, the plaintiffs had not substantiated or offered proof that the Dutch intelligence services systematically or consciously exploited such a discrepancy between Dutch law and foreign law.

260. An appeal on points of law, primarily based on alleged errors in the interpretation of the plaintiffs' claim by the Court of Appeal and on the extent of the burden of substantiation put on them, was dismissed by the *Hoge Raad* (Supreme Court) on 7 September 2018 (ECLI:NL:HR:2018:1434).

### D. United States of America

261. The United States intelligence services operate the Upstream programme, pursuant to section 702 FISA.

262. The Attorney General and Director of National Intelligence make annual certifications authorising surveillance targeting non-US persons reasonably believed to be located outside the United States of America. They do not have to specify to the FISC the particular non-US persons to be targeted, and there is no requirement to demonstrate probable cause to believe that an individual targeted is an agent of a foreign power. Instead, the section 702 certifications identify categories of information to be collected, which have to meet the statutory definition of foreign intelligence information. Authorised certifications have included information concerning international terrorism, and the acquisition of weapons of mass destruction.

263. Pursuant to the authorisation, the NSA, with the compelled assistance of service providers, copies and searches streams of Internet traffic as data flows across the Internet. Both telephone calls and Internet communications are collected. Prior to April 2017 the NSA acquired Internet transactions that were "to", "from", or "about" a tasked selector. A "to" or "from" communication was a communication for which the sender or a recipient was a user of a section 702 tasked selector. An "about" communication was one in which the tasked selector was referenced within the acquired Internet transaction, but the target was not necessarily a participant in the communication. Collection of "about" communications therefore involved searching the content of communications traversing the Internet. However, from April 2017 onwards the NSA have not been acquiring or collecting communications that are merely "about" a target. In addition the NSA stated that, as part of this curtailment, it would delete the vast majority of previously acquired Upstream Internet communications as soon as practicable.

264. Section 702 requires the government to develop targeting and minimisation procedures which are kept under review by the FISC.

265. Executive Order 12333, which was signed in 1981, authorises the collection, retention and dissemination of information obtained in the course of a lawful foreign intelligence, counterintelligence, international narcotics or international terrorism investigation. Surveillance of foreign nationals under Executive Order 12333 is not subject to domestic regulation under FISA. It is not known how much data are collected under Executive Order 12333, relative to those collected under section 702.

## THE LAW

266. Cumulatively, the applicants in the three joined cases complained about the Article 8 and Article 10 compatibility of three discrete regimes: the regime for the bulk interception of communications under section 8(4) of RIPA (see paragraph 19 above); the regime for the receipt of intelligence from foreign intelligence services; and the regime for the acquisition of communications data from CSPs.

267. Before considering each of these regimes in turn, the Grand Chamber will first address a preliminary issue.

## I. PRELIMINARY ISSUE BEFORE THE GRAND CHAMBER

268. According to the Court's settled case-law, the "case" referred to the Grand Chamber necessarily embraces all aspects of the application previously examined by the Chamber in its judgment. The "case" referred to the Grand Chamber is the application as it has been declared admissible, as well as the complaints that have not been declared inadmissible (see *S.M. v. Croatia* [GC], no. 60561/14, § 216, 25 June 2020, and the cases cited therein).

269. The applicants in the present case lodged their complaints in 2013, 2014 and 2015 respectively. Those complaints mostly concerned the State's surveillance activities under RIPA and the related Codes of Practice. The Codes of Practice were subsequently amended. More significantly, the IPA received royal assent on 29 November 2016 and its provisions began to enter into force from December 2016 onwards. The new surveillance regimes set out in the IPA were mostly operational by the summer of 2018. The provisions of Chapter I of Part I of RIPA were repealed in the course of 2018.

270. The Chamber reviewed the Convention compliance of the law in force on the date it examined the admissibility of the applicants' complaints; that is, it considered the law as is stood on 7 November 2017. As this is the "application as it has been declared admissible", the Grand Chamber must similarly limit its examination to the legislative regime as is stood on 7 November 2017. This is apposite, since the legal regimes phased in following the entry into force of the IPA are currently subject to challenge before the domestic courts and it would not be open to the Grand Chamber to examine the new legislation before those courts have first had the opportunity to do so.

271. The applicants have not challenged the Chamber's finding that the IPT afforded an effective remedy for both individual complaints and general complaints concerning the Convention compliance of a surveillance regime, and the Government have not challenged its finding that in the circumstances of the case the applicants had exhausted domestic remedies within the meaning of Article 35 § 1 of the Convention. Neither issue therefore falls to be considered by the Grand Chamber.

# II. BULK INTERCEPTION OF COMMUNICATIONS

## A. Territorial jurisdiction

272. In respect of the section 8(4) regime, the Government raised no objection under Article 1 of the Convention, nor did they suggest that the interception of communications was taking place outside the State's territorial jurisdiction. Moreover, during the hearing before the Grand Chamber the Government expressly confirmed that they had raised no objection on this ground as at least some of the applicants were clearly within the State's territorial jurisdiction. Therefore, for the purposes of the present case, the Court will proceed on the assumption that, in so far as the applicants complain about the section 8(4) regime, the matters complained of fell within the jurisdictional competence of the United Kingdom.

## B. Alleged violation of Article 8 of the Convention

273. The applicants in all three of the joined cases complained that the regime for the bulk interception of communications was incompatible with Article 8 of the Convention, which reads:

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

### *1. The Chamber judgment*

274. The Chamber expressly recognised that States enjoyed a wide margin of appreciation in deciding what type of interception regime was necessary to protect national security, but considered that the discretion afforded to States in operating an interception regime would necessarily be narrower. In this regard, it observed that the Court had identified six "minimum safeguards" which should be set out in law to avoid abuses of power: the nature of offences which may give rise to an interception order, a definition of the categories of people liable to have their communications intercepted, a limit on the duration of interception, the procedure to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties, and the circumstances in which intercepted data may or must be erased or destroyed. These safeguards, which were first set out in *Huvig v. France* (24 April 1990, § 34, Series A no. 176-B) and *Kruslin v. France* (24 April 1990, § 35, Series A no. 176-A), had been applied routinely by the Court in

its case-law on the interception of communications and in two cases specifically concerning the bulk interception of communications (see *Weber and Saravia v. Germany* (dec.), no. 54934/00, ECHR 2006-XI, and *Liberty and Others v. the United Kingdom*, no. 58243/00, 1 July 2008).

275. In the Chamber's view, the decision to operate a bulk interception regime fell within the margin of appreciation afforded to Contracting States. It assessed the operation of the United Kingdom's bulk interception regime by reference to the six minimum safeguards set out in the preceding paragraph. As the first two safeguards did not readily apply to bulk interception, the Chamber reframed these safeguards, considering first, whether the grounds upon which a warrant could be issued were sufficiently clear; secondly, whether domestic law gave citizens an adequate indication of the circumstances in which their communications might be intercepted; and thirdly, whether domestic law gave citizens an adequate indication of the circumstances in which their communications might be selected for examination. In addition, in the light of recent case-law (including *Roman Zakharov v. Russia* [GC], no. 47143/06, ECHR 2015) the Chamber also had regard to the arrangements for supervising the implementation of secret surveillance measures, the existence of notification mechanisms and any remedies provided for by national law.

276. It identified the following two areas of concern in the section 8(4) regime: first, the lack of oversight of the selection of bearers for interception, the selectors used for filtering intercepted communications, and the process by which analysts selected intercepted communications for examination; and secondly, the absence of any real safeguards applicable to the searching and selection for examination of related communications data. In view of the independent oversight provided by the Interception of Communications Commissioner ("the IC Commissioner") and the IPT, and the extensive independent investigations which followed the Edward Snowden revelations, the Chamber was satisfied that the United Kingdom was not abusing its bulk interception powers. Nevertheless, in view of the above-mentioned shortcomings, it held, by a majority, that the bulk interception regime did not meet the "quality of law" requirement and was incapable of keeping the "interference" to what was "necessary in a democratic society".

### *2. The parties' submissions*

#### (a) The applicants

277. The applicants contended that bulk interception was in principle neither necessary nor proportionate within the meaning of Article 8 of the Convention and, as such, did not fall within a State's margin of appreciation. *Szabó and Vissy v. Hungary* (no. 37138/14, 12 January 2016) suggested that a secret surveillance measure had to be "strictly necessary"

for safeguarding democratic institutions and obtaining vital intelligence, and it had not been demonstrated that bulk interception satisfied this test. While it was undoubtedly a useful capability, it was clear from the Court's case-law that not everything that was useful to the intelligence services was permissible in a democratic society (they referred to *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, ECHR 2008).

278. According to the applicants, separate interferences with the Article 8 right to respect for private life and correspondence occurred with the interception of a communication (content and/or related communications data); its storage; its automated processing; and its examination. While they agreed that a "substantial" interference occurred when intercepted communications were examined, they believed it was wrong to suggest that no "meaningful" interference occurred before this point. On the contrary, the Court's case-law indicated that even the storage of personal information by the State amounted to a serious interference with an individual's rights under Article 8 of the Convention (they referred to, for example, *Rotaru v. Romania* [GC], no. 28341/95, ECHR 2000-V, and *S. and Marper*, cited above). This was especially so when the data were subject to automated processing. In fact, as processing power and machine learning advanced rapidly, the storage and electronic processing of data could by itself be highly intrusive, without any underlying content or related communications data being viewed by an individual. In this regard, the applicants contended that, contrary to the "amorphous soup" relied on by the Government (see paragraph 288 below), the collected data were more akin to a "well organised and indexed library in which you can rapidly find anything you want". The availability of automatic processing raised particularly severe privacy concerns and did not, as the Government contended, minimise any intrusion.

279. Should the Grand Chamber consider that the operation of a bulk interception regime was within the State's margin of appreciation, the applicants argued that the section 8(4) regime was not in accordance with the law. First of all, RIPA was unnecessarily complex, a fact acknowledged by all the independent reviewers; so much so, in fact, that the true nature and scope of the surveillance being undertaken had only become clear following the Edward Snowden revelations. Moreover the "below the waterline" arrangements had been established by GCHQ itself; were neither accessible to nor approved by Parliament; were, as a matter of internal policy, subject to change at the executive's will; and were not binding. The applicants therefore argued that they should play no part in the Court's analysis.

280. In assessing foreseeability, the applicants argued that changes in both society and technology had resulted in a need for the Court to update its existing approach – and enhance the necessary safeguards – to ensure that Convention rights remained practical and effective. The Court's

existing jurisprudence on bulk interception derived from the decision in *Weber and Saravia* (cited above), but that decision dated back to 2006, when the world was a different place. Smartphones were basic and had limited functionality; Facebook was used mainly by university students; and Twitter was in its infancy. Today people lived major parts of their lives online, using the Internet to communicate, impart ideas, conduct research, conduct relationships, seek medical advice, keep diaries, arrange travel, listen to music, find their way around and conduct financial transactions. Furthermore, modern technology generated an enormous amount of communications data, which were highly revealing even if the related content was not examined, and which were structured in such a way that computers could process them and search for patterns in them faster and more effectively than similar searches over content. For example, mobile phones constantly generated communications data as they contacted the mobile network, producing a record of the location of the phone, allowing the user's movements to be tracked, and revealing his or her Internet usage.

281. In the applicants' view, the updated and enhanced safeguards should include prior independent judicial authorisation of warrants, the choice of selectors and the selection of intercepted material for examination. In addition, where selectors or search terms referred to a specified individual, there should be objective evidence of reasonable suspicion in relation to that person. Finally, there should also be subsequent notification of any clearly defined surveillance target, where it would not cause substantial harm to the public interest.

282. The applicants identified a number of elements of the United Kingdom's bulk interception regime which they considered to be inadequate. First of all, there was an absence of independent, let alone judicial, authorisation of surveillance. While judicial authorisation might not in itself be a sufficient safeguard against abuse, this did not support the conclusion that it was not a necessary one. In addition, the applicants believed that there should also be independent, if not judicial, approval of the selectors and search terms used by GCHQ. However, neither the bearers to be intercepted nor the strong selectors were listed in the warrant.

283. Secondly, the distinction between internal and external communications was not only poorly defined but also meaningless, with most communications likely to be swept up in the "external" category. In the applicants' opinion, it would have been possible to have provided more meaningful protection to internal communications. For example, in Sweden all internal communications had to be destroyed immediately if they were discovered.

284. Thirdly, there were limited safeguards for the content of communications of persons known to be in the British Islands, and there were virtually no safeguards for their related communications data. GCHQ was able to retain the entirety of related communications data obtained

under the bulk interception regime, subject only to limits on its storage capacity and the maximum retention period. These data – which were extremely intrusive – could be searched according to a factor referable to an individual known to be in the British Islands, without any requirement that the Secretary of State first certify that the search was necessary and proportionate.

285. Fourthly, the regime did not specify, in law and in detail, the purpose for which material could be examined and, according to the ISC (see paragraph 41 above), the description of material in the Secretary of State's certificate was "generic".

286. Lastly, the applicants submitted that the IC Commissioner only provided part-time oversight and, with limited resources, had been insufficient to guarantee meaningful and robust oversight. The effectiveness of the IPT was similarly limited as it could not provide a remedy for the absence of prior judicial authorisation and, in any case, persons had to have some basis for believing that they had been subject to secret surveillance before the IPT would accept their complaint.

**(b) The respondent Government**

287. The Government submitted that the information obtained under the bulk interception regime was critical to the protection of the United Kingdom from national security threats. Not only did it enable them to uncover hitherto unknown threats, but it also allowed them to conduct surveillance on known targets outside their territorial jurisdiction. The unpredictability of the route by which electronic communications were transmitted (and the fact that those communications were broken down into packets which could be transmitted via different routes) meant that in order to obtain even a small proportion of the communications of known targets overseas, it was necessary to intercept all the communications flowing over a selection of bearers. The bulk interception power had been the subject of detailed and repeated consideration by a series of independent bodies in recent years and there was a unanimity of view that there was not "any alternative" ... "or combination of alternatives sufficient to substitute for the bulk interception power". According to the Government, States should rightly be afforded a broad margin of appreciation in judging what systems were necessary to protect the general community from such threats, and in subjecting those systems to scrutiny the Court should take care not to undermine the effectiveness of a means of obtaining life-saving intelligence which could not be gathered in any other way.

288. The Government contended that the interception of communications under the bulk interception regime would only have resulted in a meaningful interference with a person's Article 8 rights if his or her communications were either selected for examination (that is, included on an index of communications from which an analyst could

potentially choose items to inspect) or actually examined by an analyst. His or her rights could not be said to have been infringed to any more than the most minimal degree if a copy of a communication was either discarded in near-real time or held for a few days at most in a general "amorphous soup" of data; in other words, if it was searched using selectors and queries but it was not examined or used. The overwhelming bulk of communications flowing over each intercepted cable could not be "selected for examination", and would therefore have to be discarded.

289. With regard to the necessary safeguards, the Government agreed with the Chamber that it was appropriate to assess a bulk interception regime by reference to the same standards that had been developed by the Court in cases concerning the targeted interception of communications. The Government also largely agreed with the Chamber's assessment of the section 8(4) regime by reference to those standards. They reiterated that there was no possibility of any communications being viewed by an analyst unless and until they had been selected for examination following the automated sifting process; selection and any ensuing examination were very carefully controlled; no intelligence report could be made of any communications or communications data unless they had been viewed by an analyst; section 16(2) RIPA required the Secretary of State to certify the necessity and proportionality of searching the content of communications according to a factor referable to an individual known to be in the British Islands; and the combined oversight functions of the ISC, the IC Commissioner and the IPT satisfied the requirements of the Convention. At all stages of the bulk interception process, the applicable safeguards were built around the Convention concepts of necessity and proportionality. Those fundamental principles governed the obtaining of the material in the first place, its examination, handling, storage, disclosure, retention and deletion.

290. In respect of those aspects of the regime which, according to the Chamber, had not provided adequate safeguards against abuse, the Government provided further clarification. First of all, although they acknowledged that the warrant did not specify the individual bearers to be targeted, as there would be serious impracticalities and difficulties with including this information in the warrant, it nevertheless contained a description of what the interception was going to involve and a description of the sorts of bearers that would be intercepted. The IC Commissioner was briefed regularly by GCHQ about the basis on which bearers were selected for interception.

291. Secondly, they clarified that the choice of selectors was in fact carefully controlled. Whenever a new selector was added to the system, the analyst adding it had to complete a written record, explaining why it was necessary and proportionate to apply the selector for the purposes within the Secretary of State's certificate. This was done by the selection of text from a

drop-down menu, followed by the addition, by the analyst, of free text explaining why it was necessary and proportionate to make the search. In the case of a "strong selector", the analyst had to explain, for example, the justification for seeking the communications of a particular target; how the selector related to the target's method of communicating; and why selection of the relevant communications would not involve an unacceptable degree of collateral intrusion into privacy. In the case of a new "complex query", the analyst had to develop selection criteria most likely to identify communications bearing intelligence of value; and similarly had to explain why the criteria were justified, and why their use would be necessary and proportionate for the purposes within the Secretary of State's certificate. Selectors used for target development or target discovery could remain in use for a maximum of three months before a review was necessary.

292. Any selector had to be as specific as possible in order to select the minimum material necessary for the intelligence purpose, and be proportionate. If, through analysis, it was established that selectors were not being used by their intended target, prompt action had to be taken to remove them from relevant systems. The use of selectors had to be recorded in an approved location that enabled them to be audited; created a searchable record of selectors in use; and enabled oversight by the IC Commissioner. Robust independent oversight of selectors and search criteria was therefore within the IC Commissioner's powers: by the time of his 2014 report he had specifically put in place systems and processes to make sure that actually occurred, and, following the Chamber judgment, the Government had been working with the IC Commissioner's office to ensure that there would be enhanced oversight of selectors and search criteria under the IPA. However, the Government asserted that prior judicial authorisation would not have been possible for each selector without fundamentally altering their ability to discover and repel threats. GCHQ systems were necessarily tasked with many thousands of selectors which sometimes had to change rapidly in order to keep pace with fast moving investigations and threat discoveries.

293. Communications to which only the "strong selector" process was applied were discarded immediately unless they matched the strong selector. Communications to which the "complex query" process was also applied were retained for a few days, in order to allow the process to be carried out, and were then automatically deleted, unless they had been selected for examination. Communications which had been selected for examination could be retained only where it was necessary and proportionate to do so. The default position was that the retention period for selected communications was no longer than a few months, after which they were automatically deleted (although if the material had been cited in intelligence reporting, the report was retained). In exceptional circumstances a case could be made to retain selected communications for longer, as provided for in the IC Code.

294. The Government reiterated that any analysts who examined selected material had to be specially authorised to do so, and received mandatory regular training, including training on the requirements of necessity and proportionality. They were also vetted. Before they examined the material, they had to create a record setting out why access to the material was required, why it was consistent with the Secretary of State's certificate and the requirements of RIPA; and why it was proportionate (including considerations of any circumstances likely to give rise to a degree of collateral infringement of privacy). Unless such a record had been created, GCHQ's systems did not permit access to material.

295. As to the safeguards in respect of related communications data, the Government argued that examining the content of the most sensitive and private communications always involved a greater degree of intrusion than examining related communications data, irrespective of whether those data were aggregated to provide a detailed picture of where an individual was located, what websites he or she visited, or with whom he or she chose to communicate. On that basis, it remained appropriate for the rules governing content to be more exacting than those governing related communications data. Nevertheless, the Government accepted that the Secretary of State should be required to certify the necessity of examining related communications data under a bulk warrant pursuant to a regime analogous (though not identical) to the certification regime in place for the content of communications under section 16 RIPA. The new Code of Practice was to be amended to this effect.

296. Until then, however, communications data were subject to the same initial filtering process as content, by which GCHQ's processing systems automatically discarded certain types of communications in near-real time. They were then subjected by automated means to simple or complex queries. However, there were two main differences between the treatment of content and the treatment of related communications data. First of all, the safeguards in section 16 – which provided that, in order to be examined, material had to fall within the Secretary of State's certificate and could not be selected according to a factor referable to an individual known for the time being to be in the British Islands and the purpose of which was to identify his or her communications – only applied to content. According to the Government, it would not be practicable to apply this safeguard to related communications data. Significantly more queries were made against communications data (as many as several thousand in one week), and in a large number of cases the identity of the person to whom the data might relate was unknown. In addition, related communications data often had a temporal quality, and having to delay conducting searches of such data pending the acquisition of an individual authority would seriously risk undermining their utility in intelligence terms. Requiring the Secretary of

State to certify necessity and proportionality in each individual case, in advance of the searches being undertaken, could not possibly be done.

297. Secondly, related communications data which were not selected for examination were not immediately discarded. The principal reason for this was that communications data were to a large extent used to discover threats or targets of which GCHQ might previously have been unaware. They therefore required more analytical work, over a lengthy period, to discover "unknown unknowns". That discovery could very often involve an exercise of piecing together disparate small items of communications data to form a "jigsaw" revealing a threat; and would include the possible examination of items that initially appeared to be of no intelligence interest. Discarding unselected communications data immediately, or after a few days only, would render that exercise impossible.

298. Nevertheless, the Government confirmed that before any analyst could examine any communications data at all, they had to complete a record explaining why it was necessary and proportionate to do so, in pursuit of GCHQ's statutory functions. An auditable record was therefore produced, setting out the justification for examination, and these records were available for inspection. Moreover, no intelligence reporting could be made on the basis of communications data unless and until they had been examined. Finally, related communications could be retained only where it was necessary and proportionate to do so, for a maximum period of several months, unless an exceptional case to retain for longer was made. Otherwise related communications data were automatically deleted once the maximum period had expired.

299. Lastly, in the light of the Chamber judgment the Government confirmed that it was taking steps to ensure that where non-content data were to be selected for examination by reference to a person believed to be in the British Islands, the selection had to be certified by the Secretary of State as necessary and proportionate on a specific thematic basis. Pending the introduction of a "thematic" certification regime, by means of changes to the code governing the interception of communications under the IPA, GCHQ had been working with the IC Commissioner's office to generate management information that could be used by the IC Commissioner to enhance *ex post facto* oversight of related communications data. In particular, GCHQ had made changes to its systems so that in any case where an analyst intended to select secondary data for examination relating to a person believed to be in the British Islands by reference to a factor relating to that person, that case would be flagged along with the supporting justification for selecting the relevant data.

### *3. Observations of the third-party interveners*

#### (a) The Government of France

300. The French Government submitted that in the face of threats such as international and cross-border crime, and in view of the increasing sophistication of communication technologies, the strategic bulk surveillance of communications was of vital importance to States in protecting democratic society. Moreover, it was wrong to assume that bulk interception constituted a greater intrusion into the private life of an individual than targeted interception, which by its nature was more likely to result in the acquisition and examination of a large volume of the subject's communications. In their view, there was no reason why the criteria set out by the Court in *Weber and Saravia* (cited above) could not be considered equally relevant to the effective supervision of data interception and processing under a bulk interception regime. These criteria should, however, be applied in the context of an overall assessment, weighing any shortcomings against existing guarantees and the effectiveness of the safeguards against abuse.

301. There was no justification for adding the need for "reasonable suspicion" to these criteria. The authorities were generally not in a position to know in advance whose electronic communications it might be useful for them to monitor in the interests of law and order or national security, and such a requirement would deprive the surveillance measure of all operational interest. Moreover, in the Government's view there was no need for a judicial authority to be involved in the authorisation of such intelligence operations, or to carry out *ex post facto* control, provided that the authorising authority was independent of the executive, the supervisory body was vested with sufficient powers and competence to exercise effective and continuous control, and the two bodies were independent of one another.

302. Lastly, the intervening Government submitted that metadata were by their nature less intrusive than content, as they clearly contained less sensitive information about the behaviour and the private life of the person concerned. This view was supported by the report of the Venice Commission (see paragraphs 196-201 above) and the CJEU in *Digital Rights Ireland and Others* (see paragraphs 209-213 above).

#### (b) The Government of the Kingdom of the Netherlands

303. The Government of the Kingdom of the Netherlands also submitted that bulk interception was necessary to identify hitherto unknown threats to national security. In order to protect national security, intelligence services needed the tools to investigate emerging threats in a timely and effective manner. For this they needed the powers necessary to enable them to detect and/or prevent not only terrorist activities (such as attack planning,

recruitment, propaganda and funding), but also intrusive State or non-State actors' cyber activities aimed at disrupting democracy (for example, by influencing national elections or obstructing investigations by national and international organisations. An example of this was the attempted hacking of the investigation of the use of chemical weapons in Syria by the Organisation for the Prohibition of Chemical Weapons in The Hague). Moreover, the increasing dependency of vital sectors on digital infrastructures meant that such sectors, including water management, energy, telecoms, transport, logistics, harbours and airports, were increasingly vulnerable to cyber-attacks. The consequences of disruption in such sectors would have a deep impact on society, far beyond the substantial monetary damage.

304. A complicating factor in all of this was the development of new means of digital communication and the exponential increase of data that were transmitted and stored globally. In many instances the nature and origin of a particular threat was unknown and the use of targeted interception was not feasible. However, while bulk interception was not as tightly defined as targeted interception, it was never completely untargeted. Rather, it was applied for specific aims.

305. In the intervening Government's view, there was no need for additional or updated minimum safeguards; those previously identified by the Court were sufficiently robust and "future proof". The additional requirements proposed by the applicants before the Chamber – in particular, the requirement to demonstrate "reasonable suspicion" – would unacceptably reduce the effectiveness of the intelligence services without providing any meaningful additional protection of individuals' fundamental rights.

306. Furthermore, according to the intervening Government, it was still relevant to distinguish between content and communications data, as the content of communications was likely to be more sensitive than communications data. The intervening Government also agreed with the Chamber that it was wrong automatically to assume that bulk interception constituted a greater intrusion into the private life of an individual than targeted interception, since with targeted interception it was likely that all, or nearly all, of the intercepted communications would be analysed. This was not true of bulk interception, where restrictions on the examination and use of data determined the intrusiveness of the interception on the individuals' fundamental rights.

307. Lastly, the intervening Government submitted that any requirement to explain or substantiate selectors or search criteria in the authorisation would seriously restrict the effectiveness of bulk interception in view of the high degree of uncertainty regarding the source of a threat. *Ex post* oversight provided sufficient safeguards.

**(c) The Government of the Kingdom of Norway**

308. The Norwegian Government submitted that with regard to the decision of States to introduce and operate some form of bulk interception regime for national security purposes, the margin of appreciation had to be wide. This was because intelligence services had to keep pace with the rapid advances in information and communications technology. Hostile actors changed their devices and digital identities at a pace which made it difficult to track them over time. It was also difficult to discover and counteract hostile cyberoperations in a timely manner without tools capable of discovering anomalies and relevant signatures. It was therefore without doubt that modern capacities like bulk interception were needed in order to find unknown threats operating in the digital domain, and to enable the services to discover and follow relevant intelligence threats.

309. In the Norwegian Government's view, the Court's oversight had to be based on an overall assessment of whether the procedural safeguards against abuse were adequate and sufficient. It should avoid absolute requirements. Nor should it apply criteria that would undermine indirectly the wide margin of appreciation afforded to States in deciding to operate a bulk interception regime for national security reasons. A "reasonable suspicion" or "subsequent notification" requirement would have this effect.

310. Lastly, the intervening Government encouraged the Court to refrain from importing concepts and criteria from the CJEU. First of all, at the relevant time nineteen Council of Europe Contracting States were not members of the European Union. Secondly, while the Convention and the Charter of Fundamental Rights had many features in common, there were also differences, most notably Article 8 of the Charter which contained a right to the protection of personal data. The CJEU also formulated "proportionality" differently, using a "strict necessity" method which did not compare to that used by the Court.

**(d) United Nations Special Rapporteur on the promotion of the right to freedom of opinion and expression**

311. The Special Rapporteur argued that surveillance cast a shadow over communications, such that individuals might refrain from engaging in activities protected under international human rights law. That was not to say that all surveillance operations constituted a violation of human rights law; some might be tolerable when the conditions of legality, necessity and legitimacy were met. However, all types of surveillance required a rigorous evaluation of whether they were consistent with the norms of international human rights law.

312. In the Special Rapporteur's view, the right to privacy had to be protected not only as a fundamental right independent of all others, but also in order to protect other rights, such as freedom of opinion and expression, which depended on a zone of privacy for their enjoyment. As the Special

Rapporteur had indicated in his 2015 report, surveillance systems might undermine the right to form an opinion as the fear of unwilling disclosure of online activity could deter individuals from accessing information.

313. The United Nations High Commissioner's report counselled against distinguishing metadata from content when examining the severity of the interference with rights protected under the International Covenant on Civil and Political Rights (ICCPR). Her 2014 report indicated that the aggregation of metadata by way of government surveillance might reveal more private detail about an individual than perhaps even a private communication would. The Special Rapporteur further indicated that the distinction between internal and external communications might run counter to the ICCPR. The ICCPR placed States under a duty to respect and ensure all the rights therein to all within their jurisdiction, and in its latest General Comment the Human Rights Committee interpreted this standard as including State activities that directly impacted rights outside its own territory.

314. Lastly, the Special Rapporteur emphasised the importance of safeguards to protect against abuse, in particular: the need for a court, tribunal or other adjudicatory body to supervise the application of an interference measure; subsequent notification of surveillance subjects; publication of information on the scope of surveillance techniques and powers; and the right to effective remedies in case of abuse.

#### (e) Access Now

315. Access Now submitted that the mass surveillance at issue in the present case had failed to comply with the ICCPR and the International Principles on the Application of Human Rights to Communications Surveillance since the United Kingdom had not demonstrated that such surveillance was strictly necessary or proportionate. They further contended that surveillance programmes should not be considered independently but should instead be viewed in relation to the entirety of a nation's surveillance activities, as machine learning – through which mathematical algorithms could draw inferences from collections of data – had increased the invasiveness of big data sets and data mining.

#### (f) ARTICLE 19

316. ARTICLE 19 submitted that the indiscriminate and "suspicionless" collection, analysis and retention of individuals' communications was inherently disproportionate. In ARTICLE 19's opinion, only targeted surveillance based on reasonable suspicion and authorised by a judge would constitute a legitimate restriction on privacy rights.

**(g) European Digital Rights and other organisations active in the field of human rights in the information society**

317. European Digital Rights (EDRi) and others argued that the present case offered the Court a crucial opportunity to revise its framework for the protection of metadata. Governments had built their surveillance programmes based on the distinction drawn between content and metadata in *Malone v. the United Kingdom* (2 August 1984, Series A no. 82), but at the time that case was decided neither the Internet nor mobile phones existed. Today, metadata could paint a detailed and intimate picture of a person: they allowed for mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns and insight into who a person interacted with. Moreover, the level of detail that could be gleaned was magnified when analysed on a large scale. Indeed, Stewart Baker, general counsel of the NSA, had indicated that metadata could disclose everything about someone's life, and that if you had enough metadata, you would not need content. As a result, different degrees of protection should not be afforded to personal data based on the arbitrary and irrelevant distinction between content and metadata, but rather on the inferences that could be drawn from the data.

**(h) Open Society Justice Initiative**

318. The Open Society Justice Initiative submitted that both the amount of data available for interception today and governments' appetite for data far exceeded what was possible in the past. Consequently, bulk interception was a particularly serious interference with privacy which could, through its "chilling effect", potentially interfere with other rights such as freedom of expression and freedom of association. To be lawful, bulk interception should therefore satisfy several preconditions: the governing law had to be sufficiently precise; the scope of the information gathered had to be limited by time and geography; and information should only be gathered based on "reasonable suspicion".

**(i) Helsinki Foundation for Human Rights**

319. The Helsinki Foundation for Human Rights described their experience challenging the surveillance of communications by public authorities in Poland, which had culminated in the Constitutional Tribunal finding certain aspects of the relevant legislation to be unconstitutional. The legislation was subsequently amended.

**(j) International Commission of Jurists**

320. The International Commission of Jurists submitted that in the light of the scale and scope of the interference with privacy entailed in mass surveillance, the distinction between metadata and content had become

outdated. Furthermore, the fact that, in a mass surveillance operation, elements of the interference with rights might take place outside a State's territorial jurisdiction did not preclude that State's responsibility, since its control over the information was sufficient to establish jurisdiction.

#### (k) Law Society of England and Wales

321. The Law Society expressed deep concern about the implications of the section 8(4) regime for the principle of legal professional privilege. In its view, the regime permitted the interception of legally privileged and confidential communications between lawyers and clients, even when both were in the United Kingdom. It also permitted the routine collection of metadata attaching to such communications. Furthermore, once intercepted these legally privileged communications could be used, provided that the primary purpose and object of the warrant was the collection of external communications. This arrangement – and the absence of adequate constraints on the use of such material – was apt to have a potentially severe chilling effect on the frankness and openness of lawyer-client communications.

### *4. The Court's assessment*

#### (a) Preliminary remarks

322. The present complaint concerns the bulk interception of cross-border communications by the intelligence services. While it is not the first time the Court has considered this kind of surveillance (see *Weber and Saravia*, and *Liberty and Others*, both cited above), in the course of the proceedings it has become apparent that the assessment of any such regime faces specific difficulties. In the current, increasingly digital, age the vast majority of communications take electronic form and are transported across global telecommunications networks using a combination of the quickest and cheapest paths without any meaningful reference to national borders. Surveillance which is not targeted directly at individuals therefore has the capacity to have a very wide reach indeed, both inside and outside the territory of the surveilling State. Safeguards are therefore pivotal and yet elusive. Unlike the targeted interception which has been the subject of much of the Court's case-law, and which is primarily used for the investigation of crime, bulk interception is also – perhaps even predominantly – used for foreign intelligence gathering and the identification of new threats from both known and unknown actors. When operating in this realm, Contracting States have a legitimate need for secrecy which means that little if any information about the operation of the scheme will be in the public domain, and such information as is available may be couched in terminology which is obscure and which may vary significantly from one State to the next.

323. While technological capabilities have greatly increased the volume of communications traversing the global Internet, the threats being faced by Contracting States and their citizens have also proliferated. These include, but are not limited to, global terrorism, drug trafficking, human trafficking and sexual exploitation of children. Many of these threats come from international networks of hostile actors with access to increasingly sophisticated technology enabling them to communicate undetected. Access to such technology also permits hostile State and non-State actors to disrupt digital infrastructure and even the proper functioning of democratic processes through the use of cyber-attacks, a serious threat to national security which by definition exists only in the digital domain and as such can only be detected and investigated there. Consequently, the Court is required to carry out its assessment of Contracting States' bulk interception regimes, a valuable technological capacity to identify new threats in the digital domain, for Convention compliance by reference to the existence of safeguards against arbitrariness and abuse, on the basis of limited information about the manner in which those regimes operate.

**(b) Existence of an interference**

324. The Government did not dispute that there had been an interference with the applicants' Article 8 rights, although they submitted that for the purposes of Article 8 of the Convention the only meaningful interference could have occurred when communications were selected for examination.

325. The Court views bulk interception as a gradual process in which the degree of interference with individuals' Article 8 rights increases as the process progresses. Bulk interception regimes may not all follow exactly the same model, and the different stages of the process will not necessarily be discrete or followed in strict chronological order. Nevertheless, subject to the aforementioned caveats, the Court considers that the stages of the bulk interception process which fall to be considered can be described as follows:

(a) the interception and initial retention of communications and related communications data (that is, the traffic data belonging to the intercepted communications);

(b) the application of specific selectors to the retained communications/ related communications data;

(c) the examination of selected communications/related communications data by analysts; and

(d) the subsequent retention of data and use of the "final product", including the sharing of data with third parties.

326. At what the Court has taken to be the first stage, electronic communications (or "packets" of electronic communications) will be intercepted in bulk by the intelligence services. These communications will belong to a large number of individuals, many of whom will be of no

interest whatsoever to the intelligence services. Some communications of a type unlikely to be of intelligence interest may be filtered out at this stage.

327. The initial searching, which is mostly automated, takes place at what the Court has taken to be the second stage, when different types of selectors, including "strong selectors" (such as an email address) and/or complex queries are applied to the retained packets of communications and related communications data. This may be the stage where the process begins to target individuals through the use of strong selectors.

328. At what the Court has taken to be the third stage, intercept material is examined for the first time by an analyst.

329. What the Court has taken to be the final stage is when the intercept material is actually used by the intelligence services. This may involve the creation of an intelligence report, the disseminating of the material to other intelligence services within the intercepting State, or even the transmission of material to foreign intelligence services.

330. The Court considers that Article 8 applies at each of the above stages. While the initial interception followed by the immediate discarding of parts of the communications does not constitute a particularly significant interference, the degree of interference with individuals' Article 8 rights will increase as the bulk interception process progresses. In this regard, the Court has clearly stated that even the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 (see *Leander v. Sweden*, 26 March 1987, § 48, Series A no. 116), and that the need for safeguards will be all the greater where the protection of personal data undergoing automatic processing is concerned (see *S. and Marper*, cited above, § 103). The fact that the stored material is in coded form, intelligible only with the use of computer technology and capable of being interpreted only by a limited number of persons, can have no bearing on that finding (see *Amann v. Switzerland* [GC], no. 27798/95, § 69, ECHR 2000-II, and *S. and Marper*, cited above, §§ 67 and 75). Lastly, at the end of the process, where information about a particular person will be analysed or the content of the communications is being examined by an analyst, the need for safeguards will be at its highest. This approach of the Court is in line with the finding of the Venice Commission, which in its report on the Democratic Oversight of Signals Intelligence Agencies considered that in bulk interception the main interference with privacy occurred when stored personal data were processed and/or accessed by the agencies (see paragraph 196 above).

331. Thus, the degree of interference with privacy rights will increase as the process moves through the different stages. In examining whether this increasing interference was justified, the Court will carry out its assessment of the section 8(4) regime on the basis of this understanding of the nature of the interference.

**(c) Whether the interference was justified**

*(i) General principles relating to secret measures of surveillance, including the interception of communications*

332. Any interference with an individual's Article 8 rights can only be justified under Article 8 § 2 if it is in accordance with the law, pursues one or more of the legitimate aims to which that paragraph refers and is necessary in a democratic society in order to achieve any such aim (see *Roman Zakharov*, cited above, § 227; see also *Kennedy v. the United Kingdom*, no. 26839/05, § 130, 18 May 2010). The wording "in accordance with the law" requires the impugned measure to have some basis in domestic law (as opposed to a practice which does not have a specific legal basis – see *Heglas v. the Czech Republic*, no. 5935/02, § 74, 1 March 2007). It must also be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must therefore be accessible to the person concerned and foreseeable as to its effects (see *Roman Zakharov*, cited above, § 228; see also, among many other authorities, the above-cited cases of *Rotaru*, § 52; *S. and Marper*, § 95; and *Kennedy*, § 151).

333. The meaning of "foreseeability" in the context of secret surveillance is not the same as in many other fields. In the special context of secret measures of surveillance, such as the interception of communications, "foreseeability" cannot mean that individuals should be able to foresee when the authorities are likely to resort to such measures so that they can adapt their conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on secret surveillance measures, especially as the technology available for use is continually becoming more sophisticated. The domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which – and the conditions on which – public authorities are empowered to resort to any such measures (see *Roman Zakharov*, cited above, § 229; see also *Malone*, cited above, § 67; *Leander*, cited above, § 51; *Huvig*, cited above, § 29; *Kruslin*, cited above, § 30; *Valenzuela Contreras v. Spain*, 30 July 1998, § 46, *Reports of Judgments and Decisions* 1998-V; *Rotaru*, cited above, § 55; *Weber and Saravia*, cited above, § 93; and *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, § 75, 28 June 2007). Moreover, the law must indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see *Roman Zakharov*, cited above, § 230; see also, among other authorities, the above-cited cases of *Malone*, § 68; *Leander*, § 51; *Huvig*, § 29; *Kruslin*, § 30; and *Weber and Saravia*, § 94).

334. In cases where legislation permitting secret surveillance is contested before the Court, the lawfulness of the interference is closely related to the question whether the "necessity" test has been complied with and it is therefore appropriate for the Court to address jointly the "in accordance with the law" and "necessity" requirements. The "quality of law" in this sense implies that the domestic law must not only be accessible and foreseeable in its application, it must also ensure that secret surveillance measures are applied only when "necessary in a democratic society", in particular by providing for adequate and effective safeguards and guarantees against abuse (see *Roman Zakharov*, cited above, § 236; see also *Kennedy*, cited above, § 155).

335. In this regard it should be reiterated that in its case-law on the interception of communications in criminal investigations, the Court has developed the following minimum requirements that should be set out in law in order to avoid abuses of power: (i) the nature of offences which may give rise to an interception order; (ii) a definition of the categories of people liable to have their communications intercepted; (iii) a limit on the duration of interception; (iv) the procedure to be followed for examining, using and storing the data obtained; (v) the precautions to be taken when communicating the data to other parties; and (vi) the circumstances in which intercepted data may or must be erased or destroyed (see the above-cited cases of *Huvig*, § 34; *Kruslin*, § 35; *Valenzuela Contreras*, § 46; *Weber and Saravia*, § 95; and *Association for European Integration and Human Rights and Ekimdzhiev*, § 76). In *Roman Zakharov* (cited above, § 231) the Court confirmed that the same six minimum safeguards also applied in cases where the interception was for reasons of national security; however, in determining whether the impugned legislation was in breach of Article 8, it also had regard to the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law (see *Roman Zakharov*, cited above, § 238).

336. Review and supervision of secret surveillance measures may come into play at three stages: when the surveillance is first ordered, while it is being carried out, or after it has been terminated. As regards the first two stages, the very nature and logic of secret surveillance dictate that not only the surveillance itself but also the accompanying review should be effected without the individual's knowledge. Consequently, since the individual will necessarily be prevented from seeking an effective remedy of his or her own accord or from taking a direct part in any review proceedings, it is essential that the procedures established should themselves provide adequate and equivalent guarantees safeguarding his or her rights. In a field where abuse in individual cases is potentially so easy and could have such harmful consequences for democratic society as a whole, the Court has held that it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a

proper procedure (see *Roman Zakharov*, cited above, § 233; see also *Klass and Others v. Germany*, 6 September 1978, §§ 55 and 56, Series A no. 28).

337. As regards the third stage, after the surveillance has been terminated, the question of subsequent notification of surveillance measures is a relevant factor in assessing the effectiveness of remedies before the courts and therefore the existence of effective safeguards against the abuse of surveillance powers. There is in principle little scope for recourse to the courts by the individual concerned unless he or she is apprised of the measures taken without his or her knowledge and is thus able to challenge their legality retrospectively (see *Roman Zakharov*, cited above, § 234; see also *Klass and Others*, § 57, and *Weber and Saravia*, § 135, both cited above) or, in the alternative, unless any person who suspects that he or she has been subject to surveillance can apply to courts whose jurisdiction does not depend on notification to the surveillance subject of the measures taken (see *Roman Zakharov*, cited above, § 234; see also *Kennedy*, cited above, § 167).

338. As to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, the Court has recognised that the national authorities enjoy a wide margin of appreciation in choosing how best to achieve the legitimate aim of protecting national security (see *Weber and Saravia*, cited above, § 106).

339. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security (and other essential national interests) may undermine or even destroy the proper functioning of democratic processes under the cloak of defending them, the Court must be satisfied that there are adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the "interference" to what is "necessary in a democratic society" (see *Roman Zakharov*, cited above, § 232; see also the above-cited cases of *Klass and Others*, §§ 49, 50 and 59; *Weber and Saravia*, § 106; and *Kennedy*, §§ 153 and 154).

*(ii) Whether there is a need to develop the case-law*

340. In *Weber and Saravia* and *Liberty and Others* (both cited above) the Court accepted that bulk interception regimes did not *per se* fall outside the States' margin of appreciation. In view of the proliferation of threats that States currently face from networks of international actors, using the Internet both for communication and as a tool, and the existence of

sophisticated technology which would enable these actors to avoid detection (see paragraph 323 above), the Court considers that the decision to operate a bulk interception regime in order to identify threats to national security or essential national interests is one which continues to fall within this margin.

341. In both *Weber and Saravia* and *Liberty and Others* (both cited above) the Court applied the above-mentioned six minimum safeguards developed in its case-law on targeted interception (see paragraph 335 above). However, while the bulk interception regimes considered in those cases were on their face similar to that in issue in the present case, both cases are now more than ten years old, and in the intervening years technological developments have significantly changed the way in which people communicate. Lives are increasingly lived online, generating both a significantly larger volume of electronic communications, and communications of a significantly different nature and quality, to those likely to have been generated a decade ago (see paragraph 322 above). The scope of the surveillance activity considered in those cases would therefore have been much narrower.

342. This is also the case when it comes to related communications data. As was observed in the report making up the Independence Surveillance Review (see paragraphs 156-62), greater volumes of communications data are currently available, for each individual, in relation to content, since every piece of content is surrounded by multiple pieces of communications data (see paragraph 159 above). While the content might be encrypted and, in any event, may not reveal anything of note about the sender or recipient, the related communications data could reveal a great deal of personal information, such as the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. Furthermore, any intrusion occasioned by the acquisition of related communications data will be magnified when they are obtained in bulk, since they are now capable of being analysed and interrogated so as to paint an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns and insight into who a person has interacted with (see paragraph 317 above).

343. More importantly, however, in *Weber and Saravia* and *Liberty and Others* the Court did not expressly address the fact that it was dealing with surveillance of a different nature and scale from that considered in previous cases. Nonetheless, targeted interception and bulk interception are different in a number of important respects.

344. To begin with, bulk interception is generally directed at international communications (that is, communications physically travelling across State borders), and while the interception and even examination of communications of persons within the surveilling State might not be excluded, in many cases the stated purpose of bulk interception is to

monitor the communications of persons outside the State's territorial jurisdiction, which could not be monitored by other forms of surveillance. For example, the German system aims only to monitor foreign telecommunications outside of German territory (see paragraph 248 above). In Sweden, the intercept material cannot relate to signals where both the sender and recipient are in Sweden (see today's judgment in *Centrum för rättvisa v. Sweden*, no. 35252/08).

345. Moreover, as already noted, the purposes for which bulk interception may be employed would appear to be different. In so far as targeted interception has been considered by the Court, in most cases it has been employed by respondent States for the purposes of investigating crime. However, while bulk interception may be used to investigate certain serious crimes, Council of Europe member States operating a bulk interception regime appear to use it for the purposes of foreign intelligence gathering, the early detection and investigation of cyber-attacks, counter-espionage and counterterrorism (see paragraphs 303, 308 and 323 above).

346. While bulk interception is not necessarily used to target specified individuals, it evidently can be – and is – used for this purpose. However, when this is the case, the targeted individuals' devices are not monitored. Rather, individuals are "targeted" by the application of strong selectors (such as their email addresses) to the communications intercepted in bulk by the intelligence services. Only those "packets" of the targeted individuals' communications which were travelling across the bearers selected by the intelligence services will have been intercepted in this way, and only those intercepted communications which matched either a strong selector or complex query could be examined by an analyst.

347. As with any interception regime, there is of course considerable potential for bulk interception to be abused in a manner adversely affecting the right of individuals to respect for private life. While Article 8 of the Convention does not prohibit the use of bulk interception to protect national security and other essential national interests against serious external threats, and while States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary for these purposes, in the operation of such a system that margin will be narrower and a number of safeguards will have to be present. The Court has already identified those safeguards which should feature in a Convention-compliant targeted interception regime. While those principles provide a useful framework for this exercise, they will have to be adapted to reflect the specific features of a bulk interception regime and, in particular, the increasing degrees of intrusion into the Article 8 rights of individuals as the operation moves through the stages identified in paragraph 325 above.

*(iii) Approach to be followed in bulk interception cases*

348. It is clear that the first two of the six "minimum safeguards" which the Court, in the context of targeted interception, has found should be defined clearly in domestic law in order to avoid abuses of power (that is, the nature of offences which may give rise to an interception order and the categories of people liable to have their communications intercepted: see paragraph 335 above) are not readily applicable to a bulk interception regime. Similarly, the requirement of "reasonable suspicion", which can be found in the Court's case-law on targeted interception in the context of criminal investigations is less germane in the bulk interception context, the purpose of which is in principle preventive, rather than for the investigation of a specific target and/or an identifiable criminal offence. Nevertheless, the Court considers it imperative that when a State is operating such a regime, domestic law should contain detailed rules on when the authorities may resort to such measures. In particular, domestic law should set out with sufficient clarity the grounds upon which bulk interception might be authorised and the circumstances in which an individual's communications might be intercepted. The remaining four minimum safeguards defined by the Court in its previous judgments – that is, that domestic law should set out a limit on the duration of interception, the procedure to be followed for examining, using and storing the data obtained, the precautions to be taken when communicating the data to other parties, and the circumstances in which intercepted data may or must be erased or destroyed – are equally relevant to bulk interception.

349. In its case-law on targeted interception, the Court has had regard to the arrangements for supervising and reviewing the interception regime (see *Roman Zakharov*, cited above, §§ 233-34). In the context of bulk interception, the importance of supervision and review will be amplified, because of the inherent risk of abuse and because the legitimate need for secrecy will inevitably mean that, for reasons of national security, States will often not be at liberty to disclose information concerning the operation of the impugned regime.

350. Therefore, in order to minimise the risk of the bulk interception power being abused, the Court considers that the process must be subject to "end-to-end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation are being defined; and the operation should be subject to supervision and independent *ex post facto* review. In the Court's view, these are fundamental safeguards which will be the cornerstone of any Article 8-compliant bulk interception regime (see also the report of the Venice Commission, at paragraph 197 above, which similarly found that two of the

most significant safeguards in a bulk interception regime were the authorisation and oversight of the process).

351. Turning first to authorisation, the Grand Chamber agrees with the Chamber that while judicial authorisation is an "important safeguard against arbitrariness" it is not a "necessary requirement" (see paragraphs 318-20 of the Chamber judgment). Nevertheless, bulk interception should be authorised by an independent body, that is, a body which is independent of the executive.

352. Furthermore, in order to provide an effective safeguard against abuse, the independent authorising body should be informed of both the purpose of the interception and the bearers or communication routes likely to be intercepted. This would enable the independent authorising body to assess the necessity and proportionality of the bulk interception operation and also to assess whether the selection of bearers is necessary and proportionate to the purposes for which the interception is being conducted.

353. The use of selectors – and strong selectors in particular – is one of the most important steps in the bulk interception process, as this is the point at which the communications of a particular individual may be targeted by the intelligence services. However, while some systems allow for the prior authorisation of categories of selectors (see, for example, the Swedish system described in detail in *Centrum för rättvisa v. Sweden*, no. 35252/08), the Court notes that the Governments of both the United Kingdom and the Netherlands have submitted that any requirement to explain or substantiate selectors or search criteria in the authorisation would seriously restrict the effectiveness of bulk interception (see paragraphs 292 and 307 above). This was accepted by the IPT, which found that the inclusion of the selectors in the authorisation would "unnecessarily undermine and limit the operation of the warrant and might in any event be entirely unrealistic" (see paragraph 49 above).

354. Taking into account the characteristics of bulk interception (see paragraphs 344-345 above), the large number of selectors employed and the inherent need for flexibility in the choice of selectors, which in practice may be expressed as technical combinations of numbers or letters, the Court would accept that the inclusion of all selectors in the authorisation may not be feasible in practice. Nevertheless, given that the choice of selectors and query terms determines which communications will be eligible for examination by an analyst, the authorisation should at the very least identify the types or categories of selectors to be used.

355. Moreover, enhanced safeguards should be in place when strong selectors linked to identifiable individuals are employed by the intelligence services. The use of every such selector must be justified – with regard to the principles of necessity and proportionality – by the intelligence services and that justification should be scrupulously recorded and be subject to a process of prior internal authorisation providing for separate and objective

verification of whether the justification conforms to the aforementioned principles.

356. Each stage of the bulk interception process – including the initial authorisation and any subsequent renewals, the selection of bearers, the choice and application of selectors and query terms, and the use, storage, onward transmission and deletion of the intercept material – should also be subject to supervision by an independent authority and that supervision should be sufficiently robust to keep the "interference" to what is "necessary in a democratic society" (see *Roman Zakharov*, cited above, § 232; see also the above-cited cases of *Klass and Others*, §§ 49, 50 and 59; *Weber and Saravia*, § 106; and *Kennedy*, §§ 153 and 154). In particular, the supervising body should be in a position to assess the necessity and proportionality of the action being taken, having due regard to the corresponding level of intrusion into the Convention rights of the persons likely to be affected. In order to facilitate this supervision, detailed records should be kept by the intelligence services at each stage of the process.

357. Lastly, an effective remedy should be available to anyone who suspects that his or her communications have been intercepted by the intelligence services, either to challenge the lawfulness of the suspected interception or the Convention compliance of the interception regime. In the targeted interception context, the Court has repeatedly found the subsequent notification of surveillance measures to be a relevant factor in assessing the effectiveness of remedies before the courts and hence the existence of effective safeguards against the abuse of surveillance powers. However, it has acknowledged that notification is not necessary if the system of domestic remedies permits any person who suspects that his or her communications are being or have been intercepted to apply to the courts – in other words, where the courts' jurisdiction does not depend on notification to the interception subject that there has been an interception of his or her communications (see *Roman Zakharov*, § 234, and *Kennedy*, § 167, both cited above).

358. The Court considers that a remedy which does not depend on notification to the interception subject could also be an effective remedy in the context of bulk interception; in fact, depending on the circumstances it may even offer better guarantees of a proper procedure than a system based on notification. Regardless of whether material was acquired through targeted or bulk interception, the existence of a national security exception could deprive a notification requirement of any real practical effect. The likelihood of a notification requirement having little or no practical effect will be more acute in the bulk interception context, since such surveillance may be used for the purposes of foreign intelligence gathering and will, for the most part, target the communications of persons outside the State's territorial jurisdiction. Therefore, even if the identity of a target is known, the authorities may not be aware of his or her location.

359. The powers and procedural guarantees an authority possesses are relevant in determining whether a remedy is effective. Therefore, in the absence of a notification requirement it is imperative that the remedy should be before a body which, while not necessarily judicial, is independent of the executive and ensures fairness of the proceedings, offering, in so far as possible, an adversarial process. The decisions of such authority must be reasoned and legally binding with regard, *inter alia*, to the cessation of unlawful interception and the destruction of unlawfully obtained and/or stored intercept material (see, *mutatis mutandis*, *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, § 120, ECHR 2006-VII, and *Leander*, cited above, §§ 81-83, where the lack of power to render a legally binding decision constituted the main weakness in the control offered).

360. In the light of the above, the Court will determine whether a bulk interception regime was Convention-compliant by conducting a global assessment of the operation of the regime. Such assessment will focus primarily on whether the domestic legal framework contained sufficient guarantees against abuse, and whether the process was subject to "end-to-end safeguards" (see paragraph 350 above). In doing so, it will have regard to the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse (see *Association for European Integration and Human Rights and Ekimdzhiev*, cited above, § 92).

361. In assessing whether the respondent State acted within its margin of appreciation (see paragraph 347 above), the Court would need to take account of a wider range of criteria than the six *Weber* safeguards. More specifically, in addressing jointly "in accordance with the law" and "necessity" as is the established approach in this area (see *Roman Zakharov*, § 236, and *Kennedy*, § 155, both cited above), the Court will examine whether the domestic legal framework clearly defined:

(i) the grounds on which bulk interception may be authorised;

(ii) the circumstances in which an individual's communications may be intercepted;

(iii) the procedure to be followed for granting authorisation;

(iv) the procedures to be followed for selecting, examining and using intercept material;

(v) the precautions to be taken when communicating the material to other parties;

(vi) the limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;

(vii) the procedures and modalities for supervision by an independent authority of compliance with the above-mentioned safeguards and its powers to address non-compliance;

(viii) the procedures for independent *ex post facto* review of such compliance and the powers vested in the competent body in addressing instances of non-compliance.

362. Despite its being one of the six *Weber* criteria, to date the Court has not yet provided specific guidance regarding the precautions to be taken when communicating intercept material to other parties. However, it is now clear that some States are regularly sharing material with their intelligence partners and even, in some instances, allowing those partners direct access to their own systems. Consequently, the Court considers that the transmission by a Contracting State to foreign States or international organisations of material obtained by bulk interception should be limited to such material as has been collected and stored in a Convention-compliant manner and should be subject to certain additional specific safeguards pertaining to the transfer itself. First of all, the circumstances in which such a transfer may take place must be set out clearly in domestic law. Secondly, the transferring State must ensure that the receiving State, in handling the data, has in place safeguards capable of preventing abuse and disproportionate interference. In particular, the receiving State must guarantee the secure storage of the material and restrict its onward disclosure. This does not necessarily mean that the receiving State must have comparable protection to that of the transferring State; nor does it necessarily require that an assurance is given prior to every transfer. Thirdly, heightened safeguards will be necessary when it is clear that material requiring special confidentiality – such as confidential journalistic material – is being transferred. Lastly, the Court considers that the transfer of material to foreign intelligence partners should also be subject to independent control.

363. For the reasons identified at paragraph 342 above, the Court is not persuaded that the acquisition of related communications data through bulk interception is necessarily less intrusive than the acquisition of content. It therefore considers that the interception, retention and searching of related communications data should be analysed by reference to the same safeguards as those applicable to content.

364. That being said, while the interception of related communications data will normally be authorised at the same time the interception of content is authorised, once obtained they may be treated differently by the intelligence services (see, for example, paragraphs 153-154 above). In view of the different character of related communications data and the different ways in which they are used by the intelligence services, as long as the aforementioned safeguards are in place, the Court is of the opinion that the legal provisions governing their treatment may not necessarily have to be identical in every respect to those governing the treatment of content.

*(iv) The Court's assessment of the case at hand*

(α) Preliminary issues

365. At the relevant time, bulk interception had a legal basis in Chapter I of RIPA. Moreover, the Court is satisfied that the said regime pursued the legitimate aims of protecting national security, preventing disorder and crime, and protecting the rights and freedoms of others. Therefore, following the approach outlined in paragraph 334 above, it remains to be considered whether the domestic law was accessible and contained adequate and effective safeguards and guarantees to meet the requirements of "foreseeability" and "necessity in a democratic society".

366. The relevant legislative provisions governing the operation of the bulk interception regime were undoubtedly complex; indeed, most of the reports on the United Kingdom's secret surveillance regimes criticised their lack of clarity (see paragraphs 143, 152 and 157 above). However, those provisions were elucidated in the accompanying Interception of Communications Code of Practice ("the IC Code" – see paragraph 96 above). Paragraph 6.4 of the IC Code made it clear that bulk interception was taking place and provided further details of how this particular surveillance regime operated in practice (see paragraph 96 above). The IC Code is a public document approved by both Houses of Parliament and published by the government, online and in print, and it has to be taken into account both by persons exercising interception duties and by the courts (see paragraphs 93-94 above). As a consequence, the Court accepted that its provisions could be taken into account in assessing the foreseeability of RIPA (see *Kennedy*, cited above, § 157). Accordingly, the Court would accept that domestic law was adequately "accessible".

367. Turning next to the question whether the law contained adequate and effective safeguards and guarantees to meet the requirements of "foreseeability" and "necessity in a democratic society", the Court will address in subsection (β) below each of the eight requirements set out in paragraph 361 above in respect of the interception of the content of electronic communications. In subsection (γ) below it will examine more specifically the interception of related communications data.

(β) Interception of the content of communications

– *Grounds on which bulk interception may be authorised*

368. Under section 5(3) RIPA and paragraph 6.11 of the IC Code (see paragraphs 62 and 96 respectively above), the Secretary of State could only issue a bulk interception warrant if he or she was satisfied that it was necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or for the purpose of safeguarding the economic well-being of the United Kingdom, in so far as those interests were also relevant to the interests of national security.

369. These grounds were subject to the following limitations. First of all, the IC Commissioner had clarified that in practice "national security" allowed surveillance of activities which threatened the safety or well-being of the State and activities which were intended to undermine or overthrow parliamentary democracy by political, industrial or violent means (see *Kennedy*, cited above, § 333). Secondly, serious crime was defined in section 81(2)(b) RIPA as a crime for which the perpetrator (assuming he or she was over the age of twenty-one and had no previous convictions) could reasonably be expected to be sentenced to imprisonment for a term of three years or more; or where the conduct involved the use of violence, resulted in substantial financial gain or was conducted by a large number of persons in pursuit of a common purpose (see paragraph 63 above). Thirdly, section 17 RIPA and paragraph 8.3 of the IC Code provided that as a general rule neither the possibility of interception, nor intercepted material itself, could play any part in legal proceedings (see paragraphs 83 and 96 respectively above). Therefore, while interception could be used for the purposes of preventing or detecting serious crime, intercept material could not be used in the prosecution of a criminal offence. In addition, paragraph 6.8 of the IC Code provided that the purpose of a section 8(4) warrant would "typically reflect one or more of the intelligence priorities set by the National Security Council" (see paragraphs 96 and 98 above).

370. In principle, the wider the grounds, the greater the potential for abuse. However, narrower and/or more tightly defined grounds would only provide an effective guarantee against abuse if there were sufficient other safeguards in place to ensure that bulk interception was only authorised for a permitted ground and that it was necessary and proportionate for that purpose. The closely related issue of whether there existed sufficient guarantees to ensure that the interception was necessary or justified is therefore as important as the degree of precision with which the grounds on which authorisation may be given are defined. Consequently, in the Court's view, a regime which permits bulk interception to be ordered on relatively wide grounds may still comply with Article 8 of the Convention, provided that, when viewed as a whole, sufficient guarantees against abuse are built into the system to compensate for this weakness.

371. In the United Kingdom, while the grounds on which bulk interception could be authorised were formulated in relatively broad terms, they still focused on national security as well as serious crime and the economic well-being of the country in so far as those interests were also relevant to the interests of national security (see paragraph 368 above). The Court will therefore turn to consider the other safeguards built into the section 8(4) regime in order to determine whether, when viewed as a whole, it was compliant with Article 8 of the Convention.

– *Circumstances in which an individual's communications may be intercepted*

372. Paragraph 6.2 of the IC Code (see paragraph 96 above) clearly stated that

> "[i]n contrast to section 8(1), a section 8(4) warrant instrument need not name or describe the interception subject or a set of premises in relation to which the interception is to take place. Neither does section 8(4) impose an express limit on the number of external communications which may be intercepted ...".

In other words, the communications bearers were targeted rather than the devices from which the communications were sent, or the senders or recipients of the communications. In the absence of any limit on the number of communications which could have been intercepted, it would appear that all packets of communications flowing across the targeted bearers while the warrant was in force were intercepted.

373. That being said, a section 8(4) warrant was a warrant for the interception of external communications (see paragraph 72 above) and paragraph 6.7 of the IC Code (see paragraph 96 above) required the intercepting agency conducting interception under a section 8(4) warrant to use its knowledge of the way in which international communications were routed, combined with regular surveys of relevant communications links, to identify those individual communications bearers that were most likely to contain external communications that met the description of material certified by the Secretary of State. The intercepting agency was also required to conduct the interception in ways that limited the collection of non-external communications to the minimal level compatible with the objective of intercepting wanted external communications. The bearers were not, therefore, chosen at random. On the contrary, they were selected because they were believed to be the most likely to carry external communications of intelligence interest.

374. Paragraph 6.5 of the IC Code defined "external communications" as communications which were either sent or received outside the British Islands (see paragraph 96 above). Where both the sender and recipient were within the British Islands, the communication was internal. Whether or not a communication was "external" therefore depended on the geographic location of the sender and recipient and not on the route the communication took to its destination. Communications which crossed the United Kingdom's borders (international communications) could still be "internal", since a communication (or packets of a communication) both sent from and received in the United Kingdom could nevertheless be routed through one or more third countries.

375. The distinction between internal and external communications did not, therefore, prevent the interception of internal communications travelling across the United Kingdom's borders, and in fact the "bycatch" of such communications was expressly permitted by section 5(6) RIPA, which provided that the conduct authorised by an interception warrant included the

interception of communications not identified by the warrant if necessary to do what was expressly authorised by the warrant (see paragraph 68 above). In addition, the definition of "external" was itself sufficiently broad to include cloud storage and the browsing and social media activities of a person in the United Kingdom (see paragraphs 75 and 76 above). Nevertheless, as the Chamber acknowledged, the "external communications" safeguard had a role to play at the macro level of selecting the bearers for interception (see paragraph 337 of the Chamber judgment); as the intercepting agency had to use its knowledge of the way in which international communications were routed to identify those communications bearers most likely to contain external communications of value to the operation, the safeguard did, albeit to a limited extent, circumscribe the categories of people liable to have their communications intercepted. It was also relevant to the question of proportionality, since States might have less intrusive measures available to them to obtain the communications of persons within their territorial jurisdiction.

376. In the light of the foregoing, the Court considers it clear that under the section 8(4) regime international communications (that is, communications crossing State borders) could be intercepted; and that the intelligence services would only use the power to intercept those bearers most likely to be carrying external communications of intelligence interest. In the bulk interception context it is difficult, in the abstract, to imagine how the circumstances in which an individual's communications might be intercepted could be further delimited. In any event, as neither the sender nor the recipient of an electronic communication could control the route it took to its destination, in practice any further restrictions on the choice of bearers would not have made domestic law any more foreseeable as to its effects. The Court would therefore accept that the circumstances in which an individual's communications could be intercepted under the section 8(4) regime were sufficiently "foreseeable" for the purposes of Article 8 of the Convention.

– *Procedure to be followed for granting authorisation*

377. An application for a section 8(4) warrant was made to the Secretary of State, who alone had the power to issue such a warrant. Prior to submission, each application was subject to a review within the agency making it. This involved scrutiny by more than one official, who had to consider whether the application was made for a purpose falling within section 5(3) RIPA and whether the proposed interception satisfied the Convention standards of necessity and proportionality (see paragraph 6.9 of the IC Code, at paragraph 96 above). This additional level of internal scrutiny was no doubt valuable, but it remained the case that at the relevant time bulk interception conducted under the section 8(4) regime was authorised by the Secretary of State and not by a body independent of the

executive. Consequently, the section 8(4) regime lacked one of the fundamental safeguards: namely, that bulk interception should be subject to independent authorisation at the outset (see paragraph 350 above).

378. As for the level of scrutiny provided by the Secretary of State, paragraph 6.10 of the IC Code set out in detail the information which had to be included in the application (see paragraph 96 above). This included a description of the communications to be intercepted, details of the CSP(s) and an assessment of the feasibility of the operation, where relevant; a description of the conduct to be authorised; the certificate that would regulate examination of intercept material (see paragraphs 378 and 379 below); an explanation of why the interception was considered necessary for one or more of the section 5(3) purposes; a consideration of why the conduct was proportionate to what was sought to be achieved; an assurance that intercept material would be read, looked at or listened to only in so far as it was certified and met the conditions of sections 16(2) to 16(6) RIPA; and an assurance that intercept material would be handled in accordance with the section 15 and section 16 safeguards.

379. The Secretary of State was therefore informed of the purpose of the operation (which had to be one of the section 5(3) purposes) and, before issuing a warrant, had to be satisfied that it was necessary for that purpose, and that it was proportionate to what it sought to achieve (see paragraphs 6.11 and 6.13 of the IC Code at paragraph 96 above). In assessing proportionality, the Secretary of State had to consider whether the warrant was excessive in the overall circumstances of the case and whether the information sought could reasonably have been obtained by less intrusive means (see paragraph 3.6 of the IC Code at paragraph 96 above). In particular, the size and scope of the interference had to be balanced against what was sought to be achieved; an explanation had to be given of how and why the methods would cause the least possible intrusion to the subject and others; consideration had to be given as to whether the activity was an appropriate way of achieving the necessary result, having considered all reasonable alternatives; and, as far as reasonably practicable, evidence had to be given of other methods considered but assessed as insufficient to fulfil operational objectives (see paragraph 3.7 of the IC Code at paragraph 96 above).

380. Although the application for a section 8(4) warrant had to include "a description of the communications to be intercepted" and "details of the Communications Service Provider(s)", the Government confirmed at the hearing that the warrant did not specify particular bearers, because there would be "serious impracticalities and difficulties" if that were to be a requirement. Nevertheless, there had to be a proper description of what the interception would involve and details of the "sorts of bearers" that would be intercepted. This information informed the Secretary of State's assessment of the necessity and proportionality of the conduct described in

the application. Furthermore, the Government confirmed in their submissions to the Grand Chamber that the IC Commissioner was briefed regularly by GCHQ about the basis on which bearers were selected for interception (see paragraph 290 above).

381. The application for a section 8(4) warrant also did not have to include an indication of the categories of selectors to be employed. As a consequence, there was no possibility for their necessity and proportionality to be assessed at the authorisation stage, although the choice of selectors was thereafter subject to independent supervision. In their submissions before the Grand Chamber the Government confirmed that whenever a new selector was added to the system, the analyst adding it had to complete a written record, explaining why it was necessary and proportionate to apply the selector for the purposes within the Secretary of State's certificate. This was done by the selection of text from a drop-down menu, followed by the addition, by the analyst, of free text explaining why it was necessary and proportionate to make the search. Furthermore, the use of selectors had to be recorded in an approved location that enabled them to be audited; created a searchable record of selectors in use; and enabled oversight by the IC Commissioner (see paragraphs 291-292 above). The choice of selectors was therefore subject to oversight by the IC Commissioner and in his 2016 annual report he "was impressed by the quality of the statements" prepared by analysts explaining the necessity and proportionality of adding a new selector (see paragraph 177 above).

382. Given that the choice of selectors and query terms determined which communications would be eligible for examination by an analyst, the Court has indicated that it is of fundamental importance for at least the categories of selectors to be identified in the authorisation and for those strong selectors linked to identifiable individuals to be subject to prior internal authorisation providing for separate and objective verification of whether the justification conforms to the aforementioned principles (see paragraphs 353-355 above).

383. In the present case, the absence of any oversight of the categories of selectors at the point of authorisation was a deficiency in the section 8(4) regime. Nor did the subsequent control of all individual selectors satisfy the requirement for enhanced safeguards for the use of strong selectors linked to identifiable individuals and the need to have in place a process of prior internal authorisation providing for separate and objective verification of whether the justification conforms to the above-mentioned principles (see paragraph 355 above). Although analysts had to record and justify the use of every selector with regard to the Convention principles of necessity and proportionality and that justification was subjected to independent supervision by the IC Commissioner, strong selectors linked to identifiable individuals were nevertheless not subject to prior internal authorisation.

– *Procedures to be followed for selecting, examining, and using intercept material*

384. Paragraph 6.4 of the IC Code stipulated that where a section 8(4) warrant resulted in the acquisition of large volumes of communications, authorised persons within the intercepting agency could apply strong selectors and complex queries to generate an index (see paragraph 96 above). This selection process was circumscribed by section 16(2) RIPA and paragraph 7.19 of the IC Code (see paragraphs 85 and 96 above), which provided that a selector could not refer to an individual known to be in the British Islands, or have as a purpose the identification of material contained in communications sent by or intended for him or her, unless the Secretary of State had personally authorised the use of the selector, having first been satisfied that it was necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or for the purpose of safeguarding the economic well-being of the United Kingdom, in so far as those interests were also relevant to the interests of national security, and that it was proportionate.

385. Only material on the index could be viewed by an analyst (see paragraphs 96 and 289 above); and no intelligence report could be made of any communications or communications data unless they had been viewed by an analyst (see paragraph 289 above). Moreover, paragraph 7.13 of the IC Code provided that only material described in the Secretary of State's certificate was available for human examination, and no official was permitted to gain access to the material other than as permitted by the certificate (see paragraph 96 above). Paragraph 6.4 further provided that before a particular communication could be accessed by an authorised person within the intercepting agency, the person had to explain why it was necessary for one of the reasons set out in the accompanying certificate, and why it was proportionate in the particular circumstances, having regard to whether the information could reasonably have been obtained by less intrusive means (see paragraph 96 above).

386. The Secretary of State's certificate was issued when he or she granted the warrant and was intended to ensure that a selection process was applied to the intercepted material so that only material described in the certificate was made available for human examination (see paragraphs 6.3 and 6.14 of the IC Code at paragraph 96 above). Although the certificate played an important role in regulating access to intercept material, the ISC report and that of the Independent Reviewer of Terrorism Legislation both criticised the fact that the material identified in those certificates was couched in very general terms (for example, "material providing intelligence on terrorism (as defined by the Terrorism Act 2000 (as amended))" – see paragraph 342 of the Chamber judgment and paragraphs 146 and 155 above). The Court agrees with the Chamber that

this was a deficiency in the system of safeguards available under the section 8(4) regime.

387. Nonetheless, according to the ISC, although the certificate set out the general categories of information which could be examined, in practice it was the selection of the bearers, the application of simple selectors and initial search criteria, and then complex searches which determined what communications were examined (see paragraphs 146-147 above). In other words, while the certificates regulated the analyst's selection of material from a computer-generated index, it was the choice of bearers and selectors/search terms which determined which communications were on that index (and therefore eligible for examination) in the first place. However, the Court has already held that both the failure to identify the categories of selectors in the application for a warrant and the absence of prior internal authorisation of those strong selectors linked to an identifiable individual represented deficiencies in the section 8(4) regime (see paragraph 382 above). These deficiencies would have been exacerbated by the general nature of the Secretary of State's certificate. Not only was there no prior independent authorisation of the categories of selectors used to generate the index, and no internal authorisation of those strong selectors linked to an identifiable individual, but also the certificate regulating access to material on that index was drafted in insufficiently precise terms to provide any meaningful restriction.

388. Paragraph 7.16 of the IC Code further required an analyst seeking access to material on the index to indicate any circumstances likely to give rise to a degree of collateral infringement of privacy, together with the measures taken to reduce the extent of that intrusion (see paragraph 96 above). Any subsequent access by the analyst was limited to a defined period of time, and if that period of time was renewed, the record had to be updated giving reasons for renewal (see paragraph 7.17 of the IC Code, at paragraph 96 above). According to paragraph 7.18 of the IC Code, regular audits were carried out which included checks to ensure that the records requesting access to material were compiled correctly, and that the material requested fell within the matters certified by the Secretary of State (see paragraph 96 above).

389. Furthermore, under paragraph 7.15, material gathered under a section 8(4) warrant could only be read, looked at or listened to by authorised persons (analysts) who had received regular mandatory training regarding the provisions of RIPA and the requirements of necessity and proportionality, and who had been appropriately vetted (see paragraph 96 above). Pursuant to paragraph 7.10, the vetting of each individual member of staff was periodically reviewed (see paragraph 96 above).

390. Paragraph 7.6 of the IC Code provided that intercept material could only be copied to the extent necessary for the authorised purposes and subject to a strict application of the "need-to-know principle", including

providing extracts or summaries where this was sufficient to satisfy the user's need to know. Section 15(5) RIPA required arrangements to be in place for securing that every copy of the material or data that was made was stored, for as long as it was retained, in a secure manner (see paragraph 81 above); and paragraph 7.7 further required that prior to its destruction, intercept material, and all copies, extracts and summaries of it, had to be stored securely and could not be accessible to persons without the required level of security clearance (see paragraph 96 above).

391. Subject to the aforementioned deficiencies relating to the authorisation of the selectors (see paragraphs 381 and 382 above) and the general nature of the Secretary of State's certificate (see paragraph 386 above), the Court considers that the circumstances in which intercept material could be selected, examined, used and stored under the section 8(4) regime were sufficiently "foreseeable" for the purposes of Article 8 of the Convention, and that they provided adequate safeguards against abuse.

– *Precautions to be taken when communicating intercept material to other parties*

392. Section 15(2) RIPA required that the following be limited to the minimum necessary for the "authorised purposes": the number of persons to whom the material or data were disclosed or made available; the extent to which the material or data were disclosed or made available; the extent to which the material or data were copied; and the number of copies that were made (see paragraph 78 above). Under section 15(4) RIPA and paragraph 7.2 of the IC Code, something was necessary for the authorised purposes if, and only if, it continued to be, or was likely to become, necessary for the purposes mentioned in section 5(3) RIPA; for facilitating the carrying-out of any of the interception functions of the Secretary of State; for facilitating the carrying-out of any functions of the IC Commissioner or of the IPT; to ensure that a person conducting a criminal prosecution had the information he or she needed to determine what was required by the duty to secure the fairness of the prosecution (although the intercept material could not itself be used in the prosecution of a criminal offence – see paragraph 8.3 of the IC Code at paragraph 96 above); or for the performance of any duty imposed on any person under public records legislation (see paragraphs 80 and 96 above).

393. Under paragraph 7.3 of the IC Code disclosure was prohibited except to persons who had been appropriately vetted and in accordance with the "need-to-know principle": intercepted material could not be disclosed to any person unless that person's duties, which had to relate to one of the authorised purposes, were such that he or she "needed to know" about the intercept material to carry out those duties. In the same way, only so much of the intercept material could be disclosed as was needed by the recipient (see paragraph 96 above). Paragraph 7.3 applied equally to disclosure to

additional persons within an agency, and to disclosure outside that agency (see paragraph 96 above). Under paragraph 7.4 it also applied not just to the original interceptor, but also to anyone to whom the intercept material was subsequently disclosed (see paragraph 96 above).

394. As the Chamber observed, since "likely to become necessary" was not further defined in RIPA or the IC Code, or indeed anywhere else, section 15(4) and paragraph 7.2 could in practice have given the authorities a broad power to disclose and copy intercept material. Nevertheless, the material could still only be disclosed to a person with the appropriate level of security clearance, who had a "need to know", and only so much of the intercept material as the individual needed to know could be disclosed. The Court therefore agrees with the Chamber that the inclusion of "likely to become necessary" did not significantly reduce the safeguards for the protection of data obtained by bulk interception (see paragraphs 368 and 369 of the Chamber judgment).

395. Turning to the transfer of intercept material outside the United Kingdom, where material has been intercepted in accordance with domestic law, the Court considers that the transfer of that material to a foreign intelligence partner or international organisation would only give rise to an issue under Article 8 of the Convention if the intercepting State did not first ensure that its intelligence partner, in handling the material, had in place safeguards capable of preventing abuse and disproportionate interference, and in particular, could guarantee the secure storage of the material and restrict its onward disclosure (see paragraph 362 above).

396. In the United Kingdom it would appear that Five Eyes partners could access elements of the product of GCHQ's interception warrants on their own systems (see paragraph 180 above). In such cases, the interception of the material by the United Kingdom intelligence services would have been conducted in accordance with domestic law including, in so far as is relevant in the present case, section 8(4) RIPA. According to paragraph 7.5 of the IC Code, where intercept material was disclosed to the authorities of a country or territory outside the United Kingdom, the intelligence services had to take reasonable steps to ensure that the authorities in question had and would maintain the necessary procedures to safeguard the intercept material, and to ensure that it was disclosed, copied, distributed and retained only to the minimum extent necessary. The intercept material could not be further disclosed to the authorities of a third country or territory unless explicitly agreed with the issuing agency and it had to be returned to the issuing agency or securely destroyed when no longer needed (see paragraph 96 above). Section 15(7) RIPA further provided that restrictions should be in force which would prevent the doing of anything in connection with legal proceedings outside the United Kingdom which would disclose the content or related communications data of an intercepted

communication where such a disclosure could not have been made in the United Kingdom (see paragraph 82 above).

397. In respect of confidential material, paragraph 4.30 of the IC Code provided that where confidential information was disseminated to an outside body, reasonable steps had to be taken to mark the information as confidential. Where there was any doubt as to the lawfulness of the proposed dissemination of confidential information, advice had to be sought from a legal adviser within the relevant intercepting agency and before any further dissemination of the material could take place (see paragraph 96 above).

398. There were therefore safeguards in place to ensure that intelligence partners would guarantee the secure storage of transferred material and restrict its onward disclosure. A final safeguard, to which the Court attaches particular weight, is the oversight provided by the IC Commissioner and the IPT (see paragraphs 411 and 414 below).

399. In the light of the foregoing, the Court considers that the precautions to be taken when communicating intercept material to other parties were sufficiently clear and afforded sufficiently robust guarantees against abuse.

– *Limits on the duration of interception, the storage of intercept material and circumstances in which such material must be erased or destroyed*

400. As regards the duration of section 8(4) warrants issued for reasons of national security or the economic well-being of the United Kingdom, in so far as those interests were also relevant to the interests of national security, pursuant to section 9 RIPA these warrants ceased to have effect after six months, unless they were renewed. Section 8(4) warrants issued by the Secretary of State for the purposes of preventing serious crime ceased to have effect after three months, unless renewed. These warrants were renewable for periods of six and three months respectively, and could be renewed at any point before their expiry date by application to the Secretary of State. That application had to contain the same information as the original application, together with an assessment of the value of the interception up to that point and an explanation of why its continuation was necessary, within the meaning of section 5(3), and proportionate (see section 9 RIPA at paragraph 67 above, and paragraphs 6.22-6.24 of the IC Code at paragraph 96 above). The Secretary of State had to cancel a warrant – even before the original expiry date – if satisfied that it was no longer necessary on section 5(3) grounds (see section 9 RIPA at paragraph 67 above).

401. In view of the clear limitation on the duration of section 8(4) warrants, and the requirement that they be kept under continuous review, the Court considers that the rules in respect of the duration of interception

under the section 8(4) regime were sufficiently clear and provided adequate safeguards against abuse.

402. Paragraph 7.9 of the IC Code provided that where an intelligence service received unanalysed intercept material and related communications data from interception under a section 8(4) warrant, it had to specify maximum retention periods for different categories of material which reflected its nature and intrusiveness. Those specified periods would normally be no longer than two years, and had to be agreed with the IC Commissioner. So far as possible, all retention periods had to be implemented by a process of automated deletion, triggered once the applicable maximum retention period had been reached (see paragraph 96 above). Pursuant to paragraph 7.8 of the IC Code, retained intercept material had to be reviewed at appropriate intervals to confirm that the justification for its retention was still valid under section 15(3) RIPA (see paragraph 96 above).

403. In their submissions to the Grand Chamber, the Government provided further information about the retention periods. Communications to which only the "strong selector" process was applied were discarded immediately unless they matched the strong selector. Communications to which the "complex query" process was also applied were retained for a few days, in order to allow the process to be carried out, and were then deleted automatically unless they had been selected for examination. Communications which had been selected for examination could be retained only where it was necessary and proportionate to do so. The default position was that the retention period for selected communications was no longer than a few months, after which they were automatically deleted (although if the material had been cited in intelligence reporting, the report would be retained), but in exceptional circumstances a case could be made to retain selected communications for longer (see paragraph 293 above). In practice, therefore, it would appear that the retention periods were significantly shorter than the two-year maximum retention period.

404. Lastly, section 15(3) RIPA and paragraph 7.8 of the IC Code required that every copy of intercept material (together with any extracts and summaries) be destroyed securely as soon as retention was no longer necessary for any of the section 5(3) purposes (see paragraphs 79 and 96 above).

405. In the *Liberty* proceedings, the IPT considered the arrangements for the retention of material and its destruction and found them to be adequate (see paragraph 50 above). The Court also considers that the "above the waterline" arrangements setting out the circumstances in which intercept material had to be erased or destroyed were sufficiently clear. However, in its view it would have been desirable for the shorter retention periods identified by the Government in the course of the present proceedings to

have been reflected in the appropriate legislative and/or other general measures.

– *Supervision*

406. Supervision of the section 8(4) regime was primarily carried out by the IC Commissioner, although according to that Commissioner a "critical quality assurance function [was] initially carried out by the staff and lawyers within the intercepting agency or the warrant-granting department", who provided independent advice to the Secretary of State and performed important pre-authorisation scrutiny of warrant applications and renewals to ensure that they were (and remained) necessary and proportionate (see paragraph 170 above).

407. The IC Commissioner was independent of the executive and the legislature, and had to have held high judicial office. His principal duty was to review the exercise and performance, by the relevant Secretaries of State and public authorities, of the powers under Part 1 (and to a limited extent Part 3) of RIPA and he oversaw an inspection regime that enabled him to carry out independent oversight of how the law was applied. He regularly reported on his activities, on a half-yearly basis, to the Prime Minister, and prepared an annual report which was placed before both Houses of Parliament. In addition, after each inspection a report was sent to the head of the inspected agency; the report contained formal recommendations and required the agency to report back within two months to confirm whether the recommendations had been implemented or what progress had been made. His periodic reports have been published from 2002, and from 2013 they were published in full with no confidential annexes. Furthermore, section 58(1) RIPA imposed a statutory obligation on every public official in an organisation within the IC Commissioner's remit to disclose or to provide to him all documents or information as might be required to enable him to carry out his functions (see paragraphs 135 and 136 above).

408. The IC Commissioner's 2016 report provides evidence of the extent of his oversight powers. In summary, during inspections he evaluated the systems in place for the interception of communications and ensured that all relevant records had been kept; examined selected interception applications to assess whether they met the necessity and proportionality requirements; interviewed case officers and analysts to assess whether interceptions and the justifications for acquiring all of the material were proportionate; examined any urgent oral approvals to check that the process was justified and used appropriately; reviewed those cases where communications subject to legal privilege or otherwise confidential information had been intercepted and retained, and any cases where a lawyer was the subject of an investigation; reviewed the adequacy of the safeguards and arrangements under sections 15 and 16 RIPA; investigated the procedures in place for the retention, storage and destruction of

intercepted material and related communications data; and reviewed reported errors and the sufficiency of any measures put in place to prevent recurrence (see paragraph 171 above).

409. In 2016 the IC Commissioner's office inspected all nine interception agencies once and the four main warrant-granting departments twice. Nine hundred and seventy warrants were inspected, representing 61% of the number of warrants in force at the end of the year and 32% of the total of new warrants issued in 2016 (see paragraphs 173 and 175 above).

410. Inspections usually involved a three-stage process. First, to achieve a representative sample of warrants, inspectors selected them across different crime types and national security threats, focusing on those of particular interest or sensitivity. Secondly, inspectors scrutinised the selected warrants and associated documentation in detail during reading days which preceded the inspections. At this stage, inspectors examined the necessity and proportionality statements made by analysts when adding a selector to the collection system for examination. Each statement had to stand on its own and had to refer to the overall requirement of priorities for intelligence collection. Thirdly, they identified those warrants, operations or areas of the process which required further information or clarification and arranged to interview relevant operational, legal or technical staff. Where necessary, they examined further documentation or systems relating to those warrants (see paragraph 174 above).

411. The IC Commissioner also had oversight of the sharing of intercept material with intelligence partners. In his 2016 report he indicated that GCHQ had provided his inspectors with "comprehensive details of the sharing arrangements whereby Five Eyes partners can access elements of the product of GCHQ's interception warrants on their own systems". In addition, his inspectors were able to meet with representatives of the Five Eyes community and they received a demonstration of how other Five Eyes members could request access to GCHQ's intercept material. He observed that "[a]ccess to GCHQ systems [was] tightly controlled and [had] to be justified in accordance with the laws of the host country and handling instructions of section 15/16 safeguards". He further observed that before obtaining any access to GCHQ's intercept material, Five Eyes analysts had to complete the same legalities training as GCHQ staff (see paragraph 180 above).

412. In the light of the foregoing, the Court is satisfied that the IC Commissioner provided independent and effective supervision of the operation of the section 8(4) regime. In particular, he and his inspectors were able to assess the necessity and proportionality of a significant number of warrant applications and the subsequent choice of selectors, and to investigate the procedures in place for the retention, storage and destruction of intercepted communications and related communications data. They were also able to make formal recommendations to the head of the public

authorities concerned and those authorities were required to report back, within two months, on the progress they had made in implementing those recommendations. Furthermore, the Government confirmed in their submissions to the Grand Chamber that the IC Commissioner was also briefed regularly by GCHQ about the basis on which bearers were selected for interception (see paragraphs 136 and 290 above). The intelligence services were required to keep records at each stage of the bulk interception process and they were obliged to grant inspectors access to those records (see paragraphs 6.27 and 6.28 of the IC Code at paragraph 96 above). Lastly, he also had oversight of the sharing of intercept material with intelligence partners (see paragraph 180 above).

– Ex post facto *review*

413. *Ex post facto* review was provided by the IPT, which in the present case was presided over at all relevant times by a High Court judge. The Chamber found – and the applicants have not disputed it – that the IPT provides an effective remedy for applicants complaining of both specific incidences of surveillance and the general Convention compliance of surveillance regimes (see paragraph 265 of the Chamber judgment). In this regard, the Chamber found it significant that the IPT had extensive jurisdiction to examine any complaint of unlawful interception which was not dependent on notification of the interception to its subject (see paragraph 122 above). Consequently, any person who believed that he or she had been subjected to secret surveillance could make an application to the IPT. To be appointed, its members had to have held high judicial office or to be a qualified lawyer of at least ten years' standing (see paragraph 123 above). Those involved in the authorisation and execution of an intercept warrant were required to disclose to it all the documents it might require, including "below the waterline" documents which could not be made public for reasons of national security (see paragraph 125 above). Furthermore, it had discretion to hold oral hearings, in public, where possible (see paragraph 129 above); in closed proceedings it could ask Counsel to the Tribunal to make submissions on behalf of claimants who could not be represented (see paragraph 132 above); and when it determined a complaint, it had the power to award compensation and make any other order it saw fit, including quashing or cancelling any warrant and requiring the destruction of any records (see paragraph 126 above). Lastly, the IPT's legal rulings were published on its own dedicated website, thereby enhancing the level of scrutiny afforded to secret surveillance activities in the United Kingdom (see *Kennedy*, cited above, § 167).

414. In addition, the IPT had jurisdiction to consider any complaint about the Convention compliance either of the transfer of intercept material to third parties, or of the regime governing the transfer of intercept material. In the present case, however, the applicants in the third of the joined cases

did not make any specific complaint in this respect in the course of the domestic proceedings. Rather, their complaints about intelligence sharing focused solely on the regime governing the receipt of intelligence from third countries (see paragraphs 467-516 below).

415. The Court is therefore satisfied that the IPT provided a robust judicial remedy to anyone who suspected that his or her communications had been intercepted by the intelligence services.

(γ) Related communications data

416. The Court has indicated that in the context of bulk interception, the interception, retention and searching of related communications data should be analysed by reference to the same safeguards applicable to content, but that the legal provisions governing the treatment of related communications data do not necessarily have to be identical in every respect to those governing the treatment of content (see paragraphs 363-364 above). In the United Kingdom section 8(4) warrants authorised the interception of both content and related communications data. The latter were, in most respects, treated identically under the section 8(4) regime. Thus, the deficiencies already identified in respect of that regime governing the interception of content (see paragraphs 377, 381 and 382 above) applied equally to related communications data, namely: the absence of independent authorisation (see paragraph 377 above); the failure to identify the categories of selectors in the application for a warrant (see paragraphs 381 and 382 above) and the failure to subject those selectors linked to identifiable individuals to prior internal authorisation; and the lack of foreseeability of the circumstances in which communications could be examined (see paragraph 391 above), having regard both to the failure to identify the categories of selectors in the application for a warrant (see paragraphs 381 and 382 above) and to the general nature of the Secretary of State's certificate (see paragraph 386 above).

417. At the same time, the treatment of communications data benefited in most part from the same safeguards as applied to content. Like the latter, the former were subject to an automated filtering process in near-real time, with a substantial proportion of them being instantly deleted at that stage; and they were also subject to simple or complex queries in order to draw out the material that was of potential intelligence value. Moreover, the selectors used in respect of related communications data were subject to the same safeguards as content; most notably, analysts had to complete a written record explaining why each new selector added to the system was necessary and proportionate. Furthermore, that record was subject to audit by the IC Commissioner, selectors had to be removed if it was established that they were not being used by their intended target, and there was a maximum time during which selectors could remain in use before a review was necessary (see paragraph 298 above).

418. Content and related communications data were also subject to many of the same procedures for storage, access, examination and use, the same precautions for communication to third parties, and the same procedures for erasure and destruction. In this regard, both content and related communications data were subject to the safeguards in section 15 RIPA; analysts wishing to access related communications data had to complete an auditable record explaining why access was necessary and proportionate; and no intelligence reporting could be made on the basis of related communications data unless and until they had been examined.

419. There were, however, two principal ways in which the bulk interception regime treated content and related communications data differently: related communications data were excluded from the section 16(2) safeguard, meaning that if an analyst wished to use a selector referable to an individual known for the time being to be in the British Islands, he or she was not required to have the use of that selector certified as necessary and proportionate by the Secretary of State; and related communications data which did not match either a strong selector or a complex query were not destroyed immediately, but were instead stored for a maximum period of up to several months (see paragraphs 296-298 above). The Court will therefore examine whether domestic law clearly defined the procedures to be followed for selecting related communications data for examination, and the limits on the duration of the storage of related communications data.

420. Under the section 8(4) regime, section 16(2) was the principal statutory safeguard circumscribing the process of selecting intercept material for examination. However, it was not the only safeguard. As already noted at paragraph 417 above, all new selectors had to be justified by analysts through the creation of a written record explaining why the choice of selector was both necessary and proportionate (see paragraphs 291-292 and 298 above); analysts wishing to examine related communications data had to complete a further record explaining why it was necessary and proportionate to do so, in pursuit of GCHQ's statutory functions (see paragraph 6.4 of the IC Code, at paragraph 96 above); and these records were subject to audit and oversight by the IC Commissioner (see paragraphs 135-136 and 381 above). According to the Government, it would not have been feasible to extend the section 16(2) safeguard to related communications data, since this would have required the Secretary of State to certify the necessity and proportionality of targeting the individual concerned in every case. The number of queries made against communications data was significantly higher than the number of queries made against content (possibly many thousands in any given week in relation to individuals known or believed to be in the United Kingdom), and in many of these cases the identity of the individual would not be known. In addition, the Government pointed out that related communications data had

a temporal quality, and having to delay the conducting of searches pending acquisition of an individual authority would seriously risk undermining their use in intelligence terms (see paragraph 296 above).

421. The Court accepts that related communications data are an essential tool for the intelligence services in the fight against terrorism and serious crime, and that there would be circumstances in which it was both necessary and proportionate to search for and access the related communications data of persons known to be in the United Kingdom. Moreover, while section 16(2) contains an important safeguard governing the process of selecting intercept material for examination, it is noteworthy that in assessing the regime governing the bulk interception of content, the Court placed considerably more weight on the existence or otherwise of an effective mechanism to ensure that the choice of selectors was subject to the Convention requirements of necessity and proportionality; and subject to both internal and external oversight. Therefore, while the Court would echo the concerns raised in respect of the choice and oversight of selectors at paragraphs 381 and 382 above, it does not consider that the exclusion of related communications data from the section 16(2) safeguard should carry decisive weight in the overall assessment.

422. As for the duration of storage, the Government contended that related communications data "requir[ed] more analytical work, over a lengthy period, to discover 'unknown unknowns'". That discovery could involve an exercise of piecing together disparate small items of communications data to form a "jigsaw" revealing a threat, and would include the possible examination of items that initially appeared to be of no intelligence interest. Discarding unselected communications data immediately, or even after a few days, would render that exercise impossible (see paragraph 297 above).

423. In the light of the foregoing, and in view of the fact that there was a maximum retention period, which did not exceed "several months", and that the difference in treatment was objectively and reasonably justified, the Court would accept that the storage provisions concerning related communications data were sufficiently robust, even though they differed in substance from the provisions relating to content. However, these retention periods were only disclosed in the proceedings before this Court. Consequently, the shorter retention periods were not evident to anyone reading the IC Code; nor was there any indication in the IC Code that the retention periods for related communications data were different from those in respect of content. In the Court's view, in order to meet the Article 8 requirement of "foreseeability", the retention periods disclosed in the proceedings before it should be included in appropriate legislative and/or other general measures.

(δ) Conclusion

424. The Court accepts that bulk interception is of vital importance to Contracting States in identifying threats to their national security. This has been recognised by the Venice Commission (see paragraph 196 above) and was the position adopted by the respondent Government and by the Governments of France and of the Netherlands in their third-party interventions (see paragraphs 300 and 303 above). It was also the conclusion of the Independent Reviewer of Terrorism Legislation, who, having examined a great deal of closed material, concluded that bulk interception was an essential capability: first, because terrorists, criminals and hostile foreign intelligence services had become increasingly sophisticated at evading detection by traditional means; and, secondly, because the nature of the global Internet meant that the route a particular communication would travel had become hugely unpredictable. Although he and his team considered alternatives to bulk interception (including targeted interception, the use of human sources and commercial cyberdefence products), they concluded that no alternative or combination of alternatives would be a sufficient substitute for the bulk interception power (see paragraph 166 above).

425. Nonetheless, the Court observes that there is considerable potential for bulk interception to be abused in a manner adversely affecting the rights of individuals to respect for their private life (see paragraph 347 above). Therefore, in a State governed by the rule of law, which is expressly mentioned in the Preamble to the Convention and is inherent in the object and purpose of Article 8 (see *Roman Zakharov*, cited above, § 228), the Court considers that, when viewed as a whole, the section 8(4) regime, despite its safeguards, including some robust ones as highlighted above (see, for example, paragraphs 412 and 415 above), did not contain sufficient "end-to-end safeguards" to provide adequate and effective guarantees against arbitrariness and the risk of abuse. In particular, it has identified the following fundamental deficiencies in the regime: the absence of independent authorisation, the failure to include the categories of selectors in the application for a warrant, and the failure to subject to prior internal authorisation selectors linked to an individual (see paragraphs 377-382 above). These weaknesses concerned not only the interception of the content of communications but also the interception of related communications data (see paragraph 416 above). While the IC Commissioner provided independent and effective oversight of the regime, and the IPT offered a robust judicial remedy to anyone who suspected that his or her communications had been intercepted by the intelligence services, these important safeguards were not sufficient to counterbalance the shortcomings highlighted in paragraphs 377-382 above.

426. In view of the aforementioned shortcomings, the Court finds that section 8(4) RIPA did not meet the "quality of law" requirement and was

therefore incapable of keeping the "interference" to what was "necessary in a democratic society".

427. There has accordingly been a violation of Article 8 of the Convention.

## C. Alleged violation of Article 10 of the Convention

428. The applicants in both the second and the third of the joined cases complained under Article 10 of the Convention about the section 8(4) regime, arguing that the protection afforded by Article 10 to privileged communications was of critical importance to them as journalists and NGOs respectively. However, as the Chamber declared the complaint by the applicants in the third of the joined cases inadmissible for failure to exhaust domestic remedies, only the Article 10 complaint relating to journalists is within the scope of the case referred to the Grand Chamber.

429. Article 10 of the Convention provides:

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

### *1. The Chamber judgment*

430. The Chamber found that as the surveillance measures under the section 8(4) regime were not aimed at monitoring journalists or uncovering journalistic sources, the interception of such communications could not, by itself, be characterised as a particularly serious interference with freedom of expression. However, it considered that the interference would be greater if those communications were selected for examination. If that were the case, the interference could only be "justified by an overriding requirement in the public interest" if it was accompanied by sufficient safeguards. In particular, the circumstances in which such communications could be selected intentionally for examination would have to be set out sufficiently clearly in domestic law, and there would have to be adequate measures in place to ensure the protection of confidentiality where such communications had been selected, either intentionally or otherwise, for examination. In the absence of any publicly available arrangements limiting the intelligence services' ability to search and examine confidential journalistic material

other than where it was justified by an overriding requirement in the public interest, the Chamber found that there had also been a violation of Article 10 of the Convention.

*2. The parties' submissions*

**(a) The applicants**

431. The applicants in the second of the joined cases argued that the bulk interception regime was in breach of Article 10 because the large scale interception and the maintaining of large databases of information had a chilling effect on freedom of communication for journalists.

432. In view of the fundamental importance of press freedom, the applicants submitted that any interference with journalistic freedom, and in particular the right to maintain confidentiality of sources, had to be attended with legal procedural safeguards commensurate with the importance of the principle at stake. In particular, the notion of "in accordance with the law" required that where a measure was capable of identifying journalistic sources or revealing journalistic material it had to have been authorised by a judge or other independent and impartial decision-making body; the review had to be *ex ante*; and the authorising body had to be invested with the power to determine whether it was "justified by an overriding requirement in the public interest" and, in particular, whether a less intrusive measure might have sufficed to serve the overriding public interest (see *Sanoma Uitgevers B.V. v. the Netherlands* [GC], no. 38224/03, 14 September 2010). None of these safeguards were present in the section 8(4) regime.

**(b) The respondent Government**

433. The Government argued first that there was no authority in the Court's case-law for the proposition that prior judicial (or independent) authorisation was required for the operation of a strategic monitoring regime by virtue of the fact that some journalistic material might be intercepted in the course of that regime's operation. Rather, the Court had drawn a sharp distinction between the strategic monitoring of communications and/or communications data, which might inadvertently "sweep up" some journalistic material, and measures that targeted journalistic material (they referred to *Weber and Saravia*, cited above, § 151, and, by contrast, to *Sanoma Uitgevers B.V.*, cited above, and *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, no. 39315/06, 22 November 2012). A requirement of prior judicial authorisation would make no sense in the context of bulk interception, since the judge could only be told that there was a possibility that the execution of the warrant might result in the interception of some confidential journalistic material.

434. That being said, the Government accepted the Chamber's conclusion that further protection was required at the point of selection for

examination. It therefore confirmed that the IC Code had been amended to provide that "[p]articular consideration should be given to the interception of communications or the selection for examination of content containing information where individuals might reasonably assume a high degree of confidentiality. This includes where the communications contain information that is legally privileged; confidential journalistic material or where communications identify a journalist's source".

**(c) The third-party interveners**

*(i) The Government of France*

435. The Government of France argued that the surveillance of journalists was permissible under Article 10 of the Convention if it pursued a legitimate aim and was necessary, and if the measure did not target the journalists and was not aimed at identifying their sources. No parallel could be drawn between the situation where journalists' communications were intercepted by chance, and where a decision of the national authorities required a journalist to reveal his or her sources.

*(ii) The Government of the Kingdom of Norway*

436. The Norwegian Government submitted that the wide margin of appreciation allowed under Article 8 with regard to the decision to introduce a bulk interception regime also logically applied when the decision was scrutinised from the point of view of Article 10. It would defeat the nature and purpose of a bulk interception regime if the Court were to subject the decision to set it up to the "justified by an overriding requirement in the public interest" test simply because some of the intercepted communications might involve contact with journalists.

*(iii) United Nations Special Rapporteur on the promotion of the right to freedom of opinion and expression*

437. The Special Rapporteur argued that surveillance measures interfered with the right to freedom of expression and therefore had to comply with Article 19(3) of the ICCPR, which required restrictions on expression to "only be such as are provided by law and are necessary" for the protection of the rights and reputations of others, national security, public order, or public health or morals. Mass surveillance programmes provided significant challenges to the requirement of accessible legislation, due to the complexity of how surveillance technologies functioned, vague legal standards for intercepting communications, and complicated and often classified administrative frameworks. In addition, there was a serious proportionality concern relating to interference with the work of journalists and protection of their sources. As human rights law afforded confidentiality a high standard of protection, restrictions should be

exceptional and implemented by judicial authorities only and circumventions not authorised by judicial authorities according to clear and narrow legal rules should not be used to undermine source confidentiality. In this regard, the scope of the protection of confidential communications had to take account of the broad understanding of "journalist" under the ICCPR.

*(iv) ARTICLE 19*

438. ARTICLE 19 urged the Court to extend the same protection to NGOs as it normally extended to journalists.

*(v) Helsinki Foundation for Human Rights*

439. The Helsinki Foundation submitted that the protection of journalistic sources was undermined not only by the surveillance of the content of journalists' communications, but also by the surveillance of related metadata which could, by itself, allow for the identification of sources and informants. It was especially problematic that confidential information could be acquired without the journalists' knowledge or control, thereby depriving them of their right to invoke confidentiality, and their sources of their ability to rely on guarantees of confidentiality.

*(vi) Media Lawyers Association*

440. The Media Lawyers Association expressed concern that mass surveillance regimes were capable of intercepting journalistic communications and communications data which could identify sources. In their view, the mere interception of journalistic material could interfere with Article 10 of the Convention, even if the material was not actually analysed. It was therefore imperative that appropriate safeguards were in place to protect the confidentiality of journalistic sources, regardless of the purpose for which information was collected. Moreover, a regime permitting States to intercept journalists' communications without prior judicial authorisation was more likely to affect journalism that was in the public interest because the nature of such stories meant that the State would have a particular interest in identifying the sources. The risk would be particularly grave where the source was a government whistle-blower. The chilling effect of the mere potential that such sources would be identified was significant. As a consequence, the Media Lawyers Association argued that at a minimum Article 10 required prior independent judicial oversight of any attempt to obtain journalistic material or identify journalistic sources, and that the judicial process be *inter partes*.

*(vii) National Union of Journalists and International Federation of Journalists*

441. The National Union of Journalists and the International Federation of Journalists submitted that the confidentiality of sources was indispensable for press freedom. They also expressed concern about the possible sharing of data retained by the United Kingdom with other countries. If confidential journalistic material were to be shared with a country which could not be trusted to handle it securely, it could end up in the hands of people who would harm the journalist or his or her source. In the interveners' view, the safeguards in the updated IC Code and the Acquisition and Disclosure of Communications Data Code of Practice were not adequate, especially where the journalist or the identification of his or her source was not the target of the surveillance measure.

### *3. The Court's assessment*

#### (a) General principles on the protection of journalists' sources

442. As freedom of expression constitutes one of the essential foundations of a democratic society, the Court has always subjected the safeguards for respect of freedom of expression in cases under Article 10 of the Convention to special scrutiny. The safeguards to be afforded to the press are of particular importance, and the protection of journalistic sources is one of the cornerstones of freedom of the press. Without such protection, sources may be deterred from assisting the press in informing the public about matters of public interest. As a result the vital public-watchdog role of the press may be undermined, and the ability of the press to provide accurate and reliable information may be adversely affected (see, *inter alia*, *Goodwin v. the United Kingdom*, 27 March 1996, § 39, *Reports* 1996-II; *Sanoma Uitgevers B.V.*, cited above, § 50; and *Weber and Saravia*, cited above, § 143).

443. Orders to disclose sources potentially have a detrimental impact, not only on the source, whose identity may be revealed, but also on the newspaper or other publication against which the order is directed, whose reputation may be negatively affected in the eyes of future potential sources by the disclosure; and on members of the public, who have an interest in receiving information imparted through anonymous sources. There is, however, "a fundamental difference" between the authorities ordering a journalist to reveal the identity of his or her sources, and the authorities carrying out searches at a journalist's home and workplace with a view to uncovering his or her sources (compare *Goodwin*, cited above, § 39, with *Roemen and Schmit v. Luxembourg*, no. 51772/99, § 57, ECHR 2003-IV). The latter, even if unproductive, constitutes a more drastic measure than an order to divulge a source's identity, since investigators who raid a journalist's workplace have access to all the documentation held by the journalist (see *Roemen and Schmit*, cited above, § 57).

444. An interference with the protection of journalistic sources cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest (see *Sanoma Uitgevers B.V.*, cited above, § 51; *Goodwin*, cited above, § 39; *Roemen and Schmit*, cited above, § 46; and *Voskuil v. the Netherlands*, no. 64752/01, § 65, 22 November 2007). Furthermore, any interference with the right to protection of journalistic sources must be attended with legal procedural safeguards commensurate with the importance of the principle at stake (see *Sanoma Uitgevers B.V.*, cited above, §§ 88-89). First and foremost among these safeguards is the guarantee of review by a judge or other independent and impartial decision-making body with the power to determine whether a requirement in the public interest overriding the principle of protection of journalistic sources exists prior to the handing-over of such material and to prevent unnecessary access to information capable of disclosing the sources' identity if it does not (ibid., §§ 88-90).

445. Given the preventive nature of such review, the judge or other independent and impartial body must be in a position to carry out this weighing-up of the potential risks and respective interests prior to any disclosure and with reference to the material that it is sought to have disclosed so that the arguments of the authorities seeking the disclosure can be assessed properly. The decision to be taken should be governed by clear criteria, including whether a less intrusive measure can suffice to serve the overriding public interests established. It should be open to the judge or other authority to refuse to make a disclosure order or to make a limited or qualified order so as to protect sources from being revealed, whether or not they are specifically named in the withheld material, on the grounds that the communication of such material creates a serious risk of compromising the identity of a journalist's sources (ibid., § 92, and see *Nordisk Film & TV A/S v. Denmark* (dec.), no. 40485/02, ECHR 2005-XIII). In situations of urgency, a procedure should exist to identify and isolate, prior to the exploitation of the material by the authorities, information that could lead to the identification of sources from information that carries no such risk (see, *mutatis mutandis*, *Wieser and Bicos Beteiligungen GmbH v. Austria*, no. 74336/01, §§ 62-66, ECHR 2007-XI).

**(b) Article 10 in the bulk interception context**

446. In *Weber and Saravia* the Court recognised that the "strategic monitoring" regime had interfered with the first applicant's freedom of expression as a journalist. However, in so finding it considered it decisive that the surveillance measures were not aimed at monitoring journalists or uncovering journalistic sources. As such, it found that the interference with the first applicant's freedom of expression could not be characterised as particularly serious and, in view of the attendant safeguards, it declared her

complaints inadmissible as manifestly ill-founded (see *Weber and Saravia*, cited above, §§ 143-45 and 151).

**(c) Approach to be adopted in the present case**

447. Under the section 8(4) regime, confidential journalistic material could have been accessed by the intelligence services either intentionally, through the deliberate use of selectors or search terms connected to a journalist or news organisation, or unintentionally, as a "bycatch" of the bulk interception operation.

448. Where the intention of the intelligence services is to access confidential journalistic material, for example, through the deliberate use of a strong selector connected to a journalist, or where, as a result of the choice of such strong selectors, there is a high probability that such material will be selected for examination, the Court considers that the interference will be commensurate with that occasioned by the search of a journalist's home or workplace; regardless of whether or not the intelligence services' intention is to identify a source, the use of selectors or search terms connected to a journalist would most likely result in the acquisition of significant amounts of confidential journalistic material which could undermine the protection of sources to an even greater extent than an order to disclose a source (see *Roemen and Schmit*, cited above, § 57). Therefore, the Court considers that before the intelligence services use selectors or search terms known to be connected to a journalist, or which would make the selection of confidential journalistic material for examination highly probable, the selectors or search terms must have been authorised by a judge or other independent and impartial decision-making body invested with the power to determine whether they were "justified by an overriding requirement in the public interest" and, in particular, whether a less intrusive measure might have sufficed to serve the overriding public interest (see *Sanoma Uitgevers B.V.*, cited above, §§ 90-92).

449. Even where there is no intention to access confidential journalistic material, and the selectors and search terms used are not such as to make the selection of confidential journalistic material for examination highly probable, there will nevertheless be a risk that such material could be intercepted, and even examined, as a "bycatch" of a bulk interception operation. In the Court's view, this situation is materially different from the targeted surveillance of a journalist through either the section 8(1) or the section 8(4) regime. As the interception of any journalistic communications would be inadvertent, the degree of interference with journalistic communications and/or sources could not be predicted at the outset. Consequently, it would not be possible at the authorisation stage for a judge or other independent body to assess whether any such interference would be "justified by an overriding requirement in the public interest" and, in

particular, whether a less intrusive measure might have sufficed to serve the overriding public interest.

450. In *Weber and Saravia* the Court held that the interference with freedom of expression caused by strategic monitoring could not be characterised as particularly serious as it was not aimed at monitoring journalists and the authorities would know only when examining the intercepted telecommunications, if at all, that a journalist's communications had been monitored (see *Weber and Saravia*, cited above, § 151). Therefore, it accepted that the initial interception, without examination of the intercepted material, did not constitute a serious interference with Article 10 of the Convention. Nevertheless, as the Court has already observed, in the current, increasingly digital, age technological capabilities have greatly increased the volume of communications traversing the global Internet, and as a consequence surveillance which is not targeted directly at individuals has the capacity to have a very wide reach indeed, both within and without the territory of the surveilling State (see paragraphs 322-323 above). As the examination of a journalist's communications or related communications data by an analyst would be capable of leading to the identification of a source, the Court considers it imperative that domestic law contain robust safeguards regarding the storage, examination, use, onward transmission and destruction of such confidential material. Moreover, even if a journalistic communication or related communications data have not been selected for examination through the deliberate use of a selector or search term known to be connected to a journalist, if and when it becomes apparent that the communication or related communications data contain confidential journalistic material, their continued storage and examination by an analyst should only be possible if authorised by a judge or other independent and impartial decision-making body vested with the power to determine whether continued storage and examination is "justified by an overriding requirement in the public interest".

**(d) Application of the aforementioned test to the facts of the present case**

451. In *Weber and Saravia* the Court expressly recognised that the impugned surveillance regime had interfered with the first applicant's right to freedom of expression as a journalist (see *Weber and Saravia*, cited above, §§ 143-45). In the present case, the Court has accepted that the operation of the section 8(4) regime interfered with all of the applicants' rights under Article 8 of the Convention (see paragraphs 324-331 above). As the applicants in the second of the joined cases were a news-gathering organisation and a journalist respectively, the Court would accept that the section 8(4) regime also interfered with their right under Article 10 of the Convention to freedom of expression as journalists.

452. As already noted above, the section 8(4) regime had a clear basis in domestic law (see paragraphs 365 and 366 above). However, in assessing

foreseeability and necessity under Article 8 of the Convention, the Court identified the following deficiencies in the regime and its attendant safeguards: the absence of independent authorisation (see paragraph 377 above); the failure to identify the categories of selectors in the application for a warrant (see paragraphs 381-382 above); and the absence of prior internal authorisation for selectors linked to an identifiable individual (see paragraph 382 above).

453. Nonetheless, some additional safeguards in respect of confidential journalistic material were set out in paragraphs 4.1-4.3 and 4.26-4.31 of the IC Code (see paragraph 96 above). According to paragraph 4.1, any application for a warrant had to state whether the interception was likely to give rise to a collateral infringement of privacy, including where journalistic communications were involved and, where possible, it had to specify the measures to be taken to reduce the extent of the collateral intrusion. However, paragraph 4.1 only required the Secretary of State to take these circumstances and measures into account when considering an application for a section 8(1) warrant, that is, a warrant authorising targeted interception. Paragraph 4.2 further provided that "particular consideration should also be given" in cases where confidential journalistic material might have been involved, and paragraph 4.26 stated that "particular consideration" had to be given to the interception of communications that involved confidential journalistic material.

454. According to the Government, paragraph 4.28 of the IC Code also applied to confidential journalistic material. Where the intention was to acquire confidential *personal* information, paragraph 4.28 indicated that the reasons and the specific necessity and proportionality of doing so had to be documented clearly. If the acquisition of such material was likely but not intended, any possible mitigation steps had to be considered and, if none were available, consideration had to be given to whether special handling arrangements were required within the intercepting agency (see paragraph 96 above). The Court notes, however, that in paragraph 4.26 of the IC Code, "confidential personal information" appeared to be something distinct from "confidential journalistic material" (see paragraph 96 above).

455. As to the storage of confidential material, paragraph 4.29 of the IC Code provided that such material could only be retained where it was necessary and proportionate for one of the authorised purposes in section 15(4) RIPA, and it had to be destroyed securely when it was no longer needed for one of those purposes (see paragraph 96 above). Furthermore, according to paragraph 4.30, if it was retained or disseminated to an outside body, reasonable steps had to be taken to mark the information as confidential. Where there was any doubt as to the lawfulness of the proposed dissemination of confidential information, advice had to be sought from a legal adviser within the relevant intercepting agency and before any further dissemination of the material could take place (see paragraph 96

above). Lastly, paragraph 4.31 required that the IC Commissioner be notified of the retention of such material as soon as reasonably practicable, and that such material be made available to him on request (see paragraph 96 above).

456. In the light of the above, the Court would accept that the safeguards in the IC Code concerning the storage, onward transmission and destruction of confidential journalistic material were adequate. However, the additional safeguards in the IC Code did not address the weaknesses identified by the Court in its analysis of the regime under Article 8 of the Convention, nor did they satisfy the requirements identified by the Court at paragraphs 448-450 above. In particular, there was no requirement that the use of selectors or search terms known to be connected to a journalist be authorised by a judge or other independent and impartial decision-making body vested with the power to determine whether it was "justified by an overriding requirement in the public interest" and whether a less intrusive measure might have sufficed to serve the overriding public interest. On the contrary, where the intention was to access confidential journalistic material – or at least that was highly probable, in view of the use of selectors connected to a journalist – all that was required was that the reasons for doing so, and the necessity and proportionality of doing so, be documented clearly.

457. Moreover, there were insufficient safeguards in place to ensure that once it became apparent that a communication which had not been selected for examination through the deliberate use of a selector or search term known to be connected to a journalist nevertheless contained confidential journalistic material, it could only continue to be stored and examined by an analyst if authorised by a judge or other independent and impartial decision-making body vested with the power to determine whether its continued storage and examination was "justified by an overriding requirement in the public interest". Instead, all that was required by paragraph 4.2 of the IC Code was that "particular consideration" be given to any interception which might have involved the interception of confidential journalistic material, including consideration of any possible mitigation steps (see paragraph 96 above).

458. In view both of this weakness, and those identified by the Court in its consideration of the complaint under Article 8 of the Convention, it finds that there has also been a breach of Article 10 of the Convention by virtue of the operation of the section 8(4) regime.

## III. RECEIPT OF INTELLIGENCE FROM FOREIGN INTELLIGENCE SERVICES

### A. Article 8 of the Convention

459. The applicants in the first of the joined cases complained about the receipt by the United Kingdom authorities of material from foreign intelligence services. The applicants in the third of the joined cases complained more specifically that the respondent State's receipt of material intercepted by the NSA under PRISM and Upstream was in breach of their rights under Article 8 of the Convention.

#### *1. Scope of the complaint before the Grand Chamber*

460. In the *Liberty* proceedings the IPT identified three categories of material which could be received from foreign intelligence partners: unsolicited intercept material; solicited intercept material; and non-intercept material. As the Government informed the Chamber that it was "implausible and rare" for intercept material to be obtained "unsolicited", the Chamber did not examine material falling into this category (see paragraph 417 of the Chamber judgment). The Chamber also declined to examine the receipt of non-intercept material, since the applicants had not specified the kind of material foreign intelligence services might obtain by methods other than interception and, as such, it was not satisfied that they had demonstrated that its acquisition would interfere with their Article 8 rights (see paragraph 449 of the Chamber judgment). The applicants have not contested either of these findings.

461. Furthermore, as the *Liberty* proceedings were brought by the applicants in the third of the joined cases, the IPT only considered the receipt of intelligence from the NSA. In their submissions before the Chamber and the Grand Chamber, the parties also focused on the receipt of material from the NSA.

462. The Grand Chamber will therefore limit its examination to the complaint about the receipt of solicited intercept material from the NSA.

#### *2. The respondent Government's preliminary objection*

463. The Government argued that the applicants in the first and third of the joined cases could not claim to be victims of the alleged violation because neither of the two conditions in *Roman Zakharov* (cited above, § 171) were met (namely, the applicants could not possibly have been affected by the legislation permitting secret surveillance measures, and remedies were available at the national level). In particular, they argued that the applicants had put forward no basis on which they were at realistic risk either of having their communications intercepted under PRISM or

Upstream, or of having their communications requested by the United Kingdom intelligence services. In addition, they submitted that the applicants had available to them an effective domestic remedy to discover whether they were the subject of unlawful intelligence sharing.

**(a) The Chamber judgment**

464. As the Chamber accepted that the IPT had afforded the applicants an effective remedy for their Convention complaint, it considered that they could only claim to be "victims" on account of the mere existence of the intelligence sharing regime if they were able to show that they were potentially at risk of having their communications obtained by the United Kingdom authorities through a request to a foreign intelligence service (see paragraphs 392-93 of the Chamber judgment, referring to *Roman Zakharov*, cited above, § 171).

465. On the basis of the information submitted to it, the Chamber found that the applicants were potentially at risk both of having their communications obtained by a foreign intelligence service, and requested from a foreign intelligence service by the United Kingdom authorities (see paragraph 395 of the Chamber judgment). Although they could only have had their communications requested if there was either a section 8(1) or 8(4) warrant in place which covered their communications, it was clear from the *Liberty* proceedings that at least two of the applicants in the third of the joined cases had their communications lawfully intercepted and selected for examination by the United Kingdom intelligence services under the section 8(4) regime. While the Chamber found no reason to believe that these applicants were themselves of interest to the intelligence services, it observed that their communications could have been obtained lawfully under the section 8(4) regime if, as they claimed, they were in contact with persons who were. Similarly, their communications could have been requested lawfully from a third country under the intelligence sharing regime if they were in contact with an individual who was the subject of a request.

466. As Upstream functioned in a similar manner to the section 8(4) regime, the Chamber also accepted that the applicants' communications could potentially have been obtained by the NSA.

**(b) The Court's assessment**

467. The applicants have not challenged the Chamber's finding that the IPT offered an effective domestic remedy for Convention complaints about the operation of a surveillance regime, and, for the reasons expounded in paragraphs 413-415 above, the Grand Chamber agrees with that finding. Therefore, as the Chamber observed, the applicants could only claim to be "victims" on account of the mere existence of the intelligence sharing

regime if they were able to show that they were potentially at risk of having their communications obtained by the United Kingdom authorities through a request to a foreign intelligence service (see *Roman Zakharov*, cited above, § 171). This would only be the case if they were potentially at risk both of having their communications intercepted by a foreign intelligence service and of having those communications requested by GCHQ.

468. The Government, focusing on the receipt of intelligence from the United States, argued that the applicants were not potentially at risk of having their communications intercepted under Upstream, as it was a targeted interception regime. However, according to the NSA, prior to April 2017 Upstream acquired communications to, from or about a section 702 selector (such as an email address); and only from April 2017 onwards did it acquire communications to or from a section 702 selector (see paragraph 263 above). Given that section 702 selectors were applied to all communications flowing over specified cables, it would appear that Upstream was not so very different from the section 8(4) regime, which also intercepted all communications flowing over a number of cables and filtered them using selectors. The only apparent difference between the two regimes was that from April 2017, the NSA could only search for communications to or from a strong selector, while GCHQ retained the ability to perform searches by way of complex queries.

469. In the course of the *Liberty* proceedings, the IPT confirmed that at least two of the applicants in the third of the joined cases had not only had some of their communications intercepted pursuant to a section 8(4) warrant, but had also had those communications lawfully and proportionately retained pursuant to that warrant (see paragraphs 58-60 above). In order to have been retained lawfully those communications must have matched either a "strong selector" (pertaining either to the applicants or someone they were in contact with) or a "complex query". The Court would accept that if some of the applicants' communications matched a "strong selector" used by GCHQ, they would also have been potentially at risk of being intercepted and retained by the NSA under Upstream on the basis that they were "to" or "from" a section 702 selector. Even if they did not match a strong selector, some of the applicants' communications must nevertheless have been of intelligence interest. Prior to April 2017 they could also have been intercepted and retained under Upstream if they were "about" a section 702 selector. If this was the case, at the relevant time (that is, 7 November 2017) those communications may still have been held by the NSA since, following the change in policy in April 2017, it only indicated that it would delete previously acquired Upstream Internet communications "as soon as practicable" (see paragraph 263 above). Therefore, communications acquired before that date which were "about" a strong selector might have continued to be stored by the NSA for some time thereafter.

470. Consequently, the Court would accept that at the relevant time (that is, 7 November 2017) the applicants in the first and third of the joined cases were potentially at risk of having had at least some of their communications intercepted and retained under Upstream.

471. Nevertheless, the applicants could still only be victims for the purposes of the intelligence sharing regime if they were also potentially at risk of having their communications requested by GCHQ, and such a request could only have been made where a warrant was already in place for the material sought. However, as the Court has already noted, the fact that the communications of at least two of the applicants in the third of the joined cases were retained by GCHQ suggests that at least some of their communications were covered by a section 8(4) warrant. Consequently, the Court would accept that the applicants in the first and third of the joined cases were potentially at risk of also having their communications requested by GCHQ.

472. Accordingly, it finds that the applicants in the first and third of the joined cases can claim to be victims in respect of their complaints about the intelligence sharing regime. The Government's preliminary objection is therefore dismissed.

### *3. Merits*

#### (a) The Chamber judgment

473. In considering the Article 8 compliance of the regime governing the receipt of intercept material from foreign intelligence services such as the NSA, the Chamber applied a modified version of the six minimum safeguards (see paragraph 275). Since the first two requirements could not apply to the act of requesting intercept material from foreign governments, the Chamber instead asked whether the circumstances in which intercept could be requested was circumscribed sufficiently to prevent States from using the power to circumvent domestic law or their Convention obligations. It then applied the final four requirements to the treatment of intercept material once it had been obtained by the United Kingdom intelligence services.

474. The Chamber considered that the domestic law, together with the clarifications brought by the amendment of the IC Code, indicated with sufficient clarity the procedure for requesting either interception or the conveyance of intercept material from foreign intelligence services. Moreover, the Chamber found no evidence of any significant shortcomings in the application and operation of the regime. It therefore held, by a majority, that there had been no violation of Article 8 of the Convention.

**(b) The parties' submissions**

475. The applicants submitted that the safeguards in place in respect of the intelligence sharing regime were inadequate. In particular, they argued that the problems which had led the Chamber to find a violation of Article 8 of the Convention in respect of the bulk interception regime (that is, the lack of oversight of the use of selectors and the inadequate safeguards in respect of related communications data) applied equally to the intelligence sharing regime.

476. The Government, on the other hand, submitted that the intelligence sharing regime had a clear basis in domestic law, being set down in statute supplemented by Chapter 12 of the IC Code; and that law had been accessible. With regard to foreseeability, the Government argued that instead of applying a modified version of the six minimum safeguards, the Chamber should instead have applied the more general test – commonly applied in intelligence gathering cases which did not involve the interception of communications – of whether the law indicated the scope of any discretion and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference. In any event, the Government contended that the intelligence sharing regime satisfied the six minimum safeguards. The IC Code clearly described the nature of offences which could lead to intelligence being obtained; the limits on the duration of such obtaining; the process for examining, using and storing the intelligence obtained; and the circumstances in which the intelligence was to be erased or destroyed.

477. Lastly, in the Government's view there was no good reason to single out intercepted communications and related communications data from other types of information that might in principle be obtained from a foreign intelligence service, such as intelligence from covert human intelligence sources, or covert audio/visual surveillance. Indeed, in many cases the intelligence services might not even know whether communications provided to them by a foreign intelligence service had been obtained as a result of interception.

**(c) Observations of the third-party interveners**

*(i) The Government of France*

478. The French Government pointed out that intelligence sharing between partner services – either on an *ad hoc* or regular basis – was vitally important, especially in the fight against the increasingly transnational and diffusive threats which States had to prevent, primarily by identifying suspects before they acted. That fight justified the development of an intelligence community, without which intelligence services, with their limited ability to act overseas, would be unable to accomplish the task assigned to them.

479. The French Government further submitted that in the context of intelligence sharing the interference occurred not with the interception but rather with the obtaining of information, even if the material was intercepted at the behest of the receiving State. It noted the approach taken by the Chamber in analysing the United Kingdom intelligence sharing regime and invited the Grand Chamber to adopt the same approach.

480. In the Government's view, the reliability of the receiving service was one of the main criteria on which the sending State based its decision to exchange data, and as a consequence the receiving State had to guarantee the strict confidentiality of the information communicated to it. Therefore, the guarantees required for the handling of intelligence collected through an exchange of data with a partner service had to be in keeping with the "third party rule", which prohibited an agency which had received information from a foreign partner from sharing it with a third party without the consent of the originator. Without such an assurance, States might refuse to transfer information.

*(ii) United Nations Special Rapporteur on the promotion of the right to freedom of opinion and expression*

481. The Special Rapporteur argued that the same standards should apply to the acquisition of data from foreign intelligence services as applied when the domestic authorities acquired data themselves. A contrary position could lead State authorities to *de facto* outsource surveillance operations circumventing the protections afforded in the ICCPR.

*(iii) Access Now*

482. Access Now contended that while Mutual Legal Assistance Treaties (MLATs) offered a transparent and formal process for one State party to request intelligence from another, the operation of secret signals intelligence programmes (for example, the Five Eyes intelligence sharing network of which the United Kingdom, the United States of America, Australia, Canada and New Zealand were members) were not transparent and were prohibited by international human rights standards. Such secret programmes were not necessary, since the relevant intelligence could be obtained under MLATs.

*(iv) Dutch Against Plasterk ("Burgers tegen Plasterk")*

483. Dutch Against Plasterk, a coalition of five individuals and four associations, were applicants in a case against the Netherlands in which they sought to challenge the exchange of data between the Dutch authorities and their foreign intelligence partners (including the United States and the United Kingdom).

484. In their third-party intervention before the Court, the coalition argued that the sharing of intelligence should only be permitted if it was accompanied by sufficient safeguards and the foreign authority had a sound legal basis for capturing the material. Otherwise, there could be a circumvention of the protection provided by Article 8 of the Convention. States should not be allowed to obtain material from foreign authorities that they could not lawfully capture themselves.

*(v) Center for Democracy & Technology ("the CDT") and Pen American Center (PEN America)*

485. The CDT and PEN America argued that the circumstances of international cooperation in bulk data and communications surveillance required that at least three conditions were met: that States actively assessed and satisfied themselves as to the adequacy of their foreign partners' legal and administrative framework governing interception, and set out these adequacy measures in domestic law; that there was independent – preferably judicial – authorisation, based on a finding of reasonable suspicion, for the use of selectors identifiable to specific targets to query information obtained from foreign partners; and that there was a requirement of subsequent notification to the surveillance subjects.

486. The CDT and PEN America submitted that the interception regimes operated by the NSA – most notably, under section 702 FISA and Executive Order 12333 – would satisfy neither the "in accordance with the law" nor the "proportionality" requirements of Article 8 of the Convention, and these deficiencies tainted the lawfulness of the United Kingdom's intelligence sharing regime.

*(vi) European Network of National Human Rights Institutions*

487. The third-party intervener provided examples from Contracting States which in its view showed that the nature of international intelligence sharing had changed significantly so that it had become difficult to distinguish between "solicited" and "unsolicited" data. Historically, international intelligence sharing had involved the transfer of evaluated data, or finished intelligence. However, the advent of new technology had resulted in the increasing exchange of unevaluated "raw" data. Even where there was an agreement governing bilateral or multilateral intelligence cooperation the advent of automation and big data made it much more challenging to evaluate what one party received from another, including whether the information remained within the parameters of the original request. Consequently, there was a need for robust independent oversight of international intelligence sharing without distinction between solicited and unsolicited data. Oversight bodies should be legally mandated to oversee all matters of international cooperation by their intelligence services; cooperate

with independent oversight bodies from the third States involved in the intelligence sharing; and hire independent specialists, with expertise in modern information and communications technology, where required.

*(vii) Human Rights Watch*

488. Although the present applications focused on the receipt of foreign intelligence from the United States, Human Rights Watch believed that the network of States with which communications intelligence was shared was vastly larger. For example, the "Five Eyes Alliance" comprised the United Kingdom, the United States, Australia, Canada and New Zealand, and there were also thought to be other, more restricted intelligence sharing coalitions (for example, the "Nine Eyes", adding Denmark, France, the Netherlands and Norway; the "Fourteen Eyes", adding Germany, Belgium, Italy, Spain and Sweden; and the "Forty-One Eyes", adding in others in the allied coalition in Afghanistan).

*(viii) Open Society Justice Initiative*

489. The Open Society Justice Initiative argued that States should not receive or request data from a third party in a manner that circumvented individuals' Article 8 rights. To ensure that this did not happen, safeguards were required at the point when the material was first gathered, including prior scrutiny of the human rights record and interception laws and practices in the foreign State, and independent, preferably judicial, *a posteriori* oversight of any sharing arrangements to ensure that the safeguards were in place and enforced.

*(ix) Electronic Privacy Information Center (EPIC)*

490. EPIC submitted that United States law authorised mass, indiscriminate surveillance of non-US persons. This surveillance took place pursuant to section 702 FISA and Executive Order 12333. Surveillance under section 702 took place in the United States with the compelled assistance of service providers and it targeted non-US persons reasonably believed to be located outside the United States. There was no prior judicial review of surveillance activity; no reasonable suspicion was required; and there was no statutory obligation to notify subjects of surveillance. All that was required was that the FISC annually review the targeting and minimisation procedures aimed at limiting the acquisition of the communications of US persons or persons located in the United States.

491. Executive Order 12333 authorised the NSA to acquire foreign intelligence and counterintelligence. The order provided broad authority to conduct signals intelligence surveillance from a wide variety of sources, including fibre optic networks. Collection occurred outside the territory of the United States. There were no reports or official disclosures concerning

the scope of surveillance under the order, which was not subject to judicial oversight.

492. In EPIC's view, surveillance by the NSA would violate Article 8 of the Convention for failure to limit the scope of application and duration, and the failure to provide adequate supervision, notice and remedies.

*(x) International Commission of Jurists*

493. The International Commission of Jurists referred the Court to Articles 15 and 16 of the Draft Articles on State Responsibility of the International Law Commission ("the ILC Draft Articles"). It contended that, under Article 15, a Contracting State could be responsible for mass surveillance conducted by a non-Contracting State if it was acting in organised and structured forms of cooperation; and that, under Article 16, a Contracting State could be responsible for mass surveillance conducted by a non-Contracting State if it contributed to the surveillance programme and had actual or constructive knowledge of the breaches of international human rights obligations inherent in the system. The International Commission of Jurists further submitted that Contracting States participating in or contributing to a mass surveillance programme were obliged to establish a system of safeguards for the protection of Article 8 rights, and were also under a duty to protect persons within their jurisdiction from violations of Article 8 rights caused by mass surveillance programmes.

*(xi) Law Society of England and Wales*

494. The Law Society submitted that the section 8(4) regime and associated Codes provided no robust or transparent safeguards for legally privileged material. Since the same safeguards applied to privileged material obtained by foreign States and disclosed to the intelligence services of the United Kingdom, the same deficiencies also tainted that regime.

**(d) The Court's assessment**

*(i) The applicable test*

495. In the Chamber's view, the interception of communications by foreign intelligence services could not engage the responsibility of a receiving State, or fall within that State's jurisdiction within the meaning of Article 1 of the Convention, even if the interception was carried out at that State's request (see paragraph 420 of the Chamber judgment). First of all, in so far as some of the third parties had invoked the ILC Draft Articles, the Chamber considered that these would only be relevant if the foreign intelligence services were placed at the disposal of the receiving State and were acting in the exercise of elements of the governmental authority of that State (Article 6); if the receiving State aided or assisted the foreign intelligence services in intercepting the communications where that

amounted to an internationally wrongful act for the State responsible for the services, the receiving State was aware of the circumstances of the internationally wrongful act, and the act would have been internationally wrongful if committed by the receiving State (Article 16); or if the receiving State exercised direction or control over the foreign government (Article 17). Secondly, according to the Court's case-law the interception of communications by a foreign intelligence service could only fall within the receiving State's jurisdiction if that State was exercising authority or control over the foreign intelligence service (see, for example, *Al-Skeini and Others v. the United Kingdom* [GC], no. 55721/07, §§ 130-39, ECHR 2011, and *Jaloud v. the Netherlands* [GC], no. 47708/08, §§ 139 and 151, ECHR 2014).

496. The Grand Chamber agrees with the Chamber that none of these elements were present in the situation under consideration and, indeed, in their pleadings before the Grand Chamber the applicants did not suggest that they were. Therefore, any interference with Article 8 of the Convention could only lie in the initial request and the subsequent receipt of intercept material, followed by its storage, examination and use by the intelligence services of the receiving State.

497. The protection afforded by the Convention would be rendered nugatory if States could circumvent their Convention obligations by requesting either the interception of communications by, or the conveyance of intercepted communications from, non-Contracting States; or even, although not directly in issue in the cases at hand, by obtaining such communications through direct access to those States' databases. Therefore, in the Court's view, where a request is made to a non-contracting State for intercept material the request must have a basis in domestic law, and that law must be accessible to the person concerned and foreseeable as to its effects (see *Roman Zakharov*, cited above, § 228). It will also be necessary to have clear detailed rules which give citizens an adequate indication of the circumstances in which and the conditions on which the authorities are empowered to make such a request (see the above-cited cases of *Roman Zakharov*, § 229; *Malone*, § 67; *Leander*, § 51; *Huvig*, § 29; *Kruslin*, § 30; *Valenzuela Contreras*, § 46; *Rotaru*, § 55; *Weber and Saravia*, § 93; and *Association for European Integration and Human Rights and Ekimdzhiev*, § 75) and which provide effective guarantees against the use of this power to circumvent domestic law and/or the States' obligations under the Convention.

498. Upon receipt of the intercept material, the Court considers that the receiving State must have in place adequate safeguards for its examination, use and storage; for its onward transmission; and for its erasure and destruction. These safeguards, first developed by the Court in its case-law on the interception of communications by Contracting States, are equally applicable to the receipt, by a Contracting State, of solicited intercept

material from a foreign intelligence service. If, as the Government contend, States do not always know whether material received from foreign intelligence services is the product of interception, then the Court considers that the same standards should apply to all material received from foreign intelligence services that could be the product of intercept.

499. Finally, the Court considers that any regime permitting the intelligence services to request either interception or intercept material from non-Contracting States, or to directly access such material, should be subject to independent supervision, and there should also be the possibility for independent *ex post facto* review.

*(ii) Application of that test to the case at hand*

500. The British-US Communication Intelligence Agreement of 5 March 1946 specifically permitted the exchange of material between the United States and the United Kingdom (see paragraph 103 above). However, details of the intelligence services' internal (or "below the waterline") arrangements were only disclosed during the *Liberty* proceedings (see paragraphs 33-36 above). This new information was later incorporated into Chapter 12 of the IC Code (see paragraph 116 above) which, as already noted, was a public document, subject to the approval of both Houses of Parliament, and which had to be taken into account both by those exercising interception duties and by courts and tribunals (see paragraphs 93-94 above). The Court has accepted that the provisions of the IC Code could be taken into consideration in assessing the foreseeability of the RIPA regime (see *Kennedy*, cited above, § 157, and paragraph 366 above) and the same must necessarily be true for the intelligence sharing regime.

501. Accordingly, the Court considers that the regime for requesting and receiving intelligence from non-Contracting States had a clear basis in domestic law and, following the amendment to the IC Code, that law was adequately accessible. As it undoubtedly pursued the legitimate aims of protecting national security, preventing disorder and crime, and protecting the rights and freedoms of others, the Court will now – in line with its usual methodology (see paragraph 334 above) – assess, jointly, the foreseeability and necessity of the intelligence sharing regime.

502. Chapter 12 of the IC Code (see paragraph 116 above) follows the same approach as the one adopted by domestic legislation in respect of bulk interception. Under Chapter 12 the intelligence services could only make a request to a foreign government for unanalysed intercepted communications and/or associated communications data if a relevant interception warrant under RIPA had already been issued by the Secretary of State, the assistance of the foreign government was necessary to obtain the particular communications because they could not be obtained under the existing warrant (see paragraph 12.2 of the IC Code at paragraph 116 above), and it was necessary and proportionate for the intercepting agency to obtain those

communications. For these purposes, a relevant RIPA interception warrant meant either a section 8(1) warrant in relation to the subject at issue; a section 8(4) warrant and an accompanying certificate which included one or more "descriptions of intercepted material" covering the subject's communications; or, where the subject was known to be within the British Islands, a section 8(4) warrant and an accompanying certificate which included one or more "descriptions of intercepted material" covering his or her communications, together with an appropriate section 16(3) modification.

503. Where exceptional circumstances existed, a request for communications could be made in the absence of a relevant RIPA interception warrant only if it did not amount to a deliberate circumvention of RIPA or otherwise frustrate its objectives (for example, because it was not technically feasible to obtain the communications via RIPA interception), and it was necessary and proportionate for the intercepting agency to obtain those communications. In such a case the request had to be considered and decided on by the Secretary of State personally, and, pursuant to the revised IC Code, notified to the IC Commissioner. According to information disclosed during the *Liberty* proceedings, and confirmed in the Government's submissions before both the Chamber and Grand Chamber, no request for intercept material had ever been made in the absence of an existing RIPA warrant (see paragraph 42 above).

504. In the light of the foregoing, the Court considers that domestic law set down clear legal rules giving citizens an adequate indication of the circumstances in which and the conditions on which the authorities could request intercept material from a foreign State.

505. Where either a relevant section 8(1) or a section 8(4) warrant was already in place, that warrant would have been authorised by the Secretary of State. More specifically, it would appear from paragraph 12.5 of the IC Code, read together with the accompanying footnote, that where a request was based on an existing warrant that request would be made to, from or about specific selectors (that is, relating to a specific individual or individuals) and the Secretary of State would already have approved the request for the communications of those individuals. While, in exceptional circumstances, a request could be made in the absence of a relevant warrant, the Secretary of State personally had to approve the request and, if based on specific selectors, he or she personally had to consider and approve the examination of those communications by reference to such factors (see paragraph 116 above).

506. Since, in respect of such requests for intelligence sharing, the domestic legislation followed the same approach as in the case of bulk interception, and since national law explicitly provided that there should be no circumvention, there is no need for the Court to look separately at the authorisation procedure.

507. As for the safeguards for the examination, use, storage, onward transmission, erasure and destruction of the solicited intercept material, it was clear from paragraph 12.6 of the IC Code that intercepted content or related communications data obtained by the United Kingdom intelligence services from another State – such material "identifying itself" as the product of an interception – had to be subject to the same internal rules and safeguards that applied to the same categories of content or data when they were obtained directly by the intercepting agencies as a result of interception under RIPA. Consequently, the safeguards in sections 15 and 16 RIPA, as supplemented by the IC Code, applied equally to intercepted communications and communications data obtained from foreign intelligence services, provided that the material "identified itself as the product of an interception".

508. The Court has examined the section 15 and section 16 safeguards in respect of the bulk interception regime and it is satisfied that the procedures for storing, accessing, examining and using the material obtained, for communicating the material to other parties, and for the erasure and destruction of the material obtained were sufficiently clear and afforded adequate protection against abuse (see paragraphs 384-405 above). In the light of the Court's findings at paragraph 498 above, it notes that paragraph 12.6 of the IC did not extend the safeguards in sections 15 and 16 RIPA, as supplemented by the IC Code, to all material received from foreign intelligence services that could be the product of interception, limiting these safeguards only to material that "identified itself" as such; however, the Court does not consider this fact alone to be fatal to the Article 8 compliance of the intelligence sharing regime.

509. In the context of the section 8(4) regime, the Court had concerns about the exemption of related communications data from the section 16 safeguard. However, under the section 8(4) regime the State was able to intercept, store and search all packets of communications travelling across certain bearers. The blanket exemption of related communications data from the section 16 safeguard therefore meant that all of these data, regardless of whether they were of any intelligence interest, could be searched by the intelligence services apparently without restriction. Under Chapter 12 of the IC Code, on the other hand, content and related communications data were not requested by the intelligence services in bulk. Paragraph 12.5 of the IC Code, together with its accompanying footnote, indicated that where a request was based on an existing warrant that request would be made to, from or about specific selectors (that is, specified individuals) and the Secretary of State would already have approved the request for the communications of those individuals. While in exceptional circumstances a request could be made in the absence of a warrant, the Secretary of State personally had to approve the request and, if based on specific selectors, he or she personally had to consider and approve the examination of those

communications by reference to such factors. If the request was not for specific selectors, any communications subsequently obtained could not be examined according to a factor referable to a person known to be in the British Islands unless the Secretary of State had approved the examination of those communications (see paragraph 116 above). In other words, the intelligence services either requested intelligence relating to an individual for whom the Secretary of State had already considered the necessity and proportionality of obtaining his or her communications; or the section 16 safeguard was applicable to the material obtained. As no request has yet been made without a warrant, it would seem that, to date, all requests have fallen into the first category.

510. Therefore, the Court considers that the United Kingdom had in place adequate safeguards for the examination, use and storage of the content and communications data received from intelligence partners; for the onward transmission of this material; and for its erasure and destruction.

511. Lastly, the Court observes that a further layer of protection was provided by the IC Commissioner and the IPT (see paragraph 41 above). The IC Commissioner had oversight of the intelligence sharing regime: paragraph 12.7 of the IC Code (see paragraph 116 above) required him or her to be notified of all requests made in the absence of a warrant, and he or she already supervised the granting of warrants and the storage of material by the intelligence services.

512. In addition to the oversight of the IC Commissioner, the IPT provided *ex post facto* review of the intelligence sharing regime. As can be seen from the *Liberty* proceedings, it was open to anyone wishing to make either a specific or general complaint about the intelligence sharing regime to complain to the IPT; and, in response, the IPT was able to examine both the "above the waterline" and "below the waterline" arrangements in order to assess the Convention compliance of the regime.

513. Consequently, the Court considers that the regime for requesting and receiving intercept material was compatible with Article 8 of the Convention. There existed clear detailed rules which gave citizens an adequate indication of the circumstances in which and the conditions on which the authorities were empowered to make a request to a foreign intelligence service; domestic law contained effective guarantees against the use of such requests to circumvent domestic law and/or the United Kingdom's obligations under the Convention; the United Kingdom had in place adequate safeguards for the examination, use, storage, onward transmission, erasure and destruction of the material; and the regime was subject to independent oversight by the IC Commissioner and there was a possibility for *ex post facto* review by the IPT.

514. Accordingly, there has been no violation of Article 8 of the Convention.

### B. Article 10 of the Convention

515. The applicants in the third of the joined cases also complained that the intelligence sharing regime had breached their rights under Article 10 of the Convention. In so far as that complaint related to their activities as NGOs, the Chamber declared it inadmissible for non-exhaustion of domestic remedies as the applicants had raised it too late in the domestic proceedings for it to be considered (see paragraph 473 of the Chamber judgment). This aspect of the complaint is therefore outwith the scope of the Grand Chamber's examination.

516. The applicants in the third of the joined cases also complained more generally about the Article 10 compliance of the intelligence sharing regime. Although this argument was raised before the IPT in good time, the Court would agree with the Chamber that it gives rise to no separate issue over and above that arising out of Article 8 of the Convention (see paragraph 474 of the Chamber judgment). It therefore considers that there has also been no violation of Article 10 of the Convention.

## IV. ACQUISITION OF COMMUNICATIONS DATA FROM COMMUNICATIONS SERVICE PROVIDERS

### A. Article 8 of the Convention

517. The applicants in the second of the joined cases complained that the regime for the acquisition of communications data under Chapter II of RIPA was incompatible with their rights under Article 8 of the Convention.

#### *1. The Chamber judgment*

518. At the date of the Chamber's examination of the case, the Government of the United Kingdom was in the process of replacing the existing legal framework for conducting secret surveillance with the new IPA. The provisions in the new legislation governing the retention of communications data by CSPs were subject to a domestic legal challenge by Liberty. In the course of those proceedings, the Government conceded that the relevant provision was inconsistent with the requirements of EU law. Consequently, the High Court found Part 4 to be incompatible with fundamental rights in EU law since, in the area of criminal justice, access to retained data was not limited to the purpose of combating "serious crime"; nor was it subject to prior review by a court or an independent administrative body (see paragraph 190 above).

519. In view of both the primacy of EU law over United Kingdom law, and the Government's concession in the domestic proceedings that the provisions of the IPA governing the retention of communications data by CSPs was incompatible with EU law, the Chamber considered it "clear" that

domestic law required that any regime permitting the authorities to access data retained by CSPs should limit access to the purpose of combating "serious crime", and that access should be subject to prior review by a court or independent administrative body. As the predecessor regime suffered from the same "flaws" as its successor, the Chamber found that it could not be in accordance with the law within the meaning of Article 8 of the Convention (see paragraphs 465-68 of the Chamber judgment).

*2. The parties' submissions*

520. The parties made no further submissions before the Grand Chamber in respect of this complaint.

*3. The Court's assessment*

521. The Government did not contest the Chamber's findings before the Grand Chamber. Furthermore, the latter finds no ground on which to disagree with the Chamber's conclusions.

522. Accordingly, the Court considers that in the present case there has been a violation of Article 8 of the Convention on account of the fact that the operation of the regime under Chapter II of RIPA was not "in accordance with the law".

## B. Article 10 of the Convention

523. The applicants in the second of the joined cases also complained under Article 10 of the Convention about the regime for the acquisition of communications data from CSPs.

*1. The Chamber judgment*

524. The Chamber acknowledged that the Chapter II regime afforded enhanced protection where data were sought for the purpose of identifying a journalist's source. In particular, paragraph 3.77 of the Acquisition and Disclosure of Communications Data Code of Practice provided that where an application was intended to determine the source of journalistic information, there had to be an overriding requirement in the public interest, and such applications had to use the procedures of the Police and Criminal Evidence Act 1984 (PACE) to apply to a court for a production order to obtain these data. Pursuant to Schedule 1 of that Act, an application for a production order was made to a judge and, where the application related to material that consisted of or included journalistic material, the application had to be made *inter partes*. Internal authorisation could only be used if there was believed to be an immediate threat of loss of human life, and that person's life could be endangered by the delay inherent in the process of judicial authorisation (see paragraph 498 of the Chamber judgment).

525. Nevertheless, these provisions only applied where the purpose of the application was to determine a source; they did not apply in every case where there was a request for the communications data of a journalist, or where such collateral intrusion was likely. Furthermore, in cases concerning access to a journalist's communications data there were no special provisions restricting access to the purpose of combating "serious crime". Consequently, the Chamber considered that the regime was not "in accordance with the law" for the purpose of the Article 10 complaint (see paragraphs 496-99 of the Chamber judgment).

*2. The parties' submissions*

526. The parties made no further submissions before the Grand Chamber in respect of this complaint.

*3. The Court's assessment*

527. The Government did not contest the Chamber's findings before the Grand Chamber. Furthermore, the latter finds no ground on which to disagree with the Chamber's conclusions.

528. Accordingly, the Court considers that in the present case there has also been a violation of Article 10 of the Convention on account of the fact that the operation of the regime under Chapter II of RIPA was not "in accordance with the law".

## V. APPLICATION OF ARTICLE 41 OF THE CONVENTION

529. Article 41 of the Convention provides:

> "If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

### A. Damage

530. The applicants did not submit any claim in respect of pecuniary or non-pecuniary damage. Accordingly, the Court considers that there is no call to award them any sum on that account.

### B. Costs and expenses

531. Before the Chamber the applicants in the first of the joined cases claimed 208,958.55 pounds sterling (GBP) in respect of their costs and expenses; and the applicants in the second of the joined cases claimed GBP 45,127.89. The applicants in the third of the joined cases made no claim in respect of costs and expenses.

532. The Chamber awarded the applicants in the first of the joined cases the sum of 150,000 euros (EUR) for the proceedings before it; and the applicants in the second of the joined cases the sum of EUR 35,000 for the proceedings before it.

533. Before the Grand Chamber the applicants in the first of the joined cases claimed a further GBP 138,036.66; the applicants in the second of the joined cases claimed a further GBP 69,200.20; and the applicants in the third of the joined cases claimed GBP 44,993.60.

534. The Government contested the quantum claimed.

535. According to the Court's case-law, an applicant is entitled to reimbursement of costs and expenses only in so far as it has been shown that these have been actually and necessarily incurred and are reasonable as to quantum. In the present case, regard being had to the documents in its possession and the above criteria, the Court considers it reasonable to award the following sums covering costs under all heads for the proceedings before the Chamber: to the applicants in the first of the joined cases the sum of EUR 150,000; and the applicants in the second of the joined cases the sum of EUR 35,000. It also considers it reasonable to award the following sums covering costs under all heads for the proceedings before the Grand Chamber: to the applicants in the first of the joined cases, the sum of EUR 77,500; to the applicants in the second of the joined cases, the sum of EUR 55,000; and to the applicants in the third of the joined cases, the sum of EUR 36,000.

### C. Default interest

536. The Court considers it appropriate that the default interest rate should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

## FOR THESE REASONS, THE COURT

1. *Holds*, unanimously, that there has been a violation of Article 8 of the Convention in respect of the section 8(4) regime;

2. *Holds*, unanimously, that there has been a violation of Article 8 of the Convention in respect of the Chapter II regime;

3. *Holds*, by twelve votes to five, that there has been no violation of Article 8 of the Convention in respect of the receipt of intelligence from foreign intelligence services;

4. *Holds*, unanimously, that, in so far as it was raised by the applicants in the second of the joined cases, there has been a violation of Article 10 of the Convention in respect of the section 8(4) regime and the Chapter II regime;

5. *Holds*, by twelve votes to five, that there has been no violation of Article 10 of the Convention in respect of the receipt of intelligence from foreign intelligence services;

6. *Holds*, unanimously,

(a) that the respondent State is to pay the applicants, within three months, the following amounts, to be converted into the currency of the respondent State at the rate applicable at the date of settlement:
   (i) to the applicants in the first of the joined cases: EUR 227,500 (two hundred and twenty-seven thousand five hundred euros), plus any tax that may be chargeable to the applicants, in respect of costs and expenses;
   (ii) to the applicants in the second of the joined cases: EUR 90,000 (ninety thousand euros), plus any tax that may be chargeable to the applicants, in respect of costs and expenses;
   (iii) to the applicants in the third of the joined cases: EUR 36,000 (thirty-six thousand euros), plus any tax that may be chargeable to the applicants, in respect of costs and expenses;

(b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amounts at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

7. *Dismisses*, unanimously, the remainder of the applicants' claim for just satisfaction.

Done in English and in French, and delivered at a hearing on 25 May 2021, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

| | |
|---|---|
| Søren Prebensen | Robert Spano |
| Deputy to the Registrar | President |

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the following separate opinions are annexed to this judgment:

(a) joint partly concurring opinion of Judges Lemmens, Vehabović and Bošnjak;
(b) partly concurring, partly dissenting opinion of Judge Pinto de Albuquerque;
(c) joint partly dissenting opinion of Judges Lemmens, Vehabović, Ranzoni and Bošnjak.

R.S.
S.C.P.

# JOINT PARTLY CONCURRING OPINION OF JUDGES LEMMENS, VEHABOVIĆ AND BOŠNJAK

1. In the present case, we agree with the majority on all counts in the operative part of the judgment, except for operative points 3 (no violation of Article 8 of the Convention in respect of the receipt of intelligence from foreign intelligence services) and 5 (no violation of Article 10 of the Convention in respect of the receipt of intelligence from foreign intelligence services). To show where we disagree with the outcome of the case, we are submitting a dissenting opinion jointly with our colleague Judge Ranzoni. In addition, we are submitting this concurring opinion to underline that while the present judgment as a whole is elegantly structured and largely clear in its message, it has also missed an excellent opportunity to fully uphold the importance of private life and correspondence when faced with interference in the form of mass surveillance.

## I. INTRODUCTORY REMARKS

2. This case is about a balancing exercise in which legitimate interests pursued by the Contracting States have to be weighed against human rights and fundamental freedoms, notably those protected by Article 8 of the Convention. At the start of its assessment (paragraphs 322 and 323 of the judgment), the Grand Chamber extensively describes the nature of the modern threats facing the Contracting States and recognises how valuable bulk interception can be in identifying and preventing those threats. Furthermore, the judgment underlines a need for secrecy of operations in this domain which it considers to be legitimate, meaning that little if any information about a given scheme will be available to the public. While one may subscribe, to a certain extent, to this description of the legitimate interest in operating a bulk interception regime, there is no similar emphasis on the importance of privacy or any other private interest in those same preliminary remarks. Although this has no direct bearing upon the assessment of the bulk interception system under scrutiny, we would have preferred a more balanced introduction to this assessment.

3. Before embarking on an analysis of what we consider to be the weak points of the present judgment, it is worthwhile remembering that privacy is a fundamental precondition for a variety of fundamental individual interests, but also for the existence of a democratic society. It is essential for a person's well-being, autonomy, self-development, and ability to enter into meaningful relationships with other persons. It is also a necessary precondition for the enjoyment of civil rights and consequently for a person's status as a free and equal member of a democratic society. Encroachments on privacy do not merely diminish individual autonomy and mental and physical health, they also inhibit democratic self-governance.

4. First, privacy is important for a person's mental and physical health. The mere feeling that one is constantly being observed and evaluated by others can have serious effects on one's mental and physical well-being. It makes individuals internalise too much of their social behaviour, so that they feel guilty or ashamed because of any feelings or thoughts, desires or practices that they would not want to express publicly. Such tensions between the demands of their inner life and the pressures of self-presentation can lead to serious health problems.

5. Second, external observation and the pressures on self-presentation may obstruct "the promotion of liberty, autonomy, selfhood, human relations, and furthering the existence of a free society"[1]. Surveillance is inhibiting because it diminishes the extent to which we can spontaneously and wholeheartedly relate to other people and engage in certain activities. A lack of privacy would have a stifling effect on our inner life, our relationships and ultimately our autonomy. "Thus will be lost ... the inner personal core that is the source of criticism of convention, of creativity, rebellion and renewal"[2].

6. Third, privacy is essential for democratic self-governance. Mass surveillance exerts internal and external pressures to conform, making individuals submissive and deferential. In order to avoid outright oppression and give itself the varnish of legitimacy, there is an inherent danger that the State will utilise surveillance to ensure compliance and conformism. As George Orwell described in the novel *Nineteen Eighty-Four*:

> "There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized."[3]

7. In securing a realm for unobserved activity, privacy fosters and encourages the moral autonomy of citizens, a central requirement of self-governance in democracies[4]. Only autonomous beings can truly govern themselves and only autonomous beings can truly enjoy all the civil rights, such as the right to vote, freedom of association and participation in civil society, the freedoms of thought and conscience, speech and expression, and freedom of religion, that are essential for self-governance. We cannot be

---

[1] Ruth Gavison (1980), "Privacy and the Limits of Law", *Yale Law Journal* 89, p. 347.

[2] Jeffrey Reiman (1995), "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Information Technology of the Future", *Santa Clara High Technology Law Journal* 11:1, p. 42.

[3] George Orwell (2008), *Nineteen Eighty-Four* (London: Penguin), pp. 4-5.

[4] Daniel Solove (2008), *Understanding Privacy* (Cambridge, MA: Harvard University Press), p. 98.

said to fully enjoy the freedoms that these rights are supposed to afford us if our inner freedom is compromised.

8. But surveillance does not merely exert internal pressures on freedom. To the extent that citizens retain their autonomy, it also exerts external pressures on their freedom to exercise their civil rights. Just as living under constant social control makes us less likely to act according to our feelings and thoughts for fear of ostracism, living under constant government surveillance can make citizens just a little more cautious when engaging with their political convictions, a little less likely to freely associate, a little less likely to speak freely, a little less likely to dissent, a little less likely to run for public office. The aggregate effect of often merely marginal inhibitions can stifle what was once a free society, especially as people grow up in an environment of increased conformism and moral cowardice. US Supreme Court Justice William O. Douglas, writing the dissent in *Osborn v. United States*, impressionably describes as follows the threat that mass surveillance poses to our democratic freedoms:

> "... The time may come when no one can be sure whether his words are being recorded for use at some future time; when everyone will fear that his most secret thoughts are no longer his own, but belong to the Government; when the most confidential and intimate conversations are always open to eager, prying ears. When that time comes, privacy, and with it liberty, will be gone. If a man's privacy can be invaded at will, who can say he is free? If his every word is taken down and evaluated, or if he is afraid every word may be, who can say he enjoys freedom of speech? If his every association is known and recorded, if the conversations with his associates are purloined, who can say he enjoys freedom of association? When such conditions obtain, our citizens will be afraid to utter any but the safest and most orthodox thoughts; afraid to associate with any but the most acceptable people. Freedom as the Constitution envisages it will have vanished."[5]

9. To conclude, the development of new technologies enabling mass surveillance and more effective use of the information collected has increased threats to privacy as well as the risk of abuse of personal data. It is not our intention to assert that these threats and risks have already materialised on a large scale or have brought about the consequences discussed above. However, one should be properly aware of their existence when designing a system capable of preventing, detecting and sanctioning any abuse that might occur.

10. In our opinion, these considerations should have led the Court to attach significantly more weight to private life in general, and to confidentiality of correspondence in particular, when weighing them in the balance against the legitimate interests of the respondent State in operating its bulk interception scheme. Consequently, the Grand Chamber should have (a) accurately identified and attached proper weight to interferences with private life and correspondence; (b) introduced clear minimum

[5] *Osborn v. United States*, 385 U.S. 323 (1966).

safeguards capable of protecting individuals against arbitrary or excessive interference; and consequently (c) assessed the impugned bulk interception scheme in a stricter manner.

## II. INTERFERENCES WITH PRIVATE LIFE AND CORRESPONDENCE

11. In paragraph 325 of the judgment, the majority describe the stages of the bulk interception system. They consider that the initial stage, described as the interception and initial retention of communications and related communications data, followed by the immediate discarding of parts of the communications, "does not constitute a particularly significant interference" (paragraph 330). We respectfully disagree. It is our belief that at this stage already, the interference is significant. First, by interception and initial retention, all communications of any individual flowing through selected bearers and all related communications data come into the hands of State authorities. Secondly, while it is true that at this stage, the content of those communications has not yet been analysed or brought to the attention of decision makers and thus cannot yet lead to any action being taken against a particular individual, the first stage is a *sine qua non* for any further stage. The exact extent of the communications and related data thereby gathered by the intelligence services is unknown. But there are reasons to believe that, on a regular basis, a large part of the communications of millions of individuals is intercepted. This situation is aggravated by the fact that the individuals concerned will, as a rule, not be aware of this interference. In such a situation, when people cannot know whether their communications are being targeted, but are aware that there exists a strong probability that this is happening, a third element of interference arises: people may adapt their behaviour, with many a serious consequence, as described above in paragraphs 3-8 of this separate opinion.

12. According to paragraph 330 of the judgment, parts of intercepted communications are discarded immediately. The Court is not in possession of any information as to how this "discarding" is performed. One may reasonably assume that it is not conducted randomly without any internal logic and that in this exercise, intelligence services apply certain criteria which separate rubbish from possibly useful material. The very fact that this act is performed in obscurity and on an unknown basis should, in our opinion, be a matter of serious concern. Such a lack of transparency, at the very least, can hardly meet the requirement of foreseeability, this in turn being one of the preconditions for the lawfulness of any interference with the rights protected by Article 8 of the Convention. Yet the majority fail to address this particular step in the bulk interception process in any way. We consider this to be an important shortcoming of the judgment.

## III. MINIMUM SAFEGUARDS PROTECTING INDIVIDUALS AGAINST ARBITRARY OR EXCESSIVE INTERFERENCE

13. In paragraph 335, the judgment outlines the Court's case-law on six minimum requirements that should be set out in domestic law in order to avoid abuses of power in cases of interception of communications for the purposes of criminal investigation. It further explains that, in *Roman Zakharov v. Russia* ([GC], no. 47143/06, ECHR 2015), the Court held that the same six minimum safeguards also applied in cases where the interception was performed for reasons of national security. In the next step, the Grand Chamber identifies a need to develop and adapt these requirements to the specificities of bulk interception and, finally, outlines a list of eight criteria which the domestic legal framework must clearly define in order to comply with Article 8 of the Convention (paragraph 361 of the judgment).

14. That list is very well supported by arguments and can certainly serve as protection against arbitrariness and abuse. However, the criteria included in this list:

(a) do not clearly serve as self-standing minimum standards, as any lack of compliance with any of those standards appears to be "reparable" in the process of a global assessment;

(b) require clear definition of particular safeguards in domestic law, but do not set any minimum safeguards themselves; and

(c) do not provide for any clear substantive protection of an individual against disproportionate interference, in particular at the stage of application of strong selectors to the material gathered, and the procedural protection provided by these criteria is also insufficient.

15. As to (a), we would like to turn the reader's attention to paragraph 360 of the judgment, announcing a need for a global assessment of a particular bulk interception regime. While this may sound appealing, it necessarily erodes the importance of each safeguard. By contrast, we believe that each safeguard labelled as a minimum one can never be offset by any counterbalancing factors provided in respect of some other criterion. In other words, lack of compliance with a safeguard which is considered to be a minimum one should automatically lead to a finding of a violation of Article 8 of the Convention, regardless of whether a global assessment might reveal a more positive picture. Regrettably, the majority do not appear to have opted for such an approach. We would add that an approach setting minimum standards as absolute limits, as thick red lines that may not be crossed, would provide for a stricter and more foreseeable protection, which is of utmost importance in a field where the action of the State authorities is conducted with a high level of secrecy, as a result of which, in the words of the present judgment (see paragraph 322), little if any information about the operation of the scheme is available and such

information as is available may be couched in terminology which is obscure.

16. In respect of (b), the majority state that the eight criteria outlined in paragraph 361 need to be clearly defined in the domestic legal framework. While this is a requirement to be welcomed, in particular from the point of view of foreseeability of the law, these criteria in themselves do not lay down minimum requirements in respect of the substantive or procedural conditions that need to be complied with in order to operate the bulk interception regime and to pass from its initial stage to the more intrusive ones. This flaw is partly remedied by the fact that certain (but not all) of those elements discussed in paragraphs 348-60 of the judgment are set out not only in descriptive passages referring to the existing case-law but also in prescriptive wording laying down certain requirements, particularly in respect of the authorisation of bulk interception in its specific stages. However, we argue that the requirements set by the majority do not go far enough in protecting an individual against arbitrary, excessive or abusive interferences with his or her private life and correspondence.

17. This brings us to our point (c). In the context of targeted interception, mostly for purposes of detecting and investigating criminal activity, the Court has referred to certain substantive safeguards against abuse. Thus, the Court has required that the nature of the offences which may give rise to an interception order be defined together with the categories of people liable to have their communications intercepted. Furthermore, on numerous occasions, the Court has had recourse to the requirement of reasonable suspicion. The majority simply consider that these safeguards are not readily applicable to bulk interception. While we can agree that they cannot be directly transposable, there remains a need for robust substantive protection to be developed, whereby safeguards developed in the framework of targeted interception for the purpose of combatting crime can serve as an excellent source of inspiration, as we will seek to explain below.

18. First, in contrast to targeted interception in crime prevention, bulk interception is largely used for purposes of national security. It is difficult to see why one should not expect the domestic legislation to clearly define the possible national security threats and the circumstances in which those threats may trigger bulk interception.

19. In respect of the second substantive requirement attached to targeted interception, namely the definition of categories of people liable to have their communications intercepted, one can acknowledge that a similar requirement would make little sense in the first stage of bulk interception, when all communications running through certain bearers are intercepted indiscriminately. Yet the breadth of the interference should not be an excuse for abandoning a particular safeguard. Additionally, at later stages of bulk interception, particularly when strong selectors are applied for the purpose

of singling out and analysing the communications of an identified individual, the situation becomes largely comparable to that of targeted interception. Expecting the legal framework to define the categories of people that can be targeted by the application of strong selectors would not be an excessive, but rather a fully appropriate, requirement.

20. Third, the requirement of reasonable suspicion is an important protection against arbitrary and disproportionate interferences with several Convention rights. It refers to the probability that a criminal offence giving rise to an interference has been committed or is about to be committed. While bulk interception should not be used in crime investigation, but rather confined to national security purposes, we believe that a standard similar to reasonable suspicion should pertain to the grounds on which bulk interception may be authorised. This is particularly true when bulk interception starts targeting an identified individual through the application of strong selectors. To be clear, we consider that in a democratic society intelligence services may only inspect communications and related communication data of an individual once they can demonstrate to an objective observer that that individual may be engaged or is about to engage in activities infringing a specific national security interest, or is a person who is or may be in contact with individuals engaged in, or about to engage, in such activities. No such or similar requirement has been introduced by the majority in the present judgment.

21. Instead of these three safeguards, the majority have set an overly broad substantive requirement, namely that the grounds on which bulk interception may be authorised and the circumstances in which an individual's communications may be intercepted must be clearly defined in the domestic legal framework. Unfortunately, the reference to "grounds" and "circumstances" is rather vague, particularly in the absence of any reference to what such grounds and circumstances may or may not be. Furthermore, according to the language used in paragraph 361 of the judgment, the specific requirement relating to the grounds only applies to the stage of authorisation of bulk interception and not to any subsequent stage, thereby giving no indication as to whether any substantive requirement is attached, for example, to the application of strong selectors targeting the communications of an identified individual.

22. The lack of appropriate substantive protection has an important bearing upon the effectiveness of procedural protection. The main element of procedural protection is the requirement of prior authorisation, which the present judgment introduces both at the first stage of bulk interception and before the application of strong selectors. The crucial point of any prior authorisation is to verify whether the envisaged interference complies with the substantive criteria for such an interference. However, if the substantive criteria are vague, overly broad or even non-existent, the requirement of

prior authorisation will necessarily fail to provide for sufficiently effective protection against arbitrariness and abuse.

23. In respect of the prior authorisation requirement, the judgment requires such authorisation to be exercised at the initial stage by a body that is independent from the executive. We can agree. However, we respectfully but strongly disagree that it suffices for the application of strong selectors relating to identifiable individuals to be subjected to a prior *internal* authorisation alone. Instead, we argue that at this stage, prior judicial control would be needed. While the existing case-law of the Court does not necessarily require judicial authorisation for targeted interception of communications of individuals, we believe that there are reasons for a reinforced standard of protection in cases of application of strong selectors in bulk interception. These reasons are as follows:

(a) Bulk interception, in contrast to targeted interception, is not limited to a specific category of people, and thus a much larger pool of communications is liable to be examined than in a case of targeted communications.

(b) Furthermore, a strong selector pertaining to an identified individual can, when applied, open the door to a much larger number of communications, namely wherever that specific individual is referred to, even if he or she has not engaged in those communications (as opposed to communicating over the communication means that he or she personally uses).

(c) In targeted interception for the purposes of law enforcement, a form of judicial control will usually occur somewhere down the line. For example, when evidence is obtained by targeted interception, it will be submitted in subsequent criminal proceedings, such that a court conducting those proceedings will be able to verify whether the targeted interception in that case complied with legal requirements. No such subsequent judicial control will normally occur in cases of bulk interception coupled with the application of strong selectors.

24. In stark contrast with this view, the majority consider that prior internal authorisation is sufficient. In our opinion, internal authorisation cannot provide for a level of protection against arbitrariness and abuse comparable to the protection offered by independent scrutiny. In particular, it is hard to imagine how a person having an organisational and, possibly, collegial connection with the requesting authority could properly assess a request in a fair and disinterested manner. It is probable that authorisation requirements will not be fully respected and, thus, the very purpose of this safeguard will not be met. This is even more likely in those High Contracting Parties where no long-standing tradition of democratic oversight of intelligence services exists.

25. We note that the Governments of the United Kingdom and the Netherlands have submitted that any requirement to explain or substantiate

selectors or search criteria would seriously restrict the effectiveness of bulk interception (paragraph 353 of the judgment) and that the majority show some sympathy for this argument (paragraph 354). We cannot subscribe to this argument. We believe that in a democratic society, communications and related communications data of an identified individual may not be singled out and examined without that individual's consent unless very convincing reasons exist to do so. If an intelligence service or other authority is not able to articulate such reasons and demonstrate them before an independent institution, this should simply mean that it ought not to have any access to such communications. We acknowledge that occasionally a situation may arise where the regular authorisation process is too cumbersome to effectively neutralise a threat to national security, and that other solutions should be provided in this respect. However, if a robust authorisation system designed to properly protect human rights is perceived as an unnecessary hurdle, democratic society should be put on notice.

## IV. ASSESSMENT OF THE BULK INTERCEPTION REGIME AT HAND

26. We agree with the other members of the Grand Chamber in their findings in points 1, 2 and 4 of the operative part of the judgment. That said, we believe that the assessment of certain features of the impugned regime does not go far enough and fails to properly identify some of its shortcomings.

27. As an example, we wish to direct the reader's attention to the grounds on which bulk interception could be authorised under the United Kingdom system (see paragraphs 368-71 of the judgment). A bulk interception warrant could be issued if this was necessary (a) in the interests of national security; (b) for the purpose of preventing or detecting serious crime; or (c) for the purpose of safeguarding the economic well-being of the United Kingdom in so far as those interests were also relevant to the interests of national security.

28. The purposes under (a) and (c) both made reference to interests of national security. It appears that neither national security nor its interests were anywhere defined. While we take note of the judgment's reference to the IC Commissioner's clarification of how practice perceived the term "national security" (paragraph 369 of the judgment), we argue that this clarification remained insufficient from the point of view of the foreseeability requirement. Furthermore, we have doubts as to whether the IC Commissioner's clarification can be assimilated to well established case-law which, according to the Court's jurisprudence, may compensate for vagueness in legislation. As a consequence of the absence of a clear definition, an individual could not be sure, even with the help of qualified

advice, on what exact grounds his or her communications were liable to be intercepted and analysed by the intelligence services.

29. The purpose under (b) did not have the above-mentioned flaws of the purposes under (a) and (c). Serious crime was defined as an offence for which the perpetrator (assuming he or she was over the age of twenty-one and had no previous convictions) could reasonably be expected to be sentenced to imprisonment for a term of three years or more, or where the conduct involved the use of violence, resulted in substantial financial gain or was conducted by a large number of persons in pursuit of a common purpose (see paragraph 369 of the judgment). Such a definition covers a very broad scope of behaviour, which raises serious doubts regarding the proportionality of this ground. Furthermore, in a democratic society, intelligence services should not have any competence in combating crime, unless the criminal activities threaten national security[6]. The explanation of the respondent Government, namely that information obtained by bulk interception could not be used in the prosecution of a criminal offence, is in our opinion unconvincing. It appears that on the basis of the information thus obtained, law enforcement agencies could act, for example, by proceeding to conduct investigative measures or even arrests, this in turn producing evidence for the purpose of prosecution. It is likely that in a not so distant future, by exploring this particular ground, crime investigation might move from targeted surveillance to bulk interception of data.

## V. CONCLUSION

30. There are rare occasions when the Court adjudicates on a case which shapes the future of our societies. The present one is such an example. The Grand Chamber has partly seized the opportunity and outlined a comprehensive set of principles which are aimed at protecting human rights and fundamental freedoms, notably those enshrined in Articles 8 and 10 of the Convention. However, for the reasons explained in this separate opinion, in performing the balancing exercise, the majority have failed to assign proper weight to private life and correspondence, which in several respects remain insufficiently protected in the face of interference by bulk interception. One may hope that in future cases raising questions of concrete interference with the rights of specific individuals, the Court will interpret and further develop the principles in a way which will properly uphold democratic society and the values it stands for.

---

[6] See, for example, Recommendation 1402 (1999) of the Parliamentary Assembly of the Council of Europe on the control of internal security services in Council of Europe member states, in particular Guideline A (ii). This Recommendation addresses activities of internal security services, but we see it as perfectly applicable to foreign intelligence also.

# PARTLY CONCURRING, PARTLY DISSENTING OPINION OF JUDGE PINTO DE ALBUQUERQUE

**I. Introduction (§ 1)**
**II. Deconstruction of the Court's *pro autoritate* regime of bulk interception (§§ 2-18)**
A. Vague language (§§ 2-3)
B. Biased methodology (§§ 4-12)
C. Defective regime of safeguards (§§ 13-15)
D. Preliminary conclusion (§§ 16-18)
**III. Construction of a *pro persona* regime of bulk interception (§§ 19-34)**
A. Bulk interception of communications (§§ 19-29)
B. Exchange of intercept data with foreign intelligence services (§§ 30-31)
C. Bulk interception of related communications data (§ 32)
D. Preliminary conclusion (§§ 33-34)
**IV. Critique of the impugned UK bulk interception regime (§§ 35-58)**
A. Bulk interception of communications (§§ 35-49)
B. Exchange of intercept data with foreign intelligence services (§§ 50-54)
C. Bulk interception of related communications data (§§ 55-57)
D. Preliminary conclusion (§ 58)
**V. Conclusion (§§ 59-60)**

## I. INTRODUCTION

1. I voted with the majority, except on the finding of no violation of Articles 8 and 10 in respect of the receipt of intercepted material from foreign intelligence services, namely of the bulk material intercepted by the United States National Security Agency (NSA) under the PRISM and Upstream programmes. In addition, I do not agree with the core of the majority's reasoning regarding the findings of violations of Articles 8 and 10. The purpose of this opinion is to present the reasons for my disagreement[1].

[1] This is the second time that I have written a separate opinion on bulk interception. In *Szábo and Vissy v. Hungary* (no. 37138/14, 12 January 2016), I had the opportunity to state my views on the slippery slope in which the Hungarian bulk interception regime had engaged and the undesirable consequences lurking at the bottom of the slope. In view of the discussion held in the Grand Chamber, and after careful weighing of all the conflicting arguments, I can now affirm that I have not moved an inch from my previous position. In

## II. DECONSTRUCTION OF THE COURT'S *PRO AUTORITATE* REGIME OF BULK INTERCEPTION

### A. Vague language

2. I regret to state from the outset that the Court's language is inadmissibly vague, as will be demonstrated in this opinion. While sometimes this language reflects the Court's deliberate intention to accord leeway for a discretionary execution of this judgment by the respondent State, at other times it shows the judges' hesitation in the performance of their adjudicatory function. In so doing, they not only weaken the Court's authority, but water down the standard-setting value of this judgment.

3. Since the legal concepts of European human rights law are autonomous, in the sense that they are not strictly dependent on the meaning and scope of the corresponding domestic legal concepts, and in view of the novel character of the legal issues at stake in the present Grand Chamber case, the Court should have established, in black and white, the meaning of the fundamental legal concepts that it uses in the present judgment[2], regardless of their meaning in the Regulation of Investigatory Powers Act 2000 ("RIPA"), the Interception of Communications Code of Practice ("the IC Code") or any "below the waterline" arrangements. For the sake of conceptual clarity, I will use the terms listed below with the following meanings:

**(a) "intercept subject"** to include natural persons and legal entities, including public services, private corporations, NGOs, and any civil society organisations, whose electronic communications may be intercepted, or have been intercepted[3];

**(b) "intercepted material" or "bulk material"** to encompass the content of the electronic communications and related communications data that have been collected by means of bulk interception[4];

**(c) "related communications data"** to include the data necessary for locating the source of an electronic communication and its destination, for determining the date, time, duration and type of communication, for identifying the communications equipment used, and for locating the terminal equipment and communications, data which comprise, *inter alia*,

---

fact, I am now even more convinced that what I wrote in 2016 is unfortunately still very much up to date. Therefore the present opinion should be read in conjunction with what I wrote five years ago.

[2] This good practice can be found, for instance, in *Rohlena v. the Czech Republic* ([GC], no. 59552/08, 27 January 2015).

[3] The domestic concept is similar. See section 20 RIPA.

[4] The domestic concept is different. See section 20 RIPA.

the name and address of the user, the telephone numbers of the caller and the person called, and the IP address for Internet services[5];

**(d) "bulk interception"** as targeted and non-targeted interception of electronic communications (and related communications data) circulating on bearers by means of strong selectors and selectors;

**(e) "bearers"** as carriers (primarily sub-marine fibre optic cables) of electronic communications;

**(f) "strong selectors"** as specific (personal) identifiers relating to an identified or identifiable target, permitting the acquisition of electronic communications to, from, or about the target;

**(g) "selectors"** as non-specific (non-personal) identifiers;

**(h) a "to" or "from" communication** as an electronic communication for which the sender or a recipient is a user of the tasked selector;

**(i) an "about" communication** as one in which the tasked selector is referenced within the acquired electronic communication, but the target is not necessarily a participant in the communication;

**(j) "external communication"** as communication sent or received outside the national territory[6];

**(k) "communication"** as "anything comprising speech, music, sounds, visual images or data of any description and signals serving either for the imparting of anything between persons, between a person and a thing or between things, or for the actuation or control of any apparatus"[7];

**(l) "'below the waterline' arrangements"** as secret, internal rules and practices of the intercepting authority.

## B. Biased methodology

4. The Court's methodological approach to this case is regrettable, for two main reasons. First, the Court was willing to decide a case of this importance "on the basis of limited information about the manner in which [the Contracting States' bulk interception] regimes operate"[8]. For example, the Government did not indicate the number or the degree of precision of the selectors they had used, the number of bearers intercepted or how exactly those bearers were selected, or the kind of intelligence reports that were being generated in respect of the related communications data, and yet the Court did not insist on obtaining that crucial information. The Investigatory Powers Tribunal ("the IPT") examined "below the waterline" arrangements[9], the Interception of Communications Commissioner ("the IC

[5] The domestic concept is more limited. See section 20 RIPA. Section 21 (4), (6) and (7) provides for the concept of "communications data".
[6] This concept is similar to that of section 20 RIPA.
[7] This concept is enshrined in section 81 RIPA, which can also be used by the Court.
[8] Paragraph 323 of this judgment.
[9] Paragraphs 33 and 50 of this judgment.

Commissioner") had access to "closed materials"[10] and even the Independent Reviewer of Terrorism legislation examined a "great deal of closed material"[11], but the Court did not, and could not. The Court was patently lacking in the detailed material necessary to make a full structural analysis and assessment of bulk interception in the United Kingdom. It is disappointing that the utmost sensitivity of the subject matter of this judgment, which was repeatedly stressed by the Court, only served the purpose of insisting on the need for the "effectiveness"[12] and "flexibility"[13] of the bulk interception system, but not that of collecting all the relevant evidence needed for a factually sound Court judgment. This self-imposed restriction on the Court's power to collect evidence demonstrates that the Strasbourg judges fail to consider the Court as a true judicial body, with the power to order the parties to provide it with unlimited and unconditional access to the evidence relevant to the subject matter of the case. As a consequence, the Court made some "educated guesses" about the likely degree of the interference with an individual's rights at different stages of the interception process. The problem of developing regulatory standards on the basis of such "educated guesses" is that it reflects the regulator's assumptions and biases. And they are clear in the present case. The Government's case boils down to a simple proposition which is "trust us". The majority were ready to accept this proposition, with the risk of erring on the side of over-collecting intelligence. I am not. As the United States Presidential Review Board put it, "Americans must not make the mistake of trusting officials"[14]. I would say the same for Europeans.

5. Second, the above-mentioned self-imposed evidential and adjudicatory limitation leads the Court to assume the inevitability of bulk interception and, even more so, that of a blanket, non-targeted, suspicionless interception regime, as pleaded by the respondent States and the third parties in both the present case and *Centrum för rättvisa v. Sweden*[15]. With circular reasoning, the United Kingdom Government affirmed that bulk interception was incompatible with a reasonable suspicion requirement, because it was, by definition, untargeted, and it was untargeted because it

[10] Paragraph 136 of this judgment.
[11] Paragraph 424 of this judgment.
[12] Paragraph 353 of this judgment.
[13] Paragraph 354 of this judgment.
[14] "Liberty and Security in a Changing World", Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies, 12 December 2013, p. 114.
[15] *Centrum för rättvisa v. Sweden* (no. 35252/08), delivered on the same day as the present judgment. It is noticeable that the Governments of France, the Netherlands and Norway focused precisely on this point: according to them, there was no justification for adding a reasonable suspicion requirement to bulk interception (paragraphs 301, 305 and 309 of this judgment).

did not require reasonable suspicion[16]. The Court followed this lead and put it in axiomatic terms:

> "[T]he requirement of 'reasonable suspicion', which can be found in the Court's case-law on targeted interception in the context of criminal investigations is less germane in the bulk interception context, the purpose of which is in principle preventive, rather than for the investigation of a specific target and/or an identifiable criminal offence[17]."

It follows from this new paradigm that the Court has departed from settled case-law according to which it "does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other"[18]. Both the German and the British bulk interception systems had already been assessed by the Court under the exact same criteria applicable to targeted interception: I refer to the generalised strategic surveillance under the G10 Act in *Weber and Saravia v. Germany*[19], as well as the indiscriminate collection of telecommunications sent or received outside the British Islands under the Interception of Communications Act 1985 in *Liberty and Others v. the United Kingdom*[20] and the capturing of vast amounts of internal communications under the Regulation of Investigatory Powers Act 2000 in *Kennedy v. the United Kingdom*[21]. The Court has departed from the fundamentals of this case-law without good reason, as I will demonstrate below.

6. Moreover, the Court did not give proper weight to the fact that it had restated and effectively applied the previous case-law in three recent cases whose subject matter included, in one case tangentially and in the other two specifically, non-targeted interception of communications. I am referring to *Roman Zakharov v. Russia*[22], *Szábo and Vissy v. Hungary*[23], and *Mustafa Sezgin Tanrıkulu v. Turkey*[24]. It is telling that *Roman Zakharov v. Russia*[25]

---

[16] See the oral submission of the respondent Government in the Grand Chamber on 10 July 2019: "They [reasonable suspicion and subsequent notification] are fundamentally incompatible with the operation of a regime which does not depend on the existence of clearly defined surveillance targets. The section 8(4) regime, is, by its nature, an untargeted regime. It exists to discover unknown national security and serious crimes threats. So reasonable suspicion simply could not be a part of it. Such requirement would cripple its utility ..." At the end of the day, the argument boils down to the "utility" of suspicionless massive bulk interception.

[17] Paragraph 348 of this judgment.

[18] *Liberty and Others v. the United Kingdom*, no. 58243/00, § 63, 1 July 2008.

[19] *Weber and Saravia v. Germany* (dec.), no. 54934/00, §§ 95 and 114, ECHR 2006-XI.

[20] *Liberty and Others*, cited above, §§ 63-65.

[21] *Kennedy v. the United Kingdom*, no. 26839/05, §§ 158-60, 18 May 2010.

[22] *Roman Zakharov v. Russia* [GC], no. 47143/06, §§ 231 and 264, ECHR 2015.

[23] *Szábo and Vissy*, cited above.

[24] *Mustafa Sezgin Tanrıkulu v. Turkey*, no. 27473/06, 18 July 2017.

[25] *Roman Zakharov*, cited above, §§ 231 and 264.

also used the *Weber and Saravia* criteria when dealing with operational search activities, including interference with postal, telegraphic and other communications, which could affect "any person using these mobile telephone services"[26], for the purposes of national, military, economic or ecological security[27]. The Grand Chamber in that case went so far as to reproach the practice of "interception authorisations which do not mention a specific person or telephone number to be tapped but authorise interception of all telephone communications in the area where a criminal offence has been committed"[28]. In *Szábo and Vissy v. Hungary*[29] the Court was even more explicit in censuring the "unlimited surveillance of a large number of citizens"[30], for the purposes of anti-terrorism and rescuing Hungarian citizens in distress abroad[31]. While admitting the need for bulk interception to counter internal and external threats, the Court required an "individual suspicion"[32] for every surveillance measure in the light of the *Weber and Saravia* criteria[33]. In the subsequent case of *Mustafa Sezgin Tanrıkulu v. Turkey*[34], the Court reproached the domestic court's decision to allow the interception of the telephone and electronic communications of anyone in Turkey for the purpose of preventing criminal acts by terrorist organisations, after having recalled and confirmed the *Weber and Saravia*, *Roman Zakharov* and *Szábo and Vissy* case-law.

7. In addition to the claim that "both cases [*Liberty and Others* and *Weber and Saravia*] are now more than ten years old", and that the surveillance activity considered in those cases was "much narrower"[35], the Court gave three reasons to abandon the previous case-law[36], all factually unsound.

8. The first argument is that the "stated purpose" of bulk interception is "in many cases" to monitor the communications of persons outside the State's territorial jurisdiction "which could not be monitored by other forms of surveillance"[37]. The Court did not provide, and could not provide, any evidence that "in many cases" bulk interception was limited, in terms of the "stated purpose", still less of the real practice, to persons outside the State's

---

[26] Ibid., §§ 175-78.
[27] Ibid., §§ 31, 246-48.
[28] Ibid., § 265. The cases of "area surveillance" authorisation clearly involved potential bulk surveillance.
[29] *Szábo and Vissy*, cited above.
[30] Ibid., § 67.
[31] Ibid., § 63.
[32] Ibid., § 71.
[33] Ibid., § 56.
[34] *Mustafa Sezgin Tanrıkulu*, cited above, §§ 56 and 57.
[35] Paragraph 341 of this judgment. This claim overlooks the *Roman Zakharov* and *Szábo and Vissy* cases, already mentioned.
[36] Paragraphs 344-46 of this judgment.
[37] Paragraph 344 of this judgment.

territorial jurisdiction. On the contrary, all the available authoritative documents on bulk interception, which the Court chose to ignore, tell a different story. It is incomprehensible that, in view of the lack of evidence provided by the respondent Government, the Court turned a blind eye to the Council of Europe and European Union factual assessments publicly available in a plethora of authoritative documents on bulk interception published after the Snowden scandal erupted, such as for example the Parliamentary Assembly of the Council of Europe (PACE) Resolutions 1954 (2013) and 2045 (2015), and Recommendation 2067 (2015), the Committee of Ministers Declaration of 11 June 2013, and its Reply to the PACE Recommendation 2067 (2015), the European Commission against Racism's General Policy Recommendation no. 11, the Commissioner for Human Rights' Comments of 24 October 2013, his issue papers of 8 December 2014 and May 2015, and his Report on the shortcomings in the oversight of German intelligence and security services of 1 October 2015, the European Parliament Resolutions of 12 March 2014 and 29 October 2015, the European Data Protection Supervisor's opinion of 20 February 2014, and the Article 29 Working Party opinion 4/2014. It also neglected the United Nations General Assembly Resolution 68/167 of 18 December 2013, the United Nations Human Rights Committee (HRC) concluding observations on the fourth report of the USA of 26 March 2014 and the United Nations Special Rapporteur and the Inter-American Commission on Human Rights Special Rapporteur for freedom of expression joint declaration of 21 June 2013[38]. Most astonishingly, the majority did not even consider the available international authoritative documents on the British bulk interception regime, such as the HRC Concluding observations on the seventh period report of the United Kingdom of 17 August 2015[39], and the Council of Europe Human Rights Commissioner's Memorandum on Surveillance and Oversight Mechanisms in the United Kingdom of May 2016[40].

9. All these documents, as well as the recent *Szábo and Vissy*[41] and *Mustafa Sezgin Tanrıkulu v. Turkey*[42] judgments of this Court and the relevant case-law of the Court of Justice of the European Union ("the CJEU")[43], contradict the alleged prevalence of monitoring of persons

[38] For a detailed analysis of these documents, see my opinion in *Szábo and Vissy*, cited above.
[39] UN doc. CCPR/C/GBR/CO/7.
[40] CommDH (2016)20.
[41] *Szábo and Vissy*, cited above, § 66: "[I]t is possible for virtually any person in Hungary to be subjected to secret surveillance."
[42] *Mustafa Sezgin Tanrıkulu*, cited above, § 7.
[43] Paragraphs 209-41 of the present judgment. I refer here to the following CJEU cases: judgment of 8 April 2014 in *Digital Rights Ireland and Others*, C-293/12 and C-594/12, EU:C:2014:238 (on the Data Retention Directive (2006/24/EC) which "entailed an interference with the fundamental rights of practically the entire European population");

outside the State's territorial jurisdiction. On the contrary, these authorities confirm that bulk surveillance is mainly aimed at people within the territorial jurisdiction of the State[44]. The Government themselves admitted that the number of queries made against related communications data under section 8(4) RIPA in respect of people who are known to be in the United Kingdom – thus as an internal surveillance tool – is up to several thousand per week[45].

10. The second argument departing from the previous case-law is that the Council of Europe member States "appear to use"[46] bulk interception for purposes other than crime investigation. The Court's line of argument seems to be the following: since targeted interception is "for the most part"[47] employed in bulk interception for the purposes of crime detection and investigation, but bulk interception may also be used for the purposes of foreign intelligence gathering, where there may be neither a specific target nor an identifiable offence, bulk interception is not (and should not be) governed by the same standards of targeted surveillance[48]. This is yet another argument that is not proven by the Court, which chose to decide based on appearances, rather than facts.

11. In reality, non-targeted bulk interception is prohibited explicitly or implicitly in twenty-three European States[49]. As PACE[50] and the Council of

---

judgment of 6 October 2015 in *Schrems*, C-362/14, EU:C:2015:650 (reproaching legislation permitting the public authorities to have access "on a generalised basis to the content of electronic communications"); judgment of 6 October 2020 in *Privacy International*, C-623/17, EU:C:2020:790 (on national legislation requiring electronic communication services to disclose traffic and location data to intelligence agencies by means of a general and indiscriminate transmission affecting "all persons using electronic communications services"); and judgment of 6 October 2020 in *La Quadrature du Net and Others*, C-511/18, C-512/18 and C-520/18, EU:C:2020:791 (censuring legislation requiring service providers to retain "generally and indiscriminately" traffic and location data). The first two cases concerned the processing of personal data for law-enforcement purposes, the last two cases the assessment of secret surveillance conducted by intelligence services.

[44] See below the full discussion on the inability of the territorial jurisdiction-based distinction between internal and external communications to justify bulk interception of the latter.

[45] See the respondent Government's Observations before the Grand Chamber of 2 May 2019, p. 42 ("many thousands in any given week in relation to individuals known or believed to be in the UK alone").

[46] Paragraph 345 of this judgment.

[47] Ibid.

[48] It should be noted that the Governments of France and the Netherlands insisted, like the Chamber, that it was wrong to assume that bulk interception constituted a greater intrusion into private life than targeted interception (paragraphs 300 and 306 of this judgment).

[49] As the Court's research report itself concluded regarding Albania, Andorra, Austria, Belgium, Bosnia and Herzegovina, Croatia, the Czech Republic, Greece, Ireland, Iceland, Italy, Liechtenstein, Moldova, Monaco, Montenegro, North Macedonia, Poland, Portugal, Romania, San Marino, Serbia, Turkey and Ukraine. Thus paragraphs 242-46 of the judgment do not portray a correct picture of the European landscape.

[50] PACE Resolution 2031 (2015).

Europe Human Rights Commissioner[51] have forcefully demonstrated, indiscriminate mass communications surveillance has proven to be ineffective for the prevention of terrorism and therefore is not only dangerous for the protection of human rights but also a waste of resources. Thus if there is a consensus in Europe on non-targeted bulk interception, the consensus is that it should be prohibited, but this has been ignored by the Court. Only seven Council of Europe member States operate such regimes[52], and they do it mainly for the prevention, detection and investigation of such crimes as terrorism, espionage, cyber-attacks and, more vaguely, "serious crimes"[53], as shown by the above-mentioned authoritative Council of Europe and European Union documents, the *Szábo and Vissy* and *Mustafa Sezgin Tanrıkulu* judgments of this Court (cited above) and the relevant case-law of the CJEU. Foreign intelligence gathering is only one among other purposes, and the Court does not have the minimum element of statistical or other evidence of how this purpose is pursued, whether based on monitoring of specific targets or otherwise. Even assuming, for the sake of the discussion, that foreign intelligence gathering is mainly pursued by means of non-targeted bulk interception, this does not necessarily imply that all bulk interception, including bulk interception with purposes related to crime detection and investigation, should be non-targeted. Otherwise, what happens is that bulk interception becomes a loophole to avoid the protections of an individual warrant in circumstances where such a warrant would be perfectly suited to acquiring the communications at issue. Having said that, nothing precludes the possibility that foreign intelligence gathering itself may be pursued by means of bulk interception based on a requirement of reasonable suspicion of the involvement of the targeted person or group of persons involved in activities harmful to national security, even if they are not criminal offences[54].

12. The third argument deals precisely with this fine line between old-fashioned targeted interception and the new forms of bulk interception used to target specified individuals, and it is the weakest argument of the Court. In the case of interception by means of strong selectors, the Court argues that the "targeted individuals' devices are not monitored"[55], and therefore bulk interception does not require the same guarantees as classical targeted

---

[51] Council of Europe Human Rights Commissioner's Memorandum on Surveillance and Oversight Mechanisms in the United Kingdom, CommDH (2016)20, May 2016, p. 10.
[52] Paragraph 242 of this judgment.
[53] Paragraph 345 of this judgment. I refer here to the critique addressed to this concept of "serious crime" by the CJEU (see paragraph 212 of this judgment).
[54] See the Venice Commission report on the democratic oversight of signals intelligence agencies, 2015, p. 9, 25 and 26 ("there must be concrete facts indicating the criminal offence/security-threatening conduct, and the investigators must have 'probable cause', 'reasonable suspicion' or satisfy some similar test"), and the Council of Europe Human Rights Commissioner's Memorandum, cited above, p. 6.
[55] Paragraph 346 of this judgment.

interception. This is not convincing. The automatic collection and processing by means of strong selectors permitting the acquisition of electronic communications to, from or about the target across the bearers chosen by the intelligence services is a potentially much more intrusive form of interference with Article 8 rights than the mere monitoring of the targeted individuals' devices[56]. It is thus misleading to say that "only" (paragraph 346 of the judgment) those packets of the targeted individuals' communications will be intercepted, leaving the impression that bulk interception based on strong selectors is less intrusive than the old-fashioned monitoring of an individual's devices.

## C. Defective regime of safeguards

13. From this factually unfounded reasoning, the Court drew two legal conclusions for "[t]he approach to be followed in bulk interception cases"[57]: domestic law does not have to identify the nature of the offences which may give rise to an interception order and the categories of people whose communications may be intercepted, and no requirement of a reasonable suspicion is needed to ground such interception order[58]. According to the Court's logic, since "the purpose of [bulk interception] is in principle preventive, rather than for the investigation of a specific target and/or an identifiable criminal offence"[59], none of the above two safeguards are required in domestic law, even when bulk interception targets a specified individual involved in an identifiable criminal offence. Thus, a general, suspicionless interception order suffices to trigger bulk interception, be it for the purposes of crime detection and investigation or others.

14. The Court's position leaves many questions unanswered. What are the admissible grounds for bulk interception? For example, is the investigation of "serious criminal offences", without any further precision, an admissible ground? How serious should the crime investigated be? Is the investigation of the theft of a wallet and a mobile phone an admissible ground?[60] Is the promotion of economic and industrial espionage for the sake of the economic well-being and national security of the intercepting State an admissible ground?[61] What are the admissible "circumstances" in

---

[56] As the CJEU explained in paragraph 55 of its *Digital Rights Ireland and Others* judgment (cited above): "the need for ... safeguards is all the greater where ... personal data are subjected to automatic processing".

[57] Section (c) (iii) of the Court's assessment.

[58] Paragraph 348 of this judgment.

[59] Ibid.

[60] The example derives from the CJEU case-law (see paragraph 220 of the present judgment).

[61] The example derives from the sharp critique addressed by the European Parliament Resolution of 12 March 2014 on the US NSA surveillance programme, the Venice

which an individual's communications may be intercepted? To justify bulk interception of an individual's communications, what is the required degree of interest of the individual's communications for the purposes pursued by the bulk interception order? Is it the individual suspicion standard mentioned by *Szábo and Vissy*[62] or the reasonable suspicion criterion required by *Roman Zakharov*[63]? How can the Court require that domestic law set out "with sufficient clarity"[64] the grounds upon which bulk interception may be authorised and the circumstances in which an individual's communications may be intercepted when the Court itself is not sufficiently clear on what kind of "grounds" and "circumstances" it is referring to?

15. Since Article 8 applies to all stages of bulk interception, including the initial retention of communications and related communications data[65], the Court has correctly established "end-to-end safeguards"[66]. The problem is that the Court is unclear regarding the legal nature of the "end-to-end safeguards". On the one hand, it has used imperative language ("should be made"[67], "should be subject"[68], "should be authorised"[69], "should be informed"[70], "must be justified"[71], and "should be scrupulously recorded"[72], "should also be subject"[73], "it is imperative that the remedy should"[74]) and has called them "fundamental safeguards"[75] and even "minimum safeguards"[76]. But on the other hand, it has diluted these safeguards in "a global assessment of the operation of the regime"[77], allowing for a trade-off among the safeguards[78]. It seems that at the end of the day each individual safeguard is not mandatory, and the prescriptive language of the Court does not really correspond to non-negotiable features of the domestic system. In some corners of Europe, zealous secret services will be strongly tempted to

---

Commission report, cited above, p. 18, and the Council of Europe Human Rights Commissioner's Memorandum, cited above, p. 8.

[62] *Szábo and Vissy*, cited above, § 71.

[63] *Roman Zakharov*, cited above, §§ 260, 262 and 263.

[64] Paragraph 348 of this judgment.

[65] Paragraph 330 of this judgment.

[66] Paragraph 350 of this judgment.

[67] Ibid.

[68] Ibid.

[69] Paragraph 351 of this judgment.

[70] Paragraph 352 of this judgment.

[71] Paragraph 355 of this judgment.

[72] Ibid.

[73] Paragraph 356 of this judgment.

[74] Paragraph 359 of this judgment.

[75] Paragraph 350 of this judgment.

[76] Paragraph 348 of this judgment.

[77] Paragraph 360 of this judgment.

[78] See, for example, paragraph 370 *in fine* of this judgment.

take advantage of the Court's very lax fashion of formulating legal standards and innocent people will pay the price sooner or later.

### D. Preliminary conclusion

16. According to the Court, an independent authority[79], i.e. one that is independent from the executive, is required at the outset to assess the purpose of the interception, the selection of the bearers[80] and the categories of selectors[81], against the backdrop of the principles of necessity and proportionality. The choice of strong selectors linked to identifiable individuals is particularly problematic, since the selection and "use of every such strong selector"[82] does not require a prior independent authorisation. For the Court, internal authorisation suffices in this case, coupled with the guarantees that the request for a strong selector is justified and the internal process is "scrupulously" recorded[83].

17. Furthermore, the execution of the interception order, including its subsequent renewals, the use, storage, onward transmission and deletion of the obtained data, should be supervised by an authority independent from the executive, with detailed records being kept at each stage of the process to facilitate this supervision[84].

18. In the end, the *ex post facto* review of the entire process should be performed by an authority independent from the executive, in a fair and adversarial procedure, with binding powers to order the cessation of unlawful interception and the destruction of unlawfully obtained or stored data, as well as obsolete, equivocal or disproportionate data[85].

## III. CONSTRUCTION OF A *PRO PERSONA* REGIME OF BULK INTERCEPTION

### A. Bulk interception of communications

19. It appears to me that the above-mentioned regime does not amount to a sufficient set of guarantees of the Articles 8 and 10 rights. In my view, the time has come not to dispense with the fundamental guarantees of

---

[79] Although the Court's language is not uniform, sometimes referring to the concept of independent authority and other times to that of independent body, it seems that there is no substantial difference between these concepts.
[80] Paragraph 352 of this judgment.
[81] Paragraph 354 of this judgment.
[82] Paragraph 355 of this judgment.
[83] Ibid. As the Venice Commission report (cited above, p. 28) put it, "internal controls are insufficient". Thus paragraph 199 of the judgment misrepresents the position of the Venice Commission.
[84] Paragraph 356 of this judgment.
[85] Paragraph 359 of this judgment.

judicial authorisation, supervision and *ex post facto* review in the field of bulk interception[86]. As a matter of principle, the end-to-end judicial oversight of bulk interception is warranted by the extremely intrusive nature of this process. I do not see why a State governed by the rule of law should not trust its serving judges, ultimately its more senior and experienced judges, to decide on such matters. Unless the Court believes that judicial-like bodies are more independent than ordinary courts ... In my view, the independence of judicial-like bodies is not a given. In addition, if ordinary courts are competent to authorise, supervise and review the interception of communications in highly complex criminal proceedings, such as investigations into organised crime and terrorism, I do not understand why they should not be competent to perform the exact same function regarding the operation of a bulk interception process. Thus, neither the independence nor the competence of ordinary courts should be called into question for the purposes of building a Convention-compliant architecture of safeguards in a bulk interception regime. A State which believes its serving judiciary to be unfit to perform these functions has a serious problem with the rule of law.

20. To be sure, judicial intervention should not be a panacea[87]. It is obvious that judicial oversight of the entire process would be meaningless if the categories of offences and activities and intercept subjects being monitored were not set out in the domestic law with the necessary degree of clarity and precision. Consequently, judicial control must encompass the choice of the specific bearers and strong selectors. By specific I mean the individual bearers and strong selectors, not "sorts" or "categories" of bearers or selectors, which would be a blank cheque for the intercepting authority to pick up whatever it likes.

21. In the case of a double-lock system, whereby the judge considers warrants previously decided by a politician or an administrative official, judicial oversight must not be limited to the possibility of overruling the administrative decision when the judge deems that the politician or the administrative official acted unreasonably. This would not be truly judicial authorisation since the Convention-required necessity and proportionality tests are more demanding than the mere reasonableness test.

---

[86] Venice Commission Report, cited above, p. 32 ("For European states, *ex ante* judicial approval in individual cases is to be preferred"). Thus paragraph 197 of the judgment distorts the message of the Venice Commission. The Council of Europe Human Rights Commissioner also suggested adopting *ex ante* judicial authorisation (Memorandum, cited above, § 28).

[87] The fact that judicial authorisation might not in itself be a sufficient safeguard against abuse does not support the conclusion that it is not a necessary one. It should be noted that *ex ante* judicial authorisation was introduced by IPA, but this is not the place to discuss *ex professo* the judicial review standard introduced by IPA, because the 2016 Act is not before the Court.

22. As I mentioned in *Szábo and Vissy*, the Convention does not allow for "data fishing", or "exploratory" expeditions, neither in the form of non-targeted surveillance based on non-specific selectors, nor in the form of surveillance based on strong selectors aimed at communications about the targeted intercept subject[88]. Nor is it admissible to broaden the net of intercept subjects through the deployment of fuzzier search terms. I would recall the fundamental reason why I have reached this conclusion. Admitting non-targeted bulk interception involves a fundamental change in how we view crime prevention and investigation and intelligence gathering in Europe, from targeting a suspect who can be identified to treating everyone as a potential suspect, whose data must be stored, analysed and profiled[89]. Of course the impact of such a change on the innocent could eventually be mitigated by a cohort of more or less flexible adjudicators and regulators and a plethora of more or less convenient laws and codes of practice, but a society built upon such foundations is more akin to a police state than to a democratic society. This would be the opposite of what the founding fathers wanted for Europe when they signed the Convention in 1950.

23. Thus any target of surveillance must always be identified or identifiable in advance based on reasonable suspicion. To leave no doubt, bulk interception should be admissible only on the basis of strong selectors aimed at the communications from and to the targeted intercept subject when there is a reasonable suspicion that he or she is involved in the legally defined categories of serious offences or activities which are harmful to national security without necessarily being criminal[90].

24. Judicial warranting should extend to the authorisation of surveillance of communications or related communications data, including privileged and confidential data, with the sole exception of urgent cases, when the competent judge is not immediately available, where authorisation may be

---

[88] See all the international authorities cited in my opinion appended to *Szábo and Vissy* (cited above).

[89] That is why I believe that the massive collection of data of innocent people accepted by the Court in the present judgment falls foul of the principles established in *S. and Marper v. the United Kingdom* (nos. 30562/04 and 30566/04, § 135, ECHR 2008); *Shimovolos v. Russia* (no. 30194/09, §§ 68 and 69, 21 June 2011); *M.K. v. France* (no. 19522/09, § 37, 18 April 2013); and most importantly, *Mustafa Sezgin Tanrıkulu* (cited above, §§ 57-59).

[90] This is the universal standard as compiled in the United Nations Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight, 17 May 2010 (A/HRC/14/46): "Practice 21. National law outlines the types of collection measures available to intelligence services; the permissible objectives of intelligence collection; the categories of persons and activities which may be subject to intelligence collection; the threshold of suspicion required to justify the use of collection measures; the limitations on the duration for which collection measures may be used; and the procedures for authorising, overseeing and reviewing the use of intelligence-collection measures."

given by a public prosecutor, subject to the competent judge's subsequent endorsement.

25. Domestic law should provide for a specific regime of protection for privileged professional communications of parliamentarians, medical doctors, lawyers and journalists[91]. Since indiscriminate and suspicionless bulk collection of communications would frustrate the protection of legally protected and confidential information, this can only be effectively guaranteed by means of judicial authorisation of interception of such communications when evidence is put forward that supports a reasonable suspicion of serious offences or conduct damaging to national security committed by these professionals[92]. In addition, any communications of these categories of professionals covered by their professional secrecy, if mistakenly intercepted, should be immediately destroyed. Domestic law should also provide for the absolute prohibition of any interception of communications covered by religious secrecy.

26. Judicial oversight should not stop at the start of the operation of the interception. Were the actual operation of the system of interception hidden from the judge's oversight, the initial intervention of a judge could be easily undermined and deprived of any real effect, rendering it a merely virtual, deceptive safeguard. On the contrary, the judge should accompany the entire process, with a regular and vigilant examination of the necessity and proportionality of the interception order, in view of the intercept data obtained. Unless he or she receives constant feedback from the intercepting authority, the authorising judge will not know how the authorisation is in fact being used. In case of non-compliance with the interception order, the judge should be able to order its immediate cessation and the destruction of the unlawfully obtained data. The same should apply in case of the lack of necessity to proceed with the operation, for example because the data obtained are of no interest for the purposes pursued by the interception order. Only a judge vested with the power to take such binding decisions can provide an effective guarantee of the lawfulness of the material that is kept. In sum, the judge should be empowered to conduct a regular review of the operation of the system, including of all records of interception and accompanying classified documents[93], with a view to avoiding unnecessary and disproportionate interference with the rights under Articles 8 and 10.

---

[91] Other than *Sanoma Uitgevers B.V. v. the Netherlands* ([GC], no. 38224/03, §§ 90-92, 14 September 2010), see European Union Fundamental Rights Agency (FRA), *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU*, volume II: *Field perspectives and legal updates*, 2017, p. 12: "EU Member States should establish specific legal procedures to safeguard the professional privilege of groups such as members of parliament, members of the judiciary, lawyers and media professionals. Implementation of these procedures should be overseen by an independent body."

[92] Venice Commission report, cited above, p. 26.

[93] This is the universal and European standard as compiled respectively by the United Nations Compilation, cited above ("Practice 25. An independent institution exists to

27. Finally, *ex post* review of the use made of an interception order should also be triggered by notification to the targeted person. When nothing hinders the notification of the person whose communications have been intercepted, it would allow him or her to contest in a fair and adversarial judicial procedure the grounds for such interception[94]. It is therefore highly speculative, to say the least, to pretend that a system which does not depend on notification of the intercept subject "may even offer better guarantees of a proper procedure than a system based on notification"[95]. No one cares more for the interests of the intercept subject than the subject himself or herself.

28. Where, for some reason, such as the interests of national security, it is not possible to notify the person whose communications have been intercepted, there is realistically no way of the person learning of the surveillance measure taken in his or her regard. In this case, it is imperative to impose on the competent judge the burden of assessing, on his or her own initiative (*ex proprio motu*) or on the initiative of a third party (for example, a public prosecutor), the way in which the interception order was executed with a view to determining whether the data in question was lawfully collected and should be kept or destroyed; the intercept subject should then be represented by a privacy lawyer.

29. Last but not least, human and financial oversight resources and capabilities should match the scale of the operations being overseen, otherwise the entire system will be a mere façade covering the discretionary administrative process of the intercepting authorities.

## B. Exchange of intercept data with foreign intelligence services

30. The Court has set a lower standard of protection for the transfer to foreign intelligence services of data obtained through bulk interception. First, the transferring State does not have an obligation to check whether the receiving State has a comparable degree of protection to its own. Furthermore, there is no need to require, prior to every transfer, an

---

oversee the use of personal data by intelligence services. This institution has access to all files held by the intelligence services and has the power to order the disclosure of information to individuals concerned, as well as the destruction of files or personal information contained therein") and FRA, *Surveillance by intelligence services*, cited above, p. 11 ("Member States should also grant oversight bodies the power to initiate their own investigations as well as permanent, complete and direct access to necessary information and documents for fulfilling their mandate").

[94] *Szábo and Vissy* (cited above, § 86). In the logic of *Szábo and Vissy*, this is a further minimum requirement over and above the *Weber and Saravia* criteria. On the advantages of the notification process "in curbing overuse", see the Venice Commission report (cited above, p. 35), and the reports of the Council of Europe Human Rights Commissioner on Germany 2015 (p. 17), and on the United Kingdom (2016, cited above, p. 5).

[95] Paragraph 358 of this judgment.

assurance that the receiving State, in handing the data, will put in place safeguards capable of preventing abuse and disproportionate interference[96]. Thus the Court has not excluded the possibility of bulk transfer of data to a foreign intelligence service in a continuous process based on a single purpose. In view of this highly discretionary framework, it is not clear what the "independent control" required by the Court consists of[97]. What is the purpose of independent control if there is no need to assess the safeguards put in place by the receiving State (including to the effect that it will "guarantee the secure storage of the material and restrict its onward disclosure"[98]) prior to every transfer? Is the independent control limited to cases where "it is clear that material requiring special confidentiality – such as confidential journalistic material – is being transferred"[99]? To whom should this be clear, to the transferring intelligence service or to the judge? Is there any difference between independent control and independent authorisation? The vagueness of the Court's language seems to serve its intentional watering-down of the specific safeguards pertaining to the transfer itself.

31. I see no reason for this lowering of the Convention protection in case of the sharing of bulk data, and the Court does not provide one either. According to the consolidated Council of Europe and European Union standards, the sharing of personal data should be limited to third countries which afford a level of protection essentially equivalent to that guaranteed within the Council of Europe and the European Union respectively[100]. The judicial oversight should here be as thorough as in any other case. This attentive judicial oversight is particularly warranted when a Council of Europe member State is transferring data to a non-member State, for the obvious reason that the future use made of that data by the non-member State is not under the Court's jurisdiction. Such judicial oversight should not be limited by the "third-party rule", according to which it is prohibited

[96] Paragraph 362 of this judgment.
[97] Ibid.
[98] Ibid.
[99] Ibid.
[100] The majority ignore the fact that Article 2 of the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS 181), states that parties must ensure an adequate level of protection for personal data transfers to third countries, and that derogations are admitted only when there are legitimate prevailing interests. The Explanatory Report to that Convention adds that exceptions must be interpreted restrictively, "so that the exception does not become the rule" (§ 31). It is important to note that this Protocol has been ratified by 44 States, including 8 non-members of the Council of Europe. The United Kingdom has not ratified it. In addition to this Council of Europe standard, the European Union only allows for the transfer of personal data to a third country which affords a level of protection essentially equivalent to that guaranteed within the European Union (paragraph 234 of this judgment).

for an intelligence authority which received data from a foreign intelligence service to share it with a third party without the consent of the originator[101].

### C. Bulk interception of related communications data

32. Finally, the Court has acknowledged the highly intrusive potential of bulk interception of related communications data[102], but has failed to provide the same degree of protection in this case[103]. On the one hand it requires that "the aforementioned safeguards [be] in place", referring to those provided for in paragraph 361 of the judgment, but on the other hand it admits that member States have the discretion to pick and choose which specific safeguards should be enshrined in the domestic law, since "legal provisions governing ... treatment [of related communications data] may not necessarily have to be identical in every respect to those governing the treatment of content"[104]. The Court's blurred message is so ambiguous that it provides no proper guidance to the States as to which of the "aforementioned safeguards" are mandatory, if any, for bulk interception of related communications data. Consequently, the Court's hesitant stance does not allay the risk of mapping of a person's entire social life that the Court itself has identified.

### D. Preliminary conclusion

33. I do not agree that "States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary for these purposes [to protect national security and other essential national interests against serious external threats], [but] in the operation of such a system that margin will be narrower"[105]. If the boundaries of State discretion are wide, even the most stringent policing of them does little to safeguard against abuse. The margin of appreciation must be the same, both for designing the system and for operating it, and this margin is a narrow one, in view of the deeply intrusive nature of the State surveillance powers in question, the inherently

---

[101] Venice Commission report, cited above, 2015, p. 34 ("The originator or 'third-party rule' should not apply to the oversight body"), as well as FRA, *Surveillance by intelligence services*, cited above, 2017, pp. 13 and 106 ("Notwithstanding the third-party rule, EU Member States should consider granting oversight bodies full access to data transferred through international cooperation. This would extend oversight powers over all data available to and processed by intelligence services.").

[102] Paragraph 342 of this judgment.

[103] Ultimately, the Court was sensitive to the Government's threat, according to which "if member states operating bulk interception regime were required to apply the same protections to RCD [related communications data], as to content, then the likely result would simply be a watering down of the protection of content" (respondent Government's Observations before the Grand Chamber of 2 May 2019, p. 42).

[104] Paragraph 364 of this judgment in conjunction with paragraph 361.

[105] Paragraph 347 of this judgment.

high risk of abuse of these powers and – not to be forgotten – the European consensus on the prohibition of non-targeted bulk interception. This risk is magnified by some security-obsessed governments with an unlimited appetite for data which now have the technological means to control worldwide digital communication.

34. In sum, domestic law must be sufficiently clear in its terms to give individuals and legal persons[106] an adequate indication of the mandatory conditions and multi-layered procedures according to which the authorities are empowered to resort to bulk interception; these conditions and procedures include the following[107]:

(a) The definition of the grounds that may justify the adoption of an interception order, such as: detection of activities posing a threat to national security or serious crime prevention, detection, or investigation, in which case the offences that may trigger the interception must correspond either to a list of specific serious offences or generally to offences punishable by four or more years' imprisonment[108].

(b) A definition of the intercept subjects, in other words, the persons or institutions who are liable to have their communications intercepted, as follows:

– strict prohibition of data fishing or exploratory expeditions, to discover "unknown unknowns", including any form of non-targeted surveillance based on non-specific selectors;

– strict prohibition of use of strong selectors aimed at communications about the targeted intercept subject; and

– admissibility of strong selectors aimed at the communications from and to the targeted intercept subject when there is a reasonable suspicion that the intercept subject is involved in the above-mentioned offences or activities.

(c) A catalogue of the forms of electronic communications that can be intercepted, such as telephone, telex, fax, email, Google search, browsing the Internet, social media and cloud storage.

(d) The observance of the principle of necessity, which requires that:

– interference with the rights of the intercept subjects must adequately serve the purposes pursued and go no further than is necessary to achieve those aims;

---

[106] In *Liberty and Others* (cited above), all the claimants were NGOs arguing that their right to protection of their correspondence had been breached. These rights are also engaged in the present case.

[107] For this purpose, other than the above-mentioned authorities in paragraph 8, I have also taken into account the United Nations Compilation (cited above, 2010), the Venice Commission report (cited above, 2015), and the FRA report (cited above, 2017).

[108] Article 2 (b) of the UN Convention against Transnational Organized Crime defines "serious crime" as conduct punishable by a maximum deprivation of liberty of at least four years or a more serious penalty. The Explanatory Report on Recommendation Rec(2005)10 of the Committee of Ministers follows that reference.

– interception must be justified only as a measure of last resort, that is, when no other means of obtaining evidence or information are available, because recourse to other less intrusive methods has proven unsuccessful or, exceptionally, if other less intrusive methods are deemed unlikely to succeed;

– the interception must be tailored to avoid, as far as possible, targeting persons or institutions that are not responsible for the above-mentioned offences or activities; and

– the interception must be immediately stopped when it no longer serves the purposes pursued.

(e) The observance of the principle of proportionality, which requires that:

– a fair balance must be struck between the competing rights of the intercept subjects and the purposes pursued, in accordance with the principle that the graver the above-mentioned offences or activities and their past or future consequences, the more intrusive and extensive the interception may be; and

– in any event the interception must ensure that the essence (or minimum core) of the rights of the intercept subjects is respected, such as the right to intimate private life in the case of physical persons. Interception must cease as soon as it becomes apparent that it is encroaching upon the core of private life.

(f) A limit on the duration of the interception order, which can be extended one or more times after an assessment of the results of the operation, but in any event with a maximum time-limit imposed for the whole operation.

(g) End-to-end judicial oversight, which includes:

– authorisation of interception, including the specific bearers to be intercepted and strong selectors to be used;

– regular control of the implementation of the interception order, at sufficiently short intervals, including extension of the duration of the interception order and transmission of the data obtained to third parties; and

– *ex post facto* review of the interception process and the data intercepted.

(h) In cases of urgency, a special interception order may be made by a public prosecutor, but must be confirmed by a judge within a short period of time.

(i) The procedure to be followed for examining, using, storing and destroying the data obtained, with a detailed description of the scope of the judge's oversight during the implementation stage and after the interception has ended and the documentation of the key steps of data deletion in so far as this is necessary for the judge's oversight.

(j) The conditions to be fulfilled and the precautions to be taken when exchanging intercepted data with foreign intelligence services, as follows:

– an absolute prohibition from outsourcing surveillance operations circumventing the domestic rules;

– an absolute prohibition for an intelligence authority which received data from a foreign intelligence service from sharing it with a third party without the consent of the originator, this rule not limiting the access of the domestic judge of the receiving State to the transferred data;

– an absolute prohibition from exchanging data with foreign intelligence services which do not ensure a level of protection essentially equivalent to that guaranteed by the Convention;

– an absolute prohibition of bulk transfer of data to, or receipt from, a foreign intelligence service in a continuous process based on a single purpose;

– judicial authorisation prior to every transfer/receipt of data in accordance with the exact same principles and rules of domestic bulk interception, including, among others, the observance of the principles of necessity and proportionality; and

– these rules apply without distinction between solicited and unsolicited data, "raw" (unevaluated) and evaluated data.

(k) The duty to notify the intercept subject when the interception is over, save where the interests of national security would be endangered by such disclosure, in which case the competent judge must be empowered to review on his or her own initiative (*ex proprio motu*) or on the initiative of a third party (for example, a public prosecutor) the entire process of interception in order to determine whether the data was obtained lawfully and whether it should be kept or destroyed, the intercept subject then being defended by a privacy lawyer.

(l) Special guarantees with regard to the secrecy of professional communications of privileged communicants such as parliamentarians, medical doctors, lawyers, journalists and priests.

(m) The guarantee that a criminal conviction may not be based solely or to a decisive extent on the evidence collected by means of bulk interception.

(n) These principles apply to surveillance conducted in the Contracting Party's own territory as well as to its surveillance performed extraterritorially, regardless of the purpose for the surveillance, the state of the data (stored or in transit), or the possession of the data (data held in the intercept subject's possession or in the possession of a service provider).

(o) The State's obligation to respect and fulfil individuals' rights is complemented by an obligation to protect individuals' rights from abuse by non-State actors, including corporate entities.

# IV. CRITIQUE OF THE IMPUGNED UK BULK INTERCEPTION REGIME

## A. Bulk interception of communications

35. Having regard to the above, I have a principled objection, well beyond the Grand Chamber's tenuous challenge, to the United Kingdom's bulk interception regime, as it stood on 7 November 2017, which means before the full entry into force of the Investigatory Powers Act 2016 ("the IPA")[109].

36. The purpose of bulk interception in detecting and investigating serious crime as defined under section 81(2)b RIPA is definitively not compatible with the concept of serious crime prevailing in international law, in so far as the domestic concept encompasses offences punishable by imprisonment for a term of less than four years. Furthermore, the purpose of safeguarding the economic well-being of the United Kingdom in so far as those interests are also relevant to the interests of national security is not sufficiently precise, allowing bulk interception to be used, for example, for economic and industrial espionage and "trade war" purposes[110].

37. The very general terms of the Secretary of State's section 8(4) certificates were also reproached, and correctly so, by the Intelligence and Security Committee of Parliament (ISC)[111].

38. The distinction between internal and external communications, as set out in section 20 RIPA, is fundamentally defective and does not sufficiently circumscribe the categories of people liable to have their communications intercepted. As concluded by the ISC, this distinction was confusing and lacked transparency[112].

39. The Government's justification for this distinction was that "[w]hen acquiring intelligence on activities overseas, the Intelligence Services do not have the same ability to identify targets or threats that they possess within the UK"[113]. The IPT reiterated the argument, stating that "it was harder to investigate terrorist and criminal threats from abroad"[114]. This justification must be understood against the background of the 2014 Government's

---

[109] Paragraph 270 of this judgment. This means that, just like the Grand Chamber, I have not taken into consideration the changes introduced by the IPA and the new 2018 IC Code. They were not before this Court.

[110] See the interesting discussion between the parties during the Grand Chamber hearing on 10 July 2019 on this exact point. The Court has defended different views on the precision of the purpose of national security (compare and contrast *Iordachi and Others v. Moldova*, no. 25198/02, § 46, 10 February 2009, and *Kennedy*, cited above, § 159).

[111] Paragraph 146 of this judgment.

[112] Paragraph 145 of this judgment.

[113] See the respondent Government's observations before the Grand Chamber of 2 May 2019, p. 9.

[114] Paragraph 51 of this judgment, which the Court reiterated in paragraph 375.

disclosures, which acknowledged that the requests for bulk material were made to a foreign intelligence service "otherwise than in accordance with an international mutual legal assistance agreement"[115]. Thus the impugned bulk interception system was created to avoid the time-consuming and resource-intensive procedures and "harder" obligations stemming from the existing international law framework of mutual legal assistance, in other words, to bypass safeguards under the existing system of international mutual assistance treaties and to take advantage of its lack of regulation of new transnational surveillance technologies.

40. Furthermore, with an increasing amount of communication being treated as external[116], and the exponential increase in bulk interception of more and more communications of individuals who are in the British Islands[117], the external/internal communications distinction is simply not technically feasible to sustain, and is therefore meaningless. The territorial jurisdiction-based distinction between external and internal communications is inherently contradictory with the reality of today's flow of communication on the Internet, where a Facebook message exchanged within a group of friends in London is routed via California and is therefore "external" to the United Kingdom[118]. As the Law Society reminded the Court, confidential communications between lawyers and clients, even when both were in the United Kingdom, could be intercepted under the section 8(4) regime[119]. In practice, the Government's expansive concept of external communications also includes cloud storage, Google searches, browsing and social media activities[120]. For many types of communication, it may not even be possible to distinguish between external and internal communications since the location of the intended recipient will not always be apparent from the related communications data. The factual analysis of whether a particular communication is external or internal may in individual cases only be possible to carry out with the benefit of hindsight[121]. Today's closer interconnectedness of living and communication conditions across borders is certainly not an argument for treating external and internal

---

[115] Paragraphs 36 and 116 of this judgment, which refers to paragraph 12.2 of the IC Code.
[116] Paragraph 47 of this judgment.
[117] As the respondent Government put it, "[b]ut the fact that electronic communications may take any route to reach their destination inevitably means that a proportion of communications flowing over a bearer between the UK and another State will consist of 'internal communications': i.e., communications between persons located in the British Islands" (see their Observations before the Grand Chamber of 2 May 2019, p. 20).
[118] Paragraph 75 of this judgment.
[119] Paragraph 321 of this judgment. See also the IPT judgment *Belhadj & Others v. the Security Service & Others*, IPT/13/132-9/H.
[120] Paragraph 75 of this judgment. This practice seems to contradict paragraph 6.5 of the IC Code.
[121] The respondent Government themselves admitted this (see their Observations before the Grand Chamber of 2 May 2019, p. 37).

communications differently, but rather the opposite. This, of course, should not be understood as an invitation to lower the level of protection of internal communications, but to increase the level of protection of external communications.

41. In this regard, it is not evident that a communication between a person in Strasbourg and a person in London should be entitled to more limited protection under the Convention than a communication between two persons in London. There does not, therefore, seem to be any objective justification for treating such persons differently, other than the assumption that threats come more often than not from abroad, and that foreigners are less deserving of trust than nationals, because they pose a more serious risk to national security and public safety than nationals, thereby justifying the need for monitoring communications sent or received outside the British Islands[122]. This is also reflected in the way foreigners are treated in court when they want to uphold their privacy rights. The IPT does not accept complaints from applicants outside the national territory[123]. This foreigner-unfriendly *Weltanschauung* could not be more alien to the spirit and letter of the Convention[124]. The Convention places at its centre the individual, not the citizen of a State, which means that Convention rights as rights of the individual ought to provide protection whenever a Contracting Party acts and thus potentially creates a need for protection – irrespective of where, towards whom and in what manner it does so. Furthermore, the Convention rights should permeate the participation of Council of Europe member States in the international community, in so far as "the Council of Europe legal order can no longer be confused with the traditional international

---

[122] It does not suffice to argue that since the British legislation "prevents intercepted material from being selected for examination according to a factor 'referable to an individual who is known to be for the time being in the British Islands', any resulting difference in treatment would not be based directly on nationality or national origin, but rather on geographical location", as the Chamber judgment did (§ 517), for the obvious reason that the vast majority of people known to be for the time being in the British Islands are British citizens, and vice versa the majority of those outside are foreigners. The more beneficial treatment of nationals was also noted by the FRA (*Surveillance by intelligence services*, cited above, p. 45: "When intelligence services conduct surveillance domestically, the applicable legal safeguards are enhanced comparing to those in place for foreign surveillance").

[123] IPT, *Human Rights Watch & Ors v. SoS for the Foreign & Commonwealth Office & Ors*, 16 May 2016: "In respect of any asserted belief that any conduct falling within s.68(5) of RIPA has been carried out by or on behalf of any of the Intelligence Services, a complainant must show that there is a basis for such belief, so that he may show that he is potentially at risk of being subjected to such conduct. Further such a claimant must show in respect of such a complaint that he is or was at a material time present in the United Kingdom."

[124] The Venice Commission Report (cited above, p. 17) makes the same critique "on fundamental grounds", as does the UN Special Rapporteur on the promotion of the right to freedom of opinion and expression, referring to the ICCPR (see paragraph 313 of this judgment).

accord of juxtaposed egoisms. Sovereignty is no longer an absolute given, as in Westphalian times, but an integral part of a human rights-serving community"[125].

42. At the end of the day, the RIPA distinction was unfit for purpose in the developing Internet age and only served the political aim of legitimising the system in the eyes of the British public with the illusion that persons within the United Kingdom's territorial jurisdiction would be spared the governmental "Big Brother". In fact, they were not. The Secretary of State could, when he or she found it necessary, determine the examination of material selected according to factors referable to an individual who was in the British Islands[126] and modify a certificate to authorise the selection of communications of that individual[127]. In addition, the by-catch of internal communications not identified in the Secretary of State's warrant was allowed whenever necessary to obtain the external communications that were the subject of the warrant[128], and according to the Government themselves, this "is in practice inevitable"[129]. That having been said, it should be noted that, in relation to bulk interception of related communications data, there was not even an external communications restriction.

43. Even if bulk interception were meant to be a foreign intelligence gathering power[130], rather than a tool for the prevention, detection and investigation of crime[131], this did not justify the lack of regulation or the breadth of the powers of the intercepting authorities. In any event, as a result of the development of digital communications, the external communications safeguard no longer acts as a meaningful constraint[132], if it ever did. And my point is that it never did, for the following reasons.

44. The Secretary of State provided no independent authorisation for a section 8(4) warrant[133], his interception warrant being a blank cheque, which did not name or describe the intercept subject, did not impose an express limit on the number of communications which could be intercepted, and did not specify bearers or selectors. No specific provision governed the case where there was a request for the communications of a journalist, or a medical doctor, or a priest, or where such collateral intrusion was likely,

---

[125] Paragraph 22 of my opinion in *Mursić v. Croatia* ([GC], no. 7334/13, 20 October 2016).
[126] Section 16(3) RIPA.
[127] Paragraph 6.2 of the IC Code.
[128] Section 5(6)(a) RIPA and paragraph 6.6 of the IC Code.
[129] Respondent Government's Observations before the Grand Chamber of 2 May 2019, p. 37.
[130] Under paragraph 6.2 of the IC Code, "section 8(4) interception is an intelligence gathering capability".
[131] Section 81 RIPA defines prevention and detection of crime, but not investigation.
[132] The Venice Commission report (cited above, p. 11) makes the same point.
[133] The United Kingdom Parliament acknowledged, in its 2015 ISC report, the lack of independence of the Secretary of State, prior to the changes introduced by the IPA in 2016.

other than the innocuous paragraphs 4.28 to 4.31 of the IC Code[134]. The choice of bearers and the application of selectors, including strong selectors, to external communications was dependent on the final say of the intercepting authority[135]. In plain words, the intelligence community was in full control of the authorisation procedure, keeping the Secretary of State at bay from essential information, with the consequence that he or she could not deliver a proper proportionality and necessity analysis, but just whitewashed politically the operation of the system[136].

45. Moreover, the code of practice issued by the Secretary of State was not binding, allowing departure from it for good reason. Worse still, the daily work of the analysts was governed by "below the waterline" arrangements, which were not available to the public, not even in a cursory fashion or redacted manner[137]. This administrative leeway of the intercepting authority defeated the purpose of the legality principle, according to which the rules governing bulk interception must have a basis in domestic law and that this law must be accessible and foreseeable as to its effects.

46. The regulatory weakness of the system was further aggravated by the status of the Interception of Communications Commissioner ("the IC Commissioner"), who was not an independent authority and provided for no effective oversight of the implementation of the interception warrant[138]. As the 2015 ISC Report put it, "while the two Commissioners are former judges, in their roles as Commissioners they are operating outside the official judicial framework", concluding that "a number of these responsibilities are currently being carried out on a non-statutory basis. This is unsatisfactory and inappropriate"[139]. This is not the worst aspect of the IC Commissioner's legal status. As a matter of law, the Prime Minister

---

[134] Provisions applicable to section 8(4) material which is selected for examination and which constitutes confidential information (paragraph 4.32 of the IC Code). The respondent Government now acknowledge "that requests for communications data intended to identify journalistic sources should be subject to judicial approval" (UK response to Council of Europe Human Rights Commissioner – Memorandum on surveillance and oversight mechanisms in the United Kingdom, p. 24).

[135] Paragraphs 146-47 of this judgment.

[136] This was also the conclusion of the 2015 ISC report (see paragraph 147 of this judgment). It comes as no surprise then that in 2016, a total of 3,007 interception warrants were issued and only five requests were refused by the Secretary of State (paragraph 170 of this judgment). The figures say it all: the Secretary of State was there just to rubber-stamp the requests.

[137] Paragraph 33 of this judgment.

[138] See paragraph 347 of the Chamber judgment, and paragraph 26 of the separate opinion of Judge Koskelo, joined by Judge Turković, which points to the fact that the United Kingdom system is in fact behind the German system of safeguards existing at the time of *Klass and Others* and *Weber and Saravia*.

[139] Regrettably, this passage of the 2015 ISC report, which is referred to in paragraph 142 of the judgment, was overlooked by the majority.

appointed the IC Commissioner, who reported to him or her and was dependent on the staff provided by the Secretary of State[140]. In addition, it was a part-time job and the IC Commissioner could be dismissed by the Prime Minister at any moment[141]. This status was evidently not compatible with the independence required for effective supervision of the operation of the section 8(4) regime. In short, the Commissioners were not "institutionally, operationally, and financially independent from the institutions they [were] mandated to oversee", as required by the Tshwane principles[142].

47. Even assuming, for the sake of the discussion, that the Commissioner's oversight in the United Kingdom was independent, it was not effective, for the simple reason that, when confronted with a serious error, the Commissioner would only have the power to make a report to the Prime Minister to draw this error to his or her attention and, if so, to decide to what extent it was possible to publish that error[143]. For example, he could neither refer the case to the IPT, nor notify the victim of excessive interception. In fact, the Commissioner even failed to identify that the applicants Amnesty International and the South African Legal Resources Centre had been subjected to unlawful surveillance!

48. The duration of interception and retention periods had no specific maximum time-limit in the law, and the practice did not fill this gap[144]. Section 8(4) warrants could be renewed *ad aeternum*[145]. Moreover, retention periods differed between different intercepting authorities[146] and the "normal" maximum time-limit for retention under paragraph 7.9 of the IC Code (i.e. two years) could be dispensed with by a senior official of the intercepting authority itself. This is a telling sign of who ran the show in the British bulk interception system[147].

---

[140] Paragraph 57 of RIPA 2000.

[141] The critique made by the applicant during the Grand Chamber hearing on 10 July 2019 is legitimate: a single retired judge working part-time and with a small secretariat and conducting a modest sample analysis "cannot hope to exercise meaningful oversight".

[142] On these principles and their role within the Council of Europe, see my separate opinion in *Szábo and Vissy* (cited above).

[143] As acknowledged by the respondent Government in the Grand Chamber hearing on 10 July 2019.

[144] As described by the respondent Government (see paragraph 403 of this judgment). It seems that even the internal policies are not complied with (see paragraph 59 of this judgment).

[145] Paragraphs 6.22 to 6.24 of the IC Code.

[146] Paragraph 176 of the judgment.

[147] It is quite astonishing that the majority, in paragraph 405 of the judgment, only found it "desirable" that the practice described by the respondent Government in the Grand Chamber be enshrined in the law.

49. There was no notification obligation at the end of the interception process[148]. In the absence of such notification, the right of access to a court was largely futile. That was the case in the United Kingdom[149]. The IPT acted only upon a complaint by a person who believed that he or she had been subjected to secret surveillance, which meant that the IPT was a purely theoretical guarantee for all those intercept subjects who had no idea that their communications had been intercepted[150]. The insufficiency of the IPT oversight was compounded by the fact that it had no power to make a declaration of incompatibility if it found primary legislation to be incompatible with the ECHR, as it was not a "court" for the purposes of section 4 of the Human Rights Act 1998; that its rulings were not subject to appeals; and, strangely enough, that the Secretary of State had the power to adopt the IPT's procedural rules, which in practice meant that the supervised entity had the power to determine the rules that governed the supervisory body[151].

### B. Exchange of intercept data with foreign intelligence services

50. There is no express statutory framework analogous to RIPA governing the authority upon which the British government can use intercept data from a foreign country. Only in January 2016 did Chapter 12 of the IC Code set the framework for such exchange[152]. Under paragraph 12.5 of the IC Code, and its accompanying footnote, requests for intercepted communications and related communications data from a foreign intelligence service could be made for "material to, from and about specific selectors"[153]. The NSA abandoned the "about" collection in April 2017, because it could not be conducted lawfully due to its inadmissible

---

[148] IPA introduced a requirement for the Commissioner to consider whether there has been a serious error and it would be in the public interest to notify the individual, but this rule is not before the Court in the present case. The IPA policy choice is a concession that the previous system was insufficient, and it will be for another day to see if the IPA solution is sufficient.

[149] This is aggravated by the NCND ("neither confirm, nor deny") policy of the Government, which "prevents a person from ever knowing if he/she has been the target of surveillance" and "shields surveillance decisions from effective scrutiny", as the Council of Europe Human Rights Commissioner concluded (Memorandum, cited above).

[150] Thus the majority's conclusion that the IPT is "a robust judicial remedy to anyone who suspected that his or her communications had been intercepted" (§ 415) fails to identify the patent shortcoming of the system: its virtual character for those who have no reason to suspect that they have been subjected to secret surveillance.

[151] Section 69(1) RIPA.

[152] The respondent Government said that, "even prior to the issue of chapter 12 of the Code, it was 'accessible' as a result of the Disclosure", referring to the October 2014 disclosure (see their Observations before the Grand Chamber of 2 May 2019, p. 49). This shows that even the Government admit that prior to that moment the law was not accessible.

[153] Paragraph 116 of this judgment.

massive overreach[154]. Yet the Court's surprising willingness to accept the "collect it all" policy of the respondent Government[155] goes beyond even the NSA playbook, admitting not only "about" collection requests, but even requests for material other than in relation to specific selectors[156].

51. According to the Court, the transfer of bulk material to foreign intelligence partners should be subject to "independent control"[157], but the receipt of bulk material collected by foreign intelligence authorities should not be[158]. If the safeguards are inadequate in relation to direct surveillance by the United Kingdom's intercepting authorities, they ought to be considered as inadequate also for indirect surveillance by them, resulting from intelligence sharing of third-party intercept material; even more so where such material is collected by a third party not bound by the Convention. When the danger of material collected and stored in a non-Convention-compliant manner is higher, and therefore independent oversight is most needed, the Court has renounced this safeguard, without any plausible justification[159]. In this regard, the oversight of the IC Commissioner and the IPT, invoked by Government and the majority in the Grand Chamber, was practically inoperative, in controlling intelligence sharing from third-party intercept material no less than in overseeing domestic surveillance, since the IPT's intervention depended on a complaint and the IC Commissioner had no power other than to make a report to the Prime Minister to draw any serious error to his or her attention.

52. The absurd consequences of the majority's reasoning are even more patent in the following example: if one Londoner sends a message on Twitter to another Londoner, and that communication is transmitted via a server in the United States, the Court accepts that the interception by the Government Communications Headquarters (GCHQ) of that message and the related communications data, when it leaves the United Kingdom on a cable bound for the United States, deserves the guarantee of independent authorisation. But if the NSA intercepts that same message at the other end of the same cable and then gives a copy to GCHQ, or the communications data relating to it, the guarantee of independent authorisation does not

---

[154] Paragraph 263 of this judgment.

[155] In the words of the respondent Government in the Grand Chamber hearing of 10 July 2019: "[S]o to the extent that the sting of the questions is have you got lots of data, even after the end of your filtering process, the answer to that question is 'yes' and a jolly good thing too, we submit."

[156] Paragraphs 502 and 503 of this judgment.

[157] Paragraph 362 of this judgment.

[158] Paragraph 513 of this judgment.

[159] Unfortunately, the Court ignored the position of the Human Rights Committee in its 2015 Concluding observations on the United Kingdom, UN Doc. CCPR/C/GBR/CO/7, 17 August 2015, paragraph 24, where it voiced concern over the "lack of sufficient safeguards in regard to obtaining of private communications from foreign security agencies and the sharing of personal communications data with such agencies".

apply. It is entirely arbitrary for there to be different legal protections for the same data based only on the accidental location of who carried out the initial interception. The absence of a statutory scheme of safeguards for the use of intercept data from a foreign country that is equally protective as that applying to intercept data collected in the home country, means that the United Kingdom law is insufficient to protect against arbitrariness and abuse[160].

53. Furthermore, under paragraph 12.6 of the IC Code, sections 15 and 16 RIPA did not apply to all material received from foreign intelligence services that could be the product of bulk interception, but only to requested intercept material or "where the material identifie[d] itself as the product of intercept", which left the triggering of the domestic guarantees of the receiving State (the United Kingdom) dependent on a decision of the foreign intelligence services.

54. The portrayal of the exchange of bulk material with other parties would be incomplete without mentioning another noteworthy feature. It should be added that paragraph 7.3 of the IC Code allowed for disclosure of intercepted material to other parties in accordance with the mere convenience of the service, an astonishingly simplistic criterion. The "need-to-know principle"[161] is the logical opposite of the necessity and proportionality tests: the principle that only so much of the intercept material can be disclosed as the recipient needs is the antithesis of those tests. The use of this disclosing power is not subject to an objective statutory threshold, but merely guided, and possibly misguided, by the purpose pursued. Thus, purely opportunistic considerations prevailed over the assessment of the necessity and proportionality of the additional interference with the intercept subject's rights constituted by the disclosure of the intercepted material to other parties. In simple words, the individual's communication is treated as a possession of the State, a commodity that the State can share with other parties at its discretion in order "to see if the haystack contains a needle"[162].

### C. Bulk interception of related communications data

55. Lastly, section 16(2) RIPA did not apply to bulk interception of related communications data, which meant that any analyst could use a strong selector referable to an individual known to be in the British Islands without any prior certification by the Secretary of State and, worse still, the intercepted data could be stored for "several months", if and as long as

[160] This is exactly what the Venice Commission calls for (see paragraph 201 of this judgment).
[161] Paragraph 7.3 of the IC Code (see paragraphs 96 and 390 of this judgment).
[162] Oral submissions of the respondent Government during the Grand Chamber hearing on 10 July 2019.

necessary to discover "unknown unknows"[163]. In practical terms, the interception and treatment of related communications data was limited only by the storage capacity of the intercepting services. In fact, RIPA does not really enshrine a foreign intelligence gathering power, because technological development has transformed it into a domestic surveillance power, and that is why the Government now pretend that the British Islands safeguard in section 16 RIPA is not "necessary" for Convention compatibility[164].

56. The Government's feasibility argument[165] does not convince me either. It is perfectly feasible for a judge to assess, in due course, the necessity and the proportionality of a request for authorisation to target the individual's related communications data in every case, without any serious risk of undermining its use[166]. If this authorisation process can be established for the targeting of journalists and other professionals whose related communications data are legally privileged, as the Court accepts[167], why cannot it be set for the targeting of the related communications data of the common mortal? Such approval systems operating in scale are perfectly possible. The point is that large-scale interferences with privacy require a large-scale system of safeguards.

57. Despite their degree of intrusiveness, both within and outside the British Islands, the Court's tolerance with these practices is incomprehensible, bearing in mind that section 16(2) is considered, by the Court itself, to be "the principal statutory safeguard circumscribing the process of selecting intercept material for examination"[168].

---

[163] Paragraphs 422-23 of this judgment.

[164] See the oral submissions of the respondent Government during the Grand Chamber hearing on 10 July 2019. This way the intercepting authority could get hold, via a bulk warrant, of content that it ought to have obtained via an individual and targeted warrant under section 8, and could therefore circumvent this Court's judgment in *Kennedy* (cited above).

[165] Paragraph 420 of this judgment.

[166] My judgment is based on my own experience as a criminal-court judge in highly complex criminal cases, where the police often requested the interception of vast amounts of related communications data.

[167] Paragraph 450 of this judgment.

[168] Compare and contrast paragraphs 420 and 421 of the judgment. Note that in paragraph 420 the language is "the principal statutory safeguard", but in paragraph 421 it is toned down to "an important safeguard". The imprecise language in paragraph 421 is perplexing, but even more disturbing is the lack of substance. The sheer manipulation of the language is instrumental for the Court's different weighting of the "concerns" raised in paragraphs 381 and 382 in the field of bulk interception of related communications data. The cherry on the cake is evidently the "overall assessment", which allows the Court to reach whatever result it wants to reach (see my analysis of this "overall fairness" criterion in my opinions appended to *Muhammad and Muhammad v. Romania* [GC], no. 80982/12, 15 October 2020, and *Murtazaliyeva v. Russia* [GC], no. 36658/05, 18 December 2018).

### D. Preliminary conclusion

58. In sum, the fact that the scope of the surveillance activity considered in *Weber and Saravia* (2006) and *Liberty and Others* (2008) was much narrower than it is today should not have led the Court to be less demanding as to the requisite level of protection of privacy rights at the present time. The exponential increase of surveillance activity in the last decade and the public outcry that it has unleashed warrant stricter oversight of the intelligence agencies' activities, for the sake of preserving democracy and defending the rule of law. Not the opposite. When the risk of State abuse increases, the Convention safeguards and corresponding domestic law guarantees should increase too, not decrease[169]. In other words, the Court's standards today should be more exacting than those of 2006 or 2008. This is exactly the opposite of what this judgment has delivered. In the present judgment the Court has succumbed to the *fait accompli* of general bulk interception, dangerously accepting that if it is useful it should be permissible. Usefulness is not the same thing as necessity and proportionality in a democratic society. As Justice Brandeis put it in *Olmstead v. United States*[170], "[i]t is also immaterial that the [telephone-tapping] intrusion was in aid of law enforcement. Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent".

## V. CONCLUSION

59. This judgment fundamentally alters the existing balance in Europe between the right to respect for private life and public security interests, in that it admits non-targeted surveillance of the content of electronic communications and related communications data, and even worse, the exchange of data with third countries which do not have comparable protection to that of the Council of Europe States. This conclusion is all the more justified in view of the CJEU's peremptory rejection of access on a generalised basis to the content of electronic communications[171], its manifest reluctance regarding general and indiscriminate retention of traffic and location data[172] and its limitation of exchanges of data with foreign intelligence services which do not ensure a level of protection essentially equivalent to that guaranteed by the Charter of Fundamental Rights of the

[169] *Szábo and Vissy*, cited above, § 70: "The guarantees required by the extant Convention case-law on interceptions need to be enhanced so as to address the issue of such surveillance practices." Likewise, PACE Resolution 2045(2015) insisted on the need for reinforced oversight of mass surveillance.
[170] 277 US 438.
[171] Paragraph 226 of this judgment.
[172] Paragraphs 211, 217 and 239-41 of this judgment.

European Union[173]. On all these three counts, the Strasbourg Court lags behind the Luxembourg Court, which remains the lighthouse for privacy rights in Europe.

60. For good or ill, and I believe for ill more than for good, with the present judgment the Strasbourg Court has just opened the gates to an electronic "Big Brother" in Europe. If this is the new normal that my learned colleagues in the majority want for Europe, I cannot join them, and this I say with a disenchanted heart, with the same consternation as that exuding from Gregorio Allegri's *Miserere mei, Deus*.

[173] Paragraph 234 of this judgment.

# JOINT PARTLY DISSENTING OPINION OF JUDGES LEMMENS, VEHABOVIĆ, RANZONI AND BOŠNJAK

1. We are in agreement with the present judgment, except for the assessment of the complaint about the receipt by the respondent State's authorities of solicited intercept material from foreign intelligence services, under Articles 8 and 10 of the Convention (see operative points 3 and 5 of the judgment).

2. In the present judgment – as also in today's judgment in *Centrum för rättvisa v. Sweden* (no. 35252/08) – for bulk interception regimes the Grand Chamber has established a system of effective "end-to-end safeguards", with three main pillars or cornerstones, in order to minimise the risk of such power being abused. These fundamental pillars are: (1) the authorisation of bulk interception at the outset, when the object and scope of the operation are being defined, by a body independent of the executive; (2) prior internal authorisation when strong selectors linked to identifiable individuals are employed; and (3) the supervision of the operation by an independent authority together with effective *ex post facto* review by a body independent of the executive (see paragraphs 350-59 of the judgment).

3. The same "end-to-end safeguards" established for a bulk interception regime should also apply to a regime where the authorities do not themselves intercept cross-border communications and related communications data, but rather ask foreign intelligence services to intercept such data or to convey already intercepted data. However, while upon receipt of the intercept material, the safeguards for its examination, use and storage, its onward transmission, and its erasure and destruction, are equally applicable (see paragraph 498 of the judgment), the first pillar, that is the prior independent authorisation, completely disappears in the majority's view. Their reasoning in that regard is not convincing for us. Why should a distinction be made according to the way the authorities have come into possession of the intercepted data, whether they intercepted the data themselves or had them intercepted by a foreign authority? Therefore, to our mind, also as far as the first pillar is concerned, the same safeguards as those established for bulk interception should apply.

4. We can fully subscribe to the Court's assessment in paragraphs 496 and 497 of the judgment, in particular that an interference with Article 8 already lies in the initial request to the foreign authorities, and that the protection afforded by the Convention would be rendered nugatory if States could circumvent their Convention obligations by requesting such data from non-Contracting States. Member States must, therefore, have clear and detailed rules which provide effective guarantees against the use of their power to circumvent domestic law and/or their obligations under the Convention.

5. Where we respectfully depart from the majority is on the question of what "effective guarantees" consist of.

6. The majority first refer to the fact that the requests were either based on warrants already authorised by the Secretary of State or explicitly approved by him or her (see paragraph 505 of the judgment). We would argue, however, that the Secretary of State is not independent of the executive and in this respect the regime governing the receipt of intelligence from foreign intelligence services is beset by the same deficiency as the bulk interception regime (see paragraph 377 of the judgment).

7. Secondly, the majority seem to assume that a national law which provides that there should be no circumvention is of itself an effective safeguard (see paragraph 506 of the judgment). We respectfully disagree. As already pointed out, for example, in the separate opinion of Judge Ranzoni in *Breyer v. Germany* (no. 50001/12, 30 January 2020), domestic law only provides for the legal basis determining the lawfulness of the interference: it does not, in addition and in itself, constitute an effective safeguard to protect the individual from the application of national law by domestic authorities in an arbitrary manner and from abuse of legal powers. Such protection must go beyond legal rules, in particular when those rules and legal powers are couched in broad terms.

8. In other words, a legal rule which prohibits circumvention or other misuse cannot at the same time be a safeguard for that not to happen. An effective safeguard supposes the availability of a mechanism capable of ensuring the correct application of that very rule. However, a safeguard of that kind is lacking with respect to requests to have data intercepted and conveyed by foreign intelligence services. In our view, as in the bulk interception regime, the first pillar within the "end-to-end safeguards" should similarly apply. Consequently, any such request should be subject to prior authorisation by an independent body capable of assessing whether it is both necessary and proportionate to the aim pursued (see paragraphs 350 and 351 of the judgment), and of ensuring that this power is not used to circumvent domestic law and/or the State's obligations under the Convention.

9. For these reasons we have voted against the finding of no violation of Article 8 of the Convention in respect of the receipt of intelligence from foreign intelligence services.

10. Since the majority conclude that the intelligence sharing regime does not violate Article 10 of the Convention, on the basis of the same reasons that led them to conclude that there has been no violation of Article 8 (see paragraph 516 of the judgment), we are equally in disagreement with their finding under Article 10.

# APPENDIX

## List of applicants

| Application no. | Applicants |
|---|---|
| 58170/13 | Big Brother Watch |
| 58170/13 | English PEN |
| 58170/13 | Open Rights Group |
| 58170/13 | Dr Constanze Kurz |
| 62322/14 | Bureau of Investigative Journalism |
| 62322/14 | Alice Ross |
| 24960/15 | Amnesty International Limited |
| 24960/15 | Bytes for All |
| 24960/15 | The National Council for Civil Liberties (“Liberty”) |
| 24960/15 | Privacy International |
| 24960/15 | The American Civil Liberties Union |
| 24960/15 | The Canadian Civil Liberties Association |
| 24960/15 | The Egyptian Initiative for Personal Rights |
| 24960/15 | The Hungarian Civil Liberties Union |
| 24960/15 | The Irish Council for Civil Liberties Limited |
| 24960/15 | The Legal Resources Centre |