Applications 24960/15, 62322/14 and 58170/13

IN THE EUROPEAN COURT OF HUMAN RIGHTS

GRAND CHAMBER

B E T W E E N:

BIG BROTHER WATCH and others

10 HUMAN RIGHTS ORGANISATIONS

BUREAU OF INVESTIGATIVE JOURNALISM and others

Applicants

- and -

UNITED KINGDOM

Respondent

APPLICANTS' WRITTEN OBSERVATIONS

Contents

Abbreviated References to Documents in Observations

Document	Bundle reference	Abbreviation
10HROs Application (24960/15) dated 31 March 2015	BG2/15	10HROs App 31 Mar 2015
10HROs Reply dated September 2016	BG2/18	10HROs Reply Sep 2016
10HROs Update Submissions in Light of Third IPT Judgment dated 31 July 2015	BG2/16	10HROs Update 31 Jul 2015
Acquisition and Disclosure of Communications Data Code of Practice (March 2015)	CB2/32	2015 Acquisition Code
Interception of Communications Code (amended in January 2016)	CB2/33	2016 Interception Code
Applicants' Consolidated Observations dated 29 September 2017	SB/2	App Cons Obs 29 Sep 2017
Independent Review of Terrorism Legislation (David Anderson QC), "A Question of Trust" dated June 2015	CB2/48	AQoT
BBW Application (58170/13) dated 30 September 2013	BG1/6	BBW App 30 Sep 2013
BBW Update Submissions dated 2 March 2015	BG1/7	BBW Update 2 Mar 2015
BIJ Application (62322/14) dated 1 September 2014	BG1/11	BIJ App 1 Sep 2014
BIJ Reply Observations	BG2/13	BIJ Reply
Expert Report of Dr George Danezis dated 13 August 2014	CB1/10	Danezis
10HROs Factual Appendix dated September 2016	BG2/19	Factual Appendix
Witness Statement of Charles Blandford Farr dated 16 May 2014	CB1/9	Farr 1
First Judgment of the Investigatory Powers Tribunal (10HROs) of 5 December 2014	CB1/14	First IPT Judgment
Judgment of the First Section in these Applications		First Section
Interception of Communications Commissioner, "Report of the Interception of Communications Commissioner" (2014 Annual Report) dated March 2015	CB2/36	IOCC 2014 Annual Report
Intelligence and Security Committee Report, "Privacy and Security: A modern and Transparent Legal Framework" dated 17 March 2015	CB2/47	ISC Report
Witness Statement of Eric King dated 8 June 2014	CB1/5	King 1
Third Judgment of the Investigatory Powers Tribunal (10HROs) of 22 June 2015	CB1/16	Third IPT Judgment
UK Observations dated 16 December 2016	BG2/14	UK Obs 16 Dec 2016
UK Observations dated 29 September 2017	SB/3	UK Obs 29 Sep 2017

Bundles:
BG: Background Documents Bundles (2 volumes)
CB: Core Documents Bundles (3 volumes)
SB: Applicants' Supplementary Bundle (1 volume)

A ***Introduction***

1. This is the first occasion on which the Grand Chamber will consider the compatibility of an overtly bulk surveillance regime with the European Convention on Human Rights. The Applicants invite the Grand Chamber to state the law authoritatively on modern bulk surveillance practices.

2. The Applicants submit that bulk surveillance is incompatible with the protection of privacy and freedom of expression of individuals which the Convention provides. The Applicants invite the Grand Chamber to find that the UK's bulk surveillance regime breaches Articles 8 and 10 of the Convention.

3. In the alternative, the Applicants invite the Grand Chamber to endorse the First Section in so far as it found the UK's regime in violation of Articles 8 and 10. The First Section was correct that the UK regime is inadequate, applying the Court's existing case law.

4. In addition, the Applicants invite the Grand Chamber to update the "minimum safeguards" established in the Court's case law. There has been an exponential increase in the use of internet-based technology to communicate and rapid advancements in the state's ability to extract, on an enormous scale, sensitive and personal information from intercepted material. Updating the Court's safeguards in light of these technological and social developments is now necessary to give practical effect to the Convention rights in the current age, as the Fourth Section recognised in *Szabó & Vissy v Hungary*, no 37138/14, 6 June 2016.

5. In summary, and in answer to the Court's questions, the Applicants submit:

   a) Bulk interception **interferes with the rights in Articles 8(1) and 10(1)**.

   b) The UK bulk interception regime is **neither strictly necessary nor proportionate** to the severe interference with Articles 8 and 10 rights entailed. The mass interception, processing and storage of private communications is not compatible with the Convention.

   c) The UK arrangements for bulk interception are in any case **not in accordance with the law**. Important rules governing the scheme are **not accessible**. The disclosed arrangements are not **foreseeable**. Nor do they provide adequate **safeguards** against arbitrary conduct:

i) The regime is extraordinarily complex and obscure and thus **not foreseeable**. The regime governing bulk interception is in part **not accessible** because much of the relevant detail is unjustifiably "*below the waterline*" (an unhelpful euphemism for "secret").

ii) The existing minimum requirements, first applied to a (more limited) bulk interception regime in *Weber & Saravia v Germany*, no 54934/00, 29 June 2006, are not satisfied. In particular, as the First Section found, the UK's controls over the use of **selectors** (specific identifiers relating to a known target) are inadequate and there is no sufficient protection for **communications data** (metadata). Automated, bulk analysis of communications data can be more invasive of private life than content.

iii) **Additional safeguards** are now required, in light of increased technological capabilities, to protect democratic societies from the risks of bulk surveillance to privacy and other fundamental freedoms. Those safeguards include:

a) **prior independent judicial authorisation** of **warrants** and **selectors or queries**;

b) a requirement for **reasonable suspicion against the person concerned**; and

c) **notice** to persons affected, where possible.

d) The UK's **intelligence sharing arrangements** for **receipt of intercepted material (in bulk or otherwise) from foreign intelligence agencies** interfere with Articles 8 and 10 rights, and are not in accordance with the law, proportionate or strictly necessary in a democratic society for the same reasons as those in respect of the bulk interception regime. It makes no difference to privacy whether the UK Government itself intercepts or is given access to the relevant material.

e) The First Section was correct to hold that the UK's regime for bulk surveillance contains insufficient protection for **journalistic sources and material**, but there are additional reasons why this regime is not in accordance with the law under Article 10.

6. Contracting States face serious risks from organised criminality, including terrorism. It is important that competent authorities have the right tools to address risks to security of the person and democratic society. Combatting these threats requires concerted police and intelligence work, including covert surveillance and interception. But such operations must be conducted within the framework of the Convention, so as to avoid "*the danger such a law poses of undermining or even destroying democracy on the ground of defending it*" (*Klass v Germany*, no 5029/71, 6 September 1978, §49).

7. By contrast, the UK regime puts at risk the very values protected by the Convention that terrorism seeks to undermine. The UK claims the power to intercept, in bulk, any communications that happen to traverse the UK. It then analyses, profiles and stores those communications and the related communications data. The UK asserts the power to receive similar bulk access to communications intercepted by intelligence services of other states. Such a regime is not compatible with the Convention and poses real dangers.

8. In any event, the UK regime also fails to satisfy this Court's minimum safeguards, both in their current form (as identified most recently by the Grand Chamber in *Roman Zakharov v Russia*, no 47143/06, 4 December 2015), and as the Applicants suggest they should be updated and enhanced. The UK safeguards are limited, especially seen alongside arrangements in other states, in particular Germany (as described in *Weber)* and Sweden (as described in *Centrum för Rättvisa v Sweden*, no 35252/08, 19 June 2018). The Applicants do not accept that the German regime considered in *Weber* and the Swedish regime meet what Articles 8 and 10 now require. However, the contrast to the UK regime is nonetheless striking and the inadequacies of the UK regime apparent. Under the UK regime:

   a) No independent, let alone judicial, authorisation is required. Only a politician needs to approve a warrant.

   b) There is no requirement to obtain independent, let alone judicial, approval before adopting selectors or search terms.

   c) The safeguards for the content of communications of persons in the British Islands are limited and partial. And they do not apply to communications data at all.

d) The part-time oversight provided by the Interception of Communications Commissioner ("**Commissioner**"), with limited resources, has been insufficient to guarantee meaningful and robust oversight. Neither is the *ex post* supervisory jurisdiction of the Investigatory Powers Tribunal ("**IPT**") sufficient, should an application be made to it. The Commissioner and the IPT failed to identify any of the defects in the scheme found by the First Section. The Commissioner's oversight failed to identify that two of the Applicants before the Court (Amnesty International and the South African Legal Resources Centre[1]) had been subjected to unlawful surveillance in breach of written (but secret) internal procedures.[2]

e) The system permits the dragnet of bulk surveillance to extend to respected human rights NGOs as well as journalists, press outlets and media organisations.

9. Despite its submissions to the Court, the Snowden documents indicate that (when speaking privately) the UK Government Communications Headquarters ("**GCHQ**") was well aware of the permissive nature of the UK legal regime. GCHQ described the UK legal regime as a "*selling point' for the Americans*".[3] GCHQ sees itself as "*less constrained by NSA's concerns about compliance*". GCHQ is dedicated to exploiting "*to the full our unique selling points of … the UK's legal regime*." In a briefing, one of GCHQ's senior legal advisers noted "*we have a light oversight regime compared with the US.*"[4]

10. In any event, changes in society and exponential changes in technological capacity to intercept and analyse bulk data mean that the Court's existing approach and safeguards need to be updated and enhanced if they are to continue to ensure that Convention rights remain

---

[1] Amnesty International is a leading human rights organisation worldwide. The Legal Resources Centre, co-founded by Arthur Chaskalson, the former president of the Constitutional Court of South Africa, is the leading human rights NGO in South Africa.

[2] Letter from the IPT to Liberty, Amnesty International and Privacy International dated 1 July 2015 **[CB/18]**; Third IPT Judgment §§14-15 **[CB1/16]**.

[3] Nick Hopkins and Julian Borger, "*Exclusive - NSA pays £100m in secret funding for GCHQ*," The Guardian, 1 August 2013 <https://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden>.

[4] Ewen MacAskill and others, "*The legal loopholes that allow GCHQ to spy on the world*", *The Guardian*, 21 June 2013 <https://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world>.

practical and effective, not theoretical and illusory. As Lord Sumption explained in *R (Catt) v ACPO* [2015] AC 1065 **[CB3/55]**, p.1077F-G at §2 in the UK Supreme Court:[5]

> "Historically, one of the main limitations on the power of the state was its lack of information and its difficulty in accessing efficiently even the information it had. The rapid expansion over the past century of man's technical capacity for recording, preserving and collating information has transformed many aspects of our lives. One of its more significant consequences has been to shift the balance between individual autonomy and public power decisively in favour of the latter." [emphasis added]

11. The Court's existing jurisprudence on bulk surveillance derives from the admissibility decision in *Weber* in 2006, based on a decision of the Bundesverfassungsgericht in 1995 and an application in 2000. In 2006, the world was a different place. Smartphones were basic and had limited functionality (the iPhone was not launched until 2007); Facebook was a website used mainly by university students; and Twitter had just been invented. Understanding of the intrusive power of mass online interception and automated analysis of large quantities of private data was in its infancy.

12. Technological developments since then mean that governments can now create detailed and intrusive profiles of individuals and groups, including intimate aspects of people's private lives, by intercepting and analysing communications in bulk. This is due to:

    a) Development of the internet and mobile devices: Previously, as in *Weber*, bulk surveillance was limited to communications over international communications links. A foreign telephone call, fax or telex transmission was uncommon and expensive. In contrast, in the modern, internet-based world, most communications travel internationally in the course of their transmission, even if the sender and intended recipient are in the same town. The development and increased use of technology means the dragnet of bulk surveillance sweeps more widely than before.

    b) Role of communications data: Modern technology generates enormous volumes of communications data (data about communications). It is highly revealing, whether analysed technologically or by an individual, regardless of whether the content of the communication is also analysed. A mobile telephone enables its owner to be tracked

[5] Despite the above comment, Lord Sumption's majority judgment concluded that there was no breach of the Convention in *Catt*. This Court disagreed: *Catt v United Kingdom* App No. 43514/15, 24 January 2019 (First Section).

in fine detail.[6] Each time a person visits a web page, sends/receives a text message, shares an opinion online, looks at a post on social media or reads a newspaper article, a digital record is created, and becomes available for retrieval and matching with other communications data to create a profile of that person. This, and the development of technology and interception capabilities, has led the US National Security Agency ("**NSA**") to describe the current era as "*the golden age of SIGINT*" [King 2/§5].

13. In this "*golden age*", the UK is a pioneer. Through its membership of the "*Five Eyes*" group of states,[7] the UK has led large-scale sharing of bulk raw intercept material with foreign governments. If the UK is correct that its scheme is lawful, a single internet communication could be routinely intercepted many times by many different countries, each time being processed and shared with that country's intelligence partners. Where a state pioneers new interferences with privacy of exceptional scope, the role of this Court is particularly important. A state claiming a pioneer role in the development of new technologies "*bears special responsibility for striking the right balance in this regard*": see *S & Marper v UK*, no 30562/04, 4 December 2008, §112.

B ***Technological developments and their serious effect on privacy and other fundamental freedoms***

14. People in Council of Europe States, and beyond, now live major parts of their lives online. Almost all communications (other than face-to-face) are online or via public telecommunications networks. We use the internet to impart ideas, conduct research, expose human rights abuses, explore our sexuality, seek and conduct relationships, obtain medical advice and treatment, correspond with lawyers and journalists, communicate with friends, colleagues and loved ones, and express our political and personal views. We conduct many

---

[6] As Roberts CJ put it in *Carpenter v United States* pp.1-2 **[SB/10]**, "*Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI) … modern cell phones generate increasingly vast amounts of increasingly precise CSLI.*"

[7] The "*Five Eyes*" comprise the signals intelligence agencies of the United States of America, Canada, the United Kingdom, Australia and New Zealand. They pool their intelligence and resources and therefore are able to conduct mass surveillance with an unparalleled global reach.

daily activities online, such as keeping records, arranging travel, listening to music and podcasts, finding our way around, and conducting financial transactions.

15. Much of this activity is conducted on mobile digital devices, such as mobile phones, tablets and laptops, which are seamlessly integrated into our personal and professional lives and usually carried everywhere we go. These devices, and cloud storage, have replaced our fixed-line telephones, filing cabinets, wallets, calendars, private diaries, photo albums, newspapers and magazines, maps, music and video collections, and address books.

16. The internet and modern communication devices also enable the creation of far greater quantities of metadata (or, under the UK's Regulation of Investigatory Powers Act 2000 ("**RIPA**"), "*communications data*"). Communications data is information about communications, which may include the identity of the sender and recipient, the date on and location from which a communication was sent and where it was received, websites visited or services used, the duration and frequency of communication.

17. Mobile phones continuously generate communications data as they constantly contact the mobile network, producing a record of the location of the phone (and therefore its user), allowing a person's movements to be tracked and, in addition, revealing their internet usage.

18. Communications data reveals enormous amounts of often sensitive information about the lives of individuals. As the Court of Justice of the European Union ("**CJEU**") said of communications data in the Judgment of 21 December 2016, *Tele2 Sverige and Watson*, C-203/15 and C-698/15, ECLI:EU:C:2016:970 §99 **[CB3/57]**:

> "That data, taken as a whole, is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them … <u>In particular, that data provides the means … of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications</u>" [emphasis added].

19. The infrastructure enabling modern mass communications has changed fundamentally and continues to evolve. Modern communications rely largely on internet technologies, rather than voice circuits over copper cables. Internet communications travel via high-bandwidth fibre-optic cables. They can transmit millions of communications simultaneously. Access to

them gives access to those communications and associated communications data. Further, data often travels via foreign servers. For example, Facebook or WhatsApp messages, or emails, between two Londoners may be routed via California servers and are thus likely to be intercepted by the UK's bulk surveillance techniques and/or accessible via the intelligence sharing arrangements with the US, and subjected to automated profiling and analysis.

20. The costs of storing, processing and collating data have also decreased drastically. This continues every year. And technical means of analysing data have also advanced rapidly as computers have become more powerful and cheaper.

21. Further, communications data is structured such that computers can process and search for patterns in the data faster and more effectively than similar searches over content. Indeed, access to content is often unnecessary: as the Royal United Services Institute ("**RUSI**") Panel (which included former heads of each of the UK's intelligence services) put it:

> "Aggregating data sets can create an extremely accurate picture of an individual's life, without having to know the content of their communications, online browsing history or detailed shopping habits. 'Given enough raw data, today's algorithms and powerful computers can reveal new insights that would previously have remained hidden'."[8]

22. More graphically, former NSA General Counsel Stewart Baker said "*metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content*". General Michael Hayden, former CIA and NSA Director, agreed. He said that Mr Baker was "*absolutely correct … we kill people based on metadata*" [**CB1/5/§24**].

23. Given the technological advances explained above, states can now quickly and easily process and search through massive amounts of information, both content and communications data. The UK Government frequently argues (as in this case) that communications data is less intrusive than content. That is incorrect, as the First Section rightly held [§356]. But the debate is also a distraction: it ignores the reality of the volume, invasive nature and ease of automated processing of modern communications data, and the ability to match across different datasets, which is qualitatively different to the type of fixed-line telephone call

[8] Royal United Services Institute, *A Democratic Licence to Operate: Report of the Independent Surveillance Review* (13 July 2015) **[CB2/49]** §2.14 ("**RUSI Report**") (citation omitted).

records (consisting only of numbers dialled) previously considered by the Court in cases such as *Malone v United Kingdom*, no. 8691/79, 2 August 1984, §§17, 64 and 84.

24. These technological advances raise serious concerns for investigative work on matters of public interest, such as human rights, as well as journalism, specifically protection of journalistic sources and information. As Professor Danezis says [Danezis/§§63-89 **CB1/10**], modern data-mining technology has led to sophisticated new ways of aggregating and exploiting communications data. This risks intrusion into journalistic material, adversely affecting journalists' right to free expression and those of their sources by its chilling effect.

C The developing case law of the Court

25. The Court has long recognised the intrusiveness inherent in government interception of communications. It has also repeatedly developed its jurisprudence, as has been necessary to protect Convention rights in the light of rapid technological change.

26. *Klass* was decided in September 1978, over 40 years ago, when only fixed-line telecommunications were available and the internet did not exist for practical purposes. The Court held "*telephone conversations*" are "*covered by the notions of 'private life' and 'correspondence'*" [§41].

27. In *Malone* §§64 and 84, the Court applied *Klass* to hold that the tapping and the recording of numbers dialled from a telephone both amounted to interferences with private life.

28. The Court expanded the scope of Article 8 protection to include "*e-mail communications*" in *Weber* §77 and email and internet browsing history in *Copland v United Kingdom*, no 62617/00, 3 April 2007, §41. In *Weber* the Third Section also applied [§95] the six minimum safeguards first identified in *Huvig v France*, no 11105/84, 24 April 1990, to a (limited) regime of bulk interception.

29. In *Liberty v United Kingdom*, no 58243/00, 1 July 2008, the Court held that the bulk interception power in the Interception of Communications Act 1985 was not compatible with the Convention on foreseeability grounds. The power was alleged to have been used to intercept a single microwave telecommunications link carrying telecommunications traffic between the UK and the Republic of Ireland, for counter-terrorism purposes [§§5, 23-24, 57]. The Court held that [§63]: "[t]*he ... approach to the foreseeability requirement in this*

field has … evolved since the Commission considered the United Kingdom's surveillance scheme in … Christie v United Kingdom."

30. In *Zakharov*, the Grand Chamber considered a Russian regime for the interception of mobile telephone communications directed at individuals [§163]. The Applicant did not argue [§§180-226], and the Court accordingly did not consider, whether it was necessary to update and enhance the minimum safeguards. The Russian surveillance regime did not comply with those requirements as they stood [§§227-305].

31. Shortly after *Zakharov*, the Fourth Section expressed the view that it should again develop its approach to foreseeability. In *Szabó*, it held:

> "… the Court must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights. These data often compile further information about the conditions in which the primary elements intercepted by the authorities were created, such as the time and place of, as well as the equipment used for, the creation of computer files, digital photographs, electronic and text messages and the like. Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives" [§68] [emphasis added].
>
> "The Court would add that the possibility occurring on the side of Governments to acquire a detailed profile … of the most intimate aspects of citizens' lives may result in particularly invasive interferences with private life. … This threat to privacy must be subjected to very close scrutiny both on the domestic level and under the Convention. 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. However, it is not warranted to embark on this matter in the present case, since the Hungarian system of safeguards appears to fall short even of the previously existing principles." [§70] [emphasis added]

32. In *Centrum för Rättvisa*, the Third Section considered a bulk surveillance regime in which:

    a) The surveillance operation, search terms (or categories of search terms) and duration for which the permit is sought had to be defined in an application and authorised in advance by a court [§18].

b) Interception of communications between persons in Sweden was prohibited and any such communications accidentally collected had to be destroyed immediately upon this becoming apparent [§§15, 26].

c) Intercepted material had to be destroyed immediately if it was protected by constitutional protections relating to media sources, contained information shared between lawyer and client, or involved information given in a religious context, absent exceptional reasons [§25].

d) There was provision for notification to the persons affected [§§44-45].

33. The Applicant did not argue [see §§116-181] and so the Third Section did not consider [see §§99-114] whether the minimum safeguards needed to be updated and enhanced or whether bulk surveillance was compatible with the Convention. The Court held that the minimum safeguards were met; however, that case has also been referred to the Grand Chamber.

34. In *Ben Faiza v France*, no 31446/12, 8 February 2018 the Applicant complained about real-time GPS geolocation of his vehicle. The Fifth Section held that the French law did not, at that time, prescribe the scope of the authorities' discretion with sufficient clarity [§§58-61].

35. The Applicant also complained about the use of Article 77-1-1 of the French Criminal Procedure Code, a specific power of a prosecutor to request documents or data relevant to an investigation from third parties, which was used to request historic cell tower data in relation to him from a telephone company. The Fifth Section considered that this limited power, which applied only to existing records necessary for the purpose of a pending criminal investigation, was sufficiently foreseeable [§§69-76]. The regime contained the following features: (i) it was subject to prior authorisation by a prosecutor; (ii) if the documents concerned lawyers or journalists (amongst others), they could not be delivered without their consent; and (iii) the criminal courts could review the legality of the measure and exclude any material obtained unlawfully from the trial [§§32, 35, 73]. None of these safeguards is present in the RIPA scheme.

D ***<u>The present applications</u>***

36. The issues in these applications first came to light as a result of the disclosures of classified information made in 2013 by Edward Snowden, who formerly worked for the CIA and as a

contractor to the NSA. Mr Snowden revealed for the first time:

a) the enormous scale of modern mass collection of communications, and the fact that GCHQ does not simply intercept, scan and store communications of the persons in whom they have an interest. GCHQ also retains and stores very large volumes of data, relating to hundreds of millions of people, even where the individuals are of no intelligence interest; and

b) that GCHQ, in partnership with the signals intelligence agencies of the other Five Eyes governments, benefits from large-scale sharing of the information collected through mass and indiscriminate surveillance.

(1) Summary of the UK's bulk interception regime

37. The First Section's judgment contains extracts of the relevant legislation and other parts of UK law [§§56-122]. The Applicants summarise the key provisions.[9]

(i) Relevant functions of the UK Intelligence Services (UKIS)

38. Sections 1(2), 3(2) of the Intelligence Services Act 1994 ("**ISA**") [**CB1/25**], and s.1(2)-(4) of the Security Service Act 1989 ("**SSA**") [**CB1/24**], identify the functions of the relevant UKIS, which are defined by reference to the "*interests of national security*", "*the economic well-being of the United Kingdom*" or "*the prevention or detection of serious crime*." The functions of the UKIS are not limited to threats to national security.

(ii) Key provisions of RIPA

39. The domestic law regulating the interception of communications is principally in RIPA.

Part I, Chapter I RIPA

40. The scope of Chapter I [**CB1/22**] is set out in three provisions.

41. Section 1(1) RIPA provides:

---

[9] A new bulk interception regime in the Investigatory Powers Act 2016 ("**IPA**") has been introduced in the UK since these applications were filed with the Court. The Applicants do not accept that this regime complies with the Convention. One of the Applicants (Liberty) has challenged it in domestic proceedings, which are pending in the High Court of England and Wales.

"It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of … (b) a public telecommunications system."

42. "*Interception*" is defined in s.2(2) as where a person modifies a system or monitors transmissions so as to make the contents of communications available while they are transmitted (other than to the sender and intended recipient).

43. Interception of communications may be authorised by a warrant issued by the Secretary of State under s.5 (s.1(5)). Section 5(2)-(3) provides that the Secretary of State may issue a warrant if satisfied that:

a) 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 United Kingdom; and

b) the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

44. Section 5(6) makes clear that conduct authorised by a warrant extends to "*related communications data*" as well as content of communications. In addition, s.5(6)(a) permits so-called "incidental" collection of "internal" communications during interception:

"**5.— Interception with a warrant.**

[…] (6) The conduct authorised by an interception warrant shall be taken to include–

(a) all such conduct (including the interception of communications not identified by the warrant) as it is necessary to undertake in order to do what is expressly authorised or required by the warrant;

(b) conduct for obtaining related communications data; and

(c) conduct by any person which is conduct in pursuance of a requirement imposed by or on behalf of the person to whom the warrant is addressed to be provided with assistance with giving effect to the warrant."

45. Section 8 sets out requirements governing the content of warrants:

"**8.— Contents of warrants.**

(1) An interception warrant must name or describe either–

(a) one person as the interception subject; or

(b) a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place.

…

(4) Subsections (1) and (2) shall not apply to an interception warrant if–

(a) the description of communications to which the warrant relates confines the conduct authorised or required by the warrant to conduct falling within subsection (5); and

(b) at the time of the issue of the warrant, a certificate applicable to the warrant has been issued by the Secretary of State certifying–

(i) the descriptions of intercepted material the examination of which he considers necessary; and

(ii) that he considers the examination of material of those descriptions necessary as mentioned in section 5(3)(a), (b) or (c).

(5) Conduct falls within this subsection if it consists in–

(a) the interception of external communications in the course of their transmission by means of a telecommunication system; and

(b) any conduct authorised in relation to any such interception by section 5(6).

(6) A certificate for the purposes of subsection (4) shall not be issued except under the hand of the Secretary of State."

46. There are therefore two types of warrant. A warrant may be: (i) a targeted warrant under s.8(1); or (ii) a bulk warrant under s.8(4).

47. Section 15 requires the Secretary of State to create arrangements to secure "*general safeguards*", in particular restrictions on storage, destruction, and disclosure.

48. Section 16(1)-(2) RIPA provides a limited additional safeguard for bulk warrants. "*Intercepted material*" may only be selected for examination if it is not selected to be read, looked at or listened to according to a factor which is "*referable to an individual*" in the British Islands and "*ha[s] as its purpose, or one of its purposes, the identification of material contained in communications sent by him, or intended for him*", unless the Secretary of State certifies such examination to be necessary for the statutory purposes.

49. However, this provision:

a) Relates only to content ("*intercepted material*" is defined in s.20 RIPA to be "*the contents of any communications intercepted by an interception to which the warrant relates*") and not to related communications data;

b) Applies only where it is known that the relevant individual is present in the UK; and

c) Allows selection of material if the selection factor is not referable to a person in the British Islands or, even if referable to them, is not used for the purpose of identifying material in communications sent to/from that person.

50. The existence or otherwise of a warrant is secret. Section 17 restricts the disclosure of the existence or content of warrants granted under Chapter I and any material intercepted.

Part 1, Chapter II RIPA

51. Part 1 Chapter II RIPA empowers the UK government to require communications service providers to give it communications data. The provisions are at First Section §§110-120.

Scrutiny of Investigatory Powers under RIPA

52. RIPA provides for the appointment of an "*Interception of Communications Commissioner*", to supervise the exercise of functions under Chapters I and II of RIPA.

53. Section 59 RIPA provides for the appointment of an "*Intelligence Services Commissioner*", to supervise the exercise of functions of the UKIS under the ISA.

54. Section 65 RIPA provides for the IPT, which has jurisdiction to hear complaints regarding the conduct of the UKIS, including on human rights grounds.

(iii) Codes of Practice

55. Section 71 RIPA requires the Secretary of State to issue Codes of Practice. A Code must be taken into account by persons exercising powers under RIPA, Commissioners and the IPT (s.72). There is an Interception of Communications Code (amended in January 2016) ("**2016 Interception Code**") **[CB2/33]** and an Acquisition and Disclosure of Communications Data Code (amended in March 2015) ("**2015 Acquisition Code**") **[CB2/32]**. Under English law, an authority exercising powers under the Act may "*depart* [from guidance such as a code] ... [if it has] *cogent reasons for* [doing so]": *R (Munjaz) v Mersey Care NHS Trust* [2005] UKHL 58, [2006] 2 AC 148 §21 (Lord Bingham) §69 (Lord Hope) [**SB/7**].

(2) Summary of the UK's intelligence sharing regime

56. The United Kingdom's statutory intelligence sharing 'regime' is skeletal, comprising only:

    a) the provisions in ISA ss.1(2), 3(2) and SSA s.1(2)-(4) — bare statutory powers; and

    b) provisions of the 2016 Interception Code introduced only after Snowden's disclosures, purporting to apply RIPA to intercept material from foreign states by analogy.

E The compatibility of bulk interception under the RIPA s.8(4) regime with the Convention

(1) Facts

57. The UK Government intercepts communications and communications data from fibre-optic cables passing through the UK and elsewhere. Given the UK's geographical position, much internet data from across the world passes through the UK. The Intelligence and Security Committee ("**ISC**") has confirmed that "*GCHQ* […] *has access to communications as they move over the internet via the major internet cables*."[10]

58. The intercepted data is then processed and stored. The extent of the processing, analysis and bulk storage is far greater than, for example, the capacity to search for "catchwords" in *Weber*:

    a) The policy of GCHQ is to "*keep the entirety of all the communications data that comes into the building*", subject only to technical limits on its storage capacity and a (secret) maximum retention period [**CB2/40/§26**]. The ISC reported that "*when GCHQ intercept a bearer, they extract all* [communications data] *from that bearer … GCHQ extract all the* [related communications data] *from all the bearers they access through their bulk interception capabilities*" [ISC Report §134(iii) **CB2/47**].

    b) This is critical as "*the primary value to GCHQ of bulk interception was not in reading the actual content of the communications, but in the information associated with those communications …* [ie] *communications data*" [ISC Report §80]. Communications data is extremely intrusive: "*there are legitimate concerns that certain categories of Communications Data … have the potential to reveal details about a person's private*

[10] Report published on 25 November 2014 into the murder of Fusilier Lee Rigby [**CB2/46**].

life (ie their habits, preferences and lifestyle) that are more intrusive. This category of information requires greater safeguards …" [ISC Report §143].

c) As for content, GCHQ reportedly applies "*selection rules*" to "*automatically discard … the majority of the traffic*" [ISC Report p. 4]. This offers no meaningful privacy safeguard. Documents Mr Snowden revealed about GCHQ bulk interception program TEMPORA show that such "rules" may merely reduce high-volume low-value traffic (eg streamed content like Netflix), whilst all meaningful content is stored: "*We keep the full sessions for 3 working days and the metadata for 30 days for you to query*" [**SB/13**]. Under TEMPORA, which GCHQ described as its "*internet buffer*", "*all web, email, social, chat*" was stored "*to allow retrospective analysis and forwarding to follow on systems*" [**SB/13**]. "Selection rules" thus do nothing to prevent storage of billions of communications relating to individuals of no legitimate intelligence interest. Even if "*the majority*" are discarded, a very large amount may be retained [see King 1/§§114-115 **CB1/5**]. Further, the vast majority of the traffic on the internet can be described by the communications data alone, which is always retained. For example, if a person watches a video or reads an article, intercepting and storing the content of the video or the article is unnecessary to know what has been viewed. Communications data suffices: it is a record that a person downloaded a particular file, video, picture or text at a particular time and place. Further, by retaining all communications data, the intelligence services avoid any need to retain the vast majority of data transmitted over the internet in terms of bandwidth, which is video or music streaming. Thus the information retained: (i) is in and of itself a large amount of information; (ii) includes all communications data; (iii) is the most intrusive information for privacy purposes.

d) Nor is the selection of particular bearers to intercept reassuring, as they each carry communications of millions of people, almost all of whom are of no intelligence interest. Further, technical measures may be used to route certain types of internet traffic of particular interest (eg email and instant messages) over particular bearers to facilitate interception of the most sensitive information [Danezis/§48 **CB1/10**].

e) Even applying these rules, billions of intercepted communications are "*collected*" daily. Material (content and communications data) is then stored and can be subjected to "*automated and bespoke searches*" [ISC Report p 4]. Analysts may conduct "*additional bespoke searches*" on the mass of unselected stored data [ISC Report §70].

f) The First Section relied on the fact that "*analysts may only examine material which appears on the automatically generated index*" [§361], but this is an incomplete summary of the process. Human analysts may add material to the index simply by typing in an appropriate search term (such as a name, email address, telephone number or a broader combination of selectors) [ISC Report §70]. Further, this overlooks the automated examination that occurs, under which communications are used to profile, triage and stimulate further automated analysis.

g) The First Section also said that "*material not on the index is discarded*" [§341]. This is also incorrect. GCHQ "*keep the entirety of all the communications data that comes into the building*" [**CB2/40/§26**]. Further, content may be stored so that it may be extracted by a search carried out in the future. This is the effect of the TEMPORA programme described below. The ISC Report redacts the period for which such content is held [ISC Report §121]. The intrusion into privacy is not transient. A database is created of massive volumes of data, including content, of persons of no intelligence interest so that it may be searched in the future.

59. As to access to material:

a) If analysts wish to access <u>content</u> of communications, internal arrangements under RIPA "*require a record to be created, explaining why access to the unanalysed intercepted material is required*" before someone accesses the "*intercepted material*" under s.16 RIPA [First IPT Judgment §126 **CB1/14**]. (This requirement was disclosed only due to and during the IPT proceedings and added to the 2016 Interception Code.)

b) There is no requirement for any independent judicial (or any other) authorisation. Access to content is achieved by the analyst typing a few words of justification into a

"drop-down" box on their computer [King 1/§143 **CB1/5**].[11]

c) Under RIPA, "*intercepted material*" is restrictively defined, in s.20(1) RIPA, to mean "*the contents of any communications intercepted by an interception to which the warrant relates*" (emphasis added). Thus these internal arrangements do not apply at all where communications data is examined.

60. The Snowden documents, disclosed half a decade ago, illustrate that the permissive RIPA regime has led to highly intrusive mass databases. Given rapid increases in computer processing power and technological development, GCHQ's current capabilities are doubtless far greater than those Mr Snowden disclosed, as summarised below (emphases added):

a) In a programme known as "KARMA POLICE", GCHQ "*aims to correlate every user visible to passive* [signals intelligence] *with every website they visit, hence providing either (a) a web browsing profile for every visible user on the internet, or (b) a user profile for every visible website on the internet*" [Factual Appendix §§5-6 **CB3/51**].

b) "BLACK HOLE" is a repository, which contains internet data "*collected by GCHQ as part of bulk 'unselected' surveillance*" [Factual Appendix §§7-8]. A 2009 GCHQ PowerPoint presentation revealed that between August 2007 and March 2009, Black Hole "*was used to store more than 1.1 trillion 'events' – a term the agency uses to refer to metadata records – with about 10 billion new entries added every day*." It also indicated that "*the largest slice of data Black Hole held – 41 percent – was about people's internet browsing histories*." The remainder consisted of "*a combination of email and instant messenger records, details about search engine queries, information about social media activity, logs related to hacking operations, and data on people's use of tools to browse the internet anonymously*."

c) A 2011 GCHQ PowerPoint presentation describes GCHQ's development of "*unprecedented' techniques to perform… 'population-scale' data mining, monitoring all communications across entire countries*" [Factual Appendix §7].

[11] There are some limited restrictions on searching for information using terms referable to persons in the British Islands. These provisions are dealt with below: see paragraphs 105-109.

d) A 2012 GCHQ PowerPoint presentation indicates that GCHQ's interception capabilities had increased to the point where it was intercepting "*approximately 50 billion events per day*" but that it was working to double capacity to 100 billion events per day [Factual Appendix §8].

e) By 2011, GCHQ also operated a rolling buffer (stored copy), known as "TEMPORA", which stored the bulk data it intercepted, regardless of whether there was any ground for suspicion ("*full sessions for 3 working days and the metadata for 30 days for you to query*" – see paragraph 58.c) above). TEMPORA is described as the "*biggest internet access*" of any intelligence agency in the Five Eyes alliance [King 1/§127 **CB1/5**].

f) Under the programme "OPTIC NERVE", GCHQ collected and stored an image from every Yahoo! Chat user's webcam calls every 5 minutes ("*does not select but simply collects in bulk, and as a trade-off only collects an image every 5 minutes*" [**SB/12**]). 1.8 million Yahoo! users had their images collected. GCHQ's documents record that around 7% of the images were intimate and explicit [King 1/§§137-138, 145-146 **CB1/5**].

61. The UK adopts a "neither confirm nor deny" stance in relation to specific Snowden documents. However, it is not disputed that these are programmes the UK considers it could lawfully operate under RIPA. The Independent Reviewer was correct in concluding that "*whether or not a true and fair picture is given by the limited selection of published documents … it is clearly prudent to construct a regulatory system on the basis that programmes of the type described in these documents either exist or might in the future do so*" [AQoT §7.10 **CB2/48**]. The extent and intrusiveness of such surveillance programmes is unprecedented in human history.

(2) Bulk interception interferes with Article 8(1) rights and Article 10(1) rights

62. The UK does not dispute that there has been an interference with the Applicants' Article 8 rights [First Section §321]. The Applicants' rights under Article 10 are also engaged.

63. The concession is rightly made. Article 8(1) provides a right to respect for "*private and family life … home and correspondence*". It is well established that the bare existence of a

secret surveillance regime which could in principle apply to the Applicants constitutes an interference with their Article 8 rights, by the "*menace of surveillance*": *Szabó* §53; see also *Zakharov* §179; *Klass* §41. In addition, the interception of a communication, its storage, its automated processing, and its being read, listened to or viewed are each a separate interference with correspondence. They are each also a separate interference with private life. The same applies to communications data – see *Malone* §84.

64. Even public information can fall within the scope of private life where "*systematically collected and stored in files held by the authorities*": *Rotaru v Romania*, no 28341/95, 4 May 2000, §43; *PG v United Kingdom*, no 44787/98, 25 September 2001, §57; *Catt v United Kingdom*, no 43514/15, 24 January 2019, §93 ("*it is well established ... that the mere storing of information amounts to an interference with the applicants' right to respect for private life as secured by Article 8 § 1 of the Convention*"). Bulk interception is *a fortiori:* it involves systematic collection, analysis and storage of private (not public) electronic correspondence.

65. Maintaining privacy of personal correspondence, what we read, who we speak to and how we relate to others is an important aspect of our person. Private life is not "*limit*[ed]… *to an inner circle in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings*": *Niemietz v Germany*, no 13710/8, 16 December 1992, §29. Without privacy, the development of relationships, the work of NGOs, journalists and lawyers is hampered or chilled.

66. The UK Government suggests (without proper explanation) that no "*substantial*" interference with privacy occurs until intercept material is examined by an individual [eg UK Obs 16 Dec 2016 §9 **BG2/14**]. A substantial interference with privacy occurs when the state reads, listens to or views a private communication. But the suggestion that no "meaningful" interception occurs prior to this point is wrong, not least since bulk technological analysis of communications data can be used to provide more extensive and detailed profiles of individuals and groups than viewing content. This submission is contrary to the Court's consistent case law in *Klass*, *Zakharov* and *Szabó*, to the effect that the existence of the regime is itself a serious privacy interference, and to *Rotaru*, *PG*, *S &*

Marper and *Catt*, to the effect that even storage of personal information (let alone electronic or human analysis and extraction of information) by the state is a serious interference.

67. This argument is also dangerous: it suggests that the Court should ignore interferences from interception, storage, and automated processing of personal data and not be concerned by anything that happens before an analyst sees intercept material. If that were right, there would be no Convention difficulty with compulsorily placing a continuously recording camera and microphone in everyone's home, providing that the arrangements for viewing the recordings were acceptable. But such arrangements of themselves would have a chilling effect on privacy and freedom of expression. Automated collection, storage and automatic analysis of mass interception databases is itself a serious interference with privacy. The state's ability to collect and automatically hold and process (extract data from) such datasets, and to combine information from many sources, makes each step particularly intrusive. And as information may be extracted without a person seeing underlying material, the UK's argument has the absurd consequence that bulk interception carries no "substantial" interference with privacy at all.

68. In short:

    a) Large-scale interception and maintaining large databases of information has a chilling effect on freedom of communication, especially for journalists, NGOs or anyone who considers that their private communications should remain so. This is especially true where the data is automatically processed to create and store profiles of large numbers of internet users, which are available for rapid selection and retrieval.

    b) Storage of large amounts of data in government files may be misused. Where information about everyone may be held, risk of misuse or loss is particularly great.

    c) The storage and electronic processing may be highly intrusive: it may be used intrusively without any underlying content or communications data being viewed by an individual. The capabilities to do this are becoming more powerful, and the results more intrusive, as processing power and machine learning rapidly advance.

    d) That bulk intrusion might go unnoticed by most people does not lessen the intrusion. The risks are increased when conduct takes place secretly, as this Court recognises.

69. As regards the protection of journalistic sources and journalistic material, the existence of the provisions challenged, and their exercise, interfere with Article 8 and 10 rights.

70. The Court has, in the context of covert surveillance, previously found that such measures engage Articles 8 and 10: see *Weber* §§78-79; First Section §490. Just as interception, retention, examination, storage and dissemination of information through bulk surveillance engage Article 8, they also engage Article 10, in particular where used in a way that is capable of identifying journalistic sources or revealing journalistic material. Whilst the chilling effect is most severe where the state obtains or may obtain confidential journalistic material, the Court has previously held that the same principles and safeguards apply in respect of any "*documentation held by* [a] *journalist*" whether strictly confidential or otherwise: *Sanoma Uitgevers BV v Netherlands*, no 38224/04, 14 September 2010 §§67, 72.

71. The Court has repeatedly emphasised that protection of journalistic sources and material are important aspects of freedom of expression and that a regime for covert surveillance inhibits free expression (*Weber* at §§144-145). In *Weber* the Court reaffirmed in the context of secret surveillance of journalists that [§143]:

> "[F]reedom of expression constitutes one of the essential foundations of a democratic society and that the safeguards to be afforded to the press are of particular importance. 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 be adversely affected …"

See also *Sanoma* §50.

72. The Court has also recognised that human rights organisations operate as "*public watchdogs*" in creating platforms for public debate and imparting information on matters of public concern, and accordingly require equivalent protection to the press under Article 10: see, for example, *Társaság a Szabadságjogokért v Hungary*, no 37374/05, 14 April 2009, §27; and *Magyar Helsinki Bizottság v Hungary*, no 18030/11, 8 November 2016, §§166-167.[12]

[12] References in these submissions to "journalistic materials" and to "journalists' sources" are to be read as encompassing equivalent concepts in relation to watchdog organisations.

(3) Absence of strict necessity and proportionality of RIPA s.8(4) bulk interception

73. The First Section has sanctioned, and the UK asks the Grand Chamber to sanction, a bulk surveillance regime that alters the relationship between the individual and the state. The Applicants therefore address strict necessity and proportionality first. The s.8(4) scheme, which permits population-scale indiscriminate interception, copying, storing and filtering of communications, is neither strictly necessary nor proportionate under Articles 8 and 10.

74. Although the technology is new, the fundamental objection to such a bulk surveillance regime is not. What is now called bulk surveillance has been the subject of litigation for over 250 years. In historical common law language, an authorisation to conduct bulk surveillance is simply a new name for a general warrant. For many years, courts have prohibited surveillance in the form of general warrants because of the risk that they allow officials to select for themselves who is a suspect. A general warrant allowed state officials to investigate a broad class of undesirable conduct (what in the 1700s was called 'sedition', or, in modern language 'a threat to national security'), rather than intrude on a specified and judicially approved suspect or place.

75. Many of the leading common law cases of the 1700s concerned general warrants. The context was very similar to that of the present case. Often, it was argued that there was an urgent threat to national security and a need to detect unknown offenders. But the Courts did not permit this:

a) In *Huckle v Money* (1763) 2 Wilson 205, 95 ER 768 Lord Pratt CJ noted that:

> "To enter a man's house by virtue of a nameless [ie without specifying a named subject] warrant, in order to procure evidence, is worse than the Spanish Inquisition; a law under which no Englishman would wish to live an hour; it was a most daring public attack made upon the liberty of the subject". **[SB/4]**

b) In *Entick v Carrington* (1765) 2 Wilson KB 275, 96 ER 807, Lord Camden stated:

> "[T]here is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society; for papers are often the dearest property a man can have." [emphasis added] **[SB/6]**

c) In *Wilkes v Wood* (1763) Lofft 1, 98 ER 489 the Lord Chief Justice said:

> "The defendants claimed a right, under precedents, to force persons houses, break open escrutores,[13] seize their papers, &c. upon a general warrant, where no inventory is made of the things thus taken away, and where no offenders names are specified in the warrant, and therefore a discretionary power given to messengers to search wherever their suspicions may chance to fall. If such a power is truly invested in a Secretary of State, and he can delegate this power, it certainly may affect the person and property of every man in this kingdom, and is totally subversive of the liberty of the subject." **[SB/5]**

76. The prohibition on general warrants was ultimately incorporated into the Fourth Amendment to the US constitution ratified in 1792 ("*no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*"). This was the response to the wide use of writs of assistance, the standard form of general warrants in colonial America.

77. As Roberts CJ put it in *Riley v California* 573 US _ (2014) at p.27 the Fourth Amendment was:

> "… the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity. Opposition to such searches was in fact one of the driving forces behind the Revolution itself."

78. Since then, the costs of intercepting and storing data have decreased dramatically, and continue to do so. The technical means of analysing data have advanced so rapidly that what were previously considered impossibly large quantities of data can now be easily processed.

79. The First Section nevertheless held that bulk surveillance was acceptable in principle, given Contracting States' margin of appreciation in the area of national security [§314].

80. The First Section failed to recognise the increased dangers of the powers at issue given technical developments. The Grand Chamber is invited to give stricter scrutiny to the necessity and proportionality of bulk surveillance, recognising the UK's role as a "*pioneer*" of such surveillance. As stated by the Court in *Szabó*, "necessary in a democratic society" must be interpreted as requiring "*strict necessity*" in two respects. The secret surveillance measure must be strictly necessary (i) for "*safeguarding the democratic institutions*" and (ii) for the "*obtaining of vital intelligence in an individual operation*". The Court considered that

[13] A lockable writing cabinet. In the modern world, escrutores have been replaced by computers and smartphones.

any secret surveillance measure which did not correspond to both these criteria would be "*prone to abuse by the authorities with formidable technologies at their disposal*" [§73].

81. Similarly, in *Zakharov*, the Court held that the authorisation mechanism for the surveillance regime "*must clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered*" [§264] and that it "*must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures*" [§260].

82. As the Court's careful judgments reflect, not everything that is useful to a secret intelligence service is permissible in a democratic society. Just because the state can do something, and it is useful in combating crime or other threats, doesn't mean that it should. As the UK Independent Reviewer (Lord Anderson QC) put it:

> "The capabilities of the state are subject to technical or cost-based limits. But if the acceptable use of vast state powers is to be guaranteed, it cannot simply be by reference to the probity of its servants, the ingenuity of its enemies or current technical limitations on what it can do. Firm limits must also be written into law: not merely safeguards, but red lines that may not be crossed… Some might find comfort in a world in which our every interaction and movement could be recorded, viewed in real-time and indefinitely retained for possible future use by the authorities. Crime-fighting, security, safety or public health justifications are never hard to find… The impact of such powers on the innocent could be mitigated by the usual apparatus of safeguards, regulators and Codes of Practice. But a country constructed on such a basis would surely be intolerable to many of its inhabitants. A state that enjoyed all of those powers would be truly totalitarian, even if the authorities had the best interests of its people at heart. There would be practical risks: not least, maintaining the security of such vast quantities of data. But… the crucial objection is of principle" [AQoT §13.18-13.21 **CB2/48**]

83. As noted in paragraph 13 above, the UK has elected to "*claim ... a pioneer role in the development of new technologies*". As such "*it bears special responsibility for striking the right balance*" [*S & Marper* §112]. It is not in doubt that having bulk access to communications may be useful to an intelligence analyst. But, as Lord Anderson QC put in his Bulk Powers Review "*the fact that an intrusive power can be successfully used to avert threats and reduce crime does not of course mean that it should automatically be passed into law: that way lies a police state*" **[CB3/50/§9.9]**.

84. In *S & Marper* the UK argued that the retention of DNA samples from people who had not been charged or convicted of a criminal offence was of "*inestimable value*" and produced "*enormous*" benefits in the fight against crime and terrorism [§92]. It gave specific examples of crimes that could not have been solved without DNA records from persons who had not been charged or convicted. The Grand Chamber nonetheless held that the retention of such profiles was a "*disproportionate interference*" with those individuals' private lives [§125].

85. Similarly, in *MK v France*, no 19522/09, 18 April 2013, the Court rejected the justification given for the French national fingerprint database by the first instance court, that "*retaining the fingerprints was in the interests of the investigating authorities, as it provided them with a database comprising as full a set of references as possible*" [§14]. It warned that the logic of France's arguments "*would in practice be tantamount to justifying the storage of information on the whole population of France, which would most definitely be excessive and irrelevant*" [§40].

86. As Brandeis J (dissenting, but subsequently approved in later cases) put it in *Olmstead v United States* (1928) 277 US 438 **[SB/9]**, a telephone tapping case:

> "… it is also immaterial that the 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. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding."

87. For example, assume a hypothetical law requiring individuals to report a list of each of the books, newspapers and other publications they read, so that the data could be automatically analysed for patterns of suspicious behaviour. There would be independent oversight of how the data was used and the usual panoply of arrangements and Codes of Practice. Such a scheme would not be permitted by the Convention, because it treats everyone as under suspicion, would have a chilling effect on freedom of expression and would not permit people to privately learn and read without fear or embarrassment.

88. A bulk surveillance regime is yet worse: it involves the collection of far more intimate and detailed information than what we read. Bulk interception of data produced by modern devices produces a "*digital record of nearly every aspect of* [our] *lives*": *Riley v California*

573 US _ (2014) at pp.19-20 per Roberts CJ **[CB3/52]**. The types of data stored on modern devices, as distinct from physical records, are "*qualitatively different*":

> "An Internet search and browsing history, for example … could reveal an individual's private interests or concerns — perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building … a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."

89. The UK argues that bulk interception is proportionate because of the automatic processing techniques used. That is incorrect. As explained above, automatic processing expands the state's ability to undertake covert surveillance. It does not minimise it. As the CJEU explained in the Judgment of 8 April 2014, *Digital Rights Ireland*, C-293/12, ECLI:EU:C:2014:238 §55, "*the need for … safeguards is all the greater where … personal data are subjected to automatic processing*" **[CB3/54]**. It is the modern capability to store, search and automatically analyse data, and to match across databases, that makes bulk techniques particularly intrusive. It is because of the availability of automatic processing that modern bulk surveillance raises particularly severe privacy concerns.

90. As the Independent Reviewer put it, "*no means of communication is immune [from surveillance] … [B]ecause [prior to bulk interception] such techniques were haphazard, risky and resource-intensive, they have generally been used sparingly, and on a targeted basis. Bulk collection of electronic messages, as the Snowden Documents brought home, can be achieved with far less effort and so brings the potential (if not properly regulated) for spying on a truly industrial scale*" [AQoT §2.31 **CB2/48**].

91. The First Section failed to consider whether bulk surveillance was strictly necessary by reference to the criteria in *Szabó* (see paragraph 80 above) and erred in finding that the regime was proportionate on the basis that it saw "*no reason to disagree*" with the analysis of the Independent Reviewer that "*bulk interception is a valuable means to achieve the legitimate aims pursued, particularly given the current threat level from both global terrorism and serious crime*" [§386].

92. The First Section also wrongly held that the operation of a bulk interception regime was within a state's margin of appreciation at [§314]. It addressed the matter in a single paragraph by reference to the current threats states face and the previous case law, which it recognised to be "*now more than ten years old*". The Applicants invite the Grand Chamber itself to reconsider this question in light of modern technological developments and the particularly severe risks they create for people's rights, and to find that the regime is neither strictly necessary nor proportionate.

(4) In any event, the RIPA s.8(4) regime is not in accordance with law

93. Alternatively, if the Court considers the RIPA s.8(4) regime not to be disproportionate, it must in any event be accessible and subject to strict safeguards to "*in accordance with the law*" under Article 8(2), in accordance with the Court's case law. The RIPA scheme falls short. In summary:

a) So-called "*below the waterline*" arrangements are not accessible and should play no part in the Court's consideration of the Article 8 of the regime;

b) The RIPA s.8(4) regime fails to meet even the requirements of foreseeability, as explained by this Court in *Weber* and most recently by the Grand Chamber in *Zakharov*; and

c) The Court should enhance the *Zakharov*/*Weber* minimum safeguards by requiring prior independent judicial authorisation, objective evidence of reasonable suspicion in relation to the person about whom information is sought, and subsequent notification of the surveillance subject.[14]

(i) The unnecessary complexity and obscurity of the RIPA s.8(4) regime

94. The RIPA scheme is extraordinarily complex and obscure. UK law is neither comprehensible nor accessible. The true nature and scope of what was occurring was not clear, even to an informed reader, until Mr Snowden's disclosures.

---

[14] See App Cons Obs 29 Sep 2017 §§120-129 **[SB/2]**.

95. The difficulty and complexity of the RIPA scheme is reflected in the length of the judgment of the First Section and the UK's observations before the First Section (which each run to approximately 200 pages). The point was made graphically by Mr Tom Watson MP (currently Deputy Leader of the Opposition in the UK and the Claimant in *Tele 2/ Watson* in the CJEU) on 31 October 2013:

> "The Minister … may point to … section 16 of RIPA to suggest that the TEMPORA programme is legal. Interpreting that section requires the unravelling of a triple-nested inversion of meanings across six cross-referenced subsections linked to a dozen other cross-linked definitions, which are all dependent on a highly ambiguous "*notwithstanding*" [in section 16(3)]. The section is probably the single most confusing and complex drafting ever put on the statute book, and I have heard that a former GCHQ director said it was drafted in that way intentionally; it is what a computer programme[r] would call "*spaghetti code*." There is not a snowball's chance on a hot day in Strasbourg that the section would pass the tests of foreseeability and quality of law."

96. More politely, but equally firmly, the same point has been made by all of the independent reviewers of RIPA:

a) The Independent Reviewer described RIPA as "*incomprehensible to all but a tiny band of initiates*" and "*impenetrable*" to the point of "*corrod*[ing] *democracy itself, because neither the public to whom they apply, nor even the legislators who debate and amend them, fully understand what they mean*" **[CB2/48]**.[15] Such a situation falls short of the minimum requirement in the Court's caselaw that law be accessible.

b) The ISC described the RIPA arrangements as "*unnecessarily complicated*", "*difficult to understand*", and "*unnecessarily secretive*".[16]

c) The RUSI Panel (including the former heads of each of the UK's intelligence agencies) described RIPA as "*unclear*" and failing to "*serve either the government or members of the public satisfactorily*."[17]

---

[15] *A Question of Trust: Report of the Investigatory Powers Review*, June 2015 ("**AQoT**") **[CB2/48]**, §13.31, p.252.

[16] In its 2015 Report entitled, "*Privacy and Security: A modern and transparent legal framework*" ("**ISC Report**") **[CB2/47]**, §§xvi, 275.

[17] RUSI Report **[CB2/49]** pp.xi-xii.

97. This is not a novel problem in UK surveillance legislation. A series of secret surveillance regimes introduced by the UK Government have been found to be incompatible with the quality of law requirements under Article 8: see, for example, *Malone* (paragraph 27 above) and *Liberty* (at paragraph 29 above).

(ii) Accessibility – Reliance by the UK on "below the waterline" (ie secret) "arrangements"

98. Many of the key "*arrangements*" governing the use of intercepted data remain secret and unavailable to the public. If and to the extent that the UK Government relies upon internal "*arrangements … below the waterline*" [c.f. UK Obs 29 Sep 2017 §44 **SB/3**], it is wrong to suggest they may be taken into account in assessing the foreseeability of the law. They are analogous to the undisclosed "*arrangements*" criticised by the Court in *Liberty* [§77]:

> "The fact that the Commissioner in his annual reports concluded that the Secretary of State's 'arrangements' had been complied with, while an important safeguard against abuse of power, did not contribute towards the accessibility and clarity of the scheme, since he was not able to reveal what the 'arrangements' were. […] the procedures to be followed for examining, using and storing intercepted material, *inter alia*, should be set out in a form which is open to public scrutiny and knowledge." [emphasis added]

99. While this Court has previously given weight to Codes of Practice or sufficiently established administrative practices which are accessible (*Silver v United Kingdom*, no 5947/72, 25 March 1983, §§88-89; *Kennedy v United Kingdom*, no 26839/05, 10 May 2010, §156), in the context of a bulk interception regime leading to "*indiscriminate capturing of vast amounts of communications*" (*Kennedy* at §160), the absence of public rules adversely affects the quality of the law. A public statutory Code of Practice is entirely different from secret "*arrangements*" such as those on which the UK Government relies. As the Court noted in *Liberty* [§§40 and 60], a Code is a public document, and it must be subject to consultation and approved by both Houses of the UK Parliament (s.71(9) RIPA).

100. In contrast, arrangements "*below the waterline*" — a euphemism the Grand Chamber is invited to deprecate — are (i) established by the intelligence agencies; (ii) not published, accessible or approved by Parliament (ie entirely secret); (iii) a matter of internal policy and thus subject to change at the executive's will; and (iv) not in practice enforceable (because they are secret and may be departed from if UKIS think there is cogent reason to do so).

101. The inadequacy of such secret arrangements is made clear by the revision of the 2016

Interception Code **[CB2/33]**. The publication of the revised Code confirms that there was no good reason for keeping information now in the Code secret. As in *Liberty*, the publication of the revised Code showed that the previous secrecy was unnecessary [§68]. In any event, the revised Code is insufficient to address the flaws in the UK regime, given that it applies the inadequate RIPA regime to intelligence sharing.

102. "*Below the waterline*" arrangements should play no part in the consideration of the Convention compliance of the RIPA s.8(4) regime.

(iii) Foreseeability

103. The Applicants set out below why the RIPA regime falls short of the minimum safeguards the Court has developed and explain the enhanced safeguards that should apply.

104. In considering the particular defects, it is important to bear in mind (i) the broad permitted purposes of interception in RIPA s.5(3); and (ii) the vast scope of communications subject to interception.

<u>*Foreseeability – Meaningless distinction between internal versus external communications*</u>

105. RIPA provides that a s.8(4) warrant must be targeted at "*external*" not "*internal*" communications. However, due to technological changes in how data is transmitted, the distinction in RIPA between the legal regimes governing "*internal*" and "*external*" communications has become meaningless in practice, with most communications likely to be swept up in the "*external*" category to which the s.8(4) regime applies. This is for two reasons:

a) First, it is now routine for "*internal*" communications, such as an email between people who might be in the same office building, to be routed through servers on the other side of the world in the course of delivery. It is not possible to distinguish between "*internal*" and "*external*" communications at the point of interception. So "*internal*" communications have effectively become subject to the bulk interception powers as an *"incidental"* product of bulk surveillance of *"external"* communications: see RIPA s.5(6).

b) Secondly, the UK Government has adopted a very broad interpretation of "*external*". Whenever a person in the UK communicates with an online service hosted abroad, this will be classified as an "*external*" communication [eg Farr 1/§§126-141 **CB1/9**].

106. For example, assume a group of friends in London wish to arrange to meet:

a) In 1990, they would have phoned or written to each other and perhaps left messages on answerphones to arrange a time and meeting agenda. It is unlikely that such communications ever left the British Islands (or even the London area). They would not have been swept up under a bulk warrant because the messages would never have been transmitted over external communications links.

b) In 2000 (when RIPA was enacted), they would probably have made arrangements by mobile phone call or text message. Such calls or texts would again have been routed over local networks and never subjected to any bulk surveillance.

c) By 2019, the friends may send a group message using a social media platform such as Facebook or on a messaging service such as WhatsApp from their smartphones. These communications will leave the UK during transmission via a foreign server, and so be treated as "external" and subject to bulk interception, filtering and storage.

107. The world has changed dramatically from the position considered by the Court in *Liberty*. *Liberty* focussed on a communications link carrying telephone calls between the UK and the Republic of Ireland. It was unlikely that many "*internal*" communications would be incidentally collected. Telephone calls between two Londoners would be unlikely to be routed via Dublin. But today Facebook messages between two Londoners will be routed via California. The exclusion of "*internal*" communications is no longer a meaningful safeguard.

108. Notably, in other countries, legislative schemes provide more meaningful protection for internal communications. For example, in Sweden, all internal communications must be filtered out and if any are discovered, the internal communications must be destroyed immediately (see paragraph 124 below).

109. Further, during the course of the IPT proceedings, the UK Government said that communications transmitted via "*a web-based platform*", for example, "*a Google search, a Facebook post, or a 'tweet' on Twitter*", that rely on servers outside the UK, including

Facebook, Google or YouTube, are "*external*" not "*internal*" communications [Farr 1 §§136-137, 139 **CB1/9**]. By classifying a much wider range of communications as "*external*" it becomes possible to justify the interception of a much wider range of communications links and to examine a much wider range of communications, without the additional protections in UK legislation for "*internal*" communications. This weakens yet further a "safeguard" that was already meaningless in light of technological change.

110. This expansive interpretation was not made public until the IPT hearings. It remains unclear what other online services fall within the Government's definition of an "*external*" communication. The term "*platform*" does not appear in RIPA or the Codes of Practice.

111. The ISC concluded that "*the current system of 'internal' and 'external' communications is confusing and lacks transparency. The Government must publish an explanation of which internet communications fall under which category, and ensure that this includes a clear and comprehensive list of communications*" [ISC Report Annex A §O, p.113 **CB2/47**]. The Government has not done so.

112. The Chamber held at §§336-337 that the regime was sufficiently certain because "*at least at the macro level of selecting the bearers for interception – only external communications can be targeted*". But the First Section did not consider the breadth and uncertainty of this concept on the UK's (previously secret) interpretation, or how this previously important "safeguard" has lost its effectiveness with the development of technology.

Foreseeability – Adequacy of protection for communications data

113. The First Section rightly held that "*it is a matter of some concern that the intelligence services can search and examine 'related communications data' apparently without restriction*" [§355]. This can include location data, web browsing information, email headers, and logs of files sent and received.

114. The First Section noted that it "*is not persuaded that the acquisition of related communications data is necessarily less intrusive than the acquisition of content…. In bulk the degree of intrusion is magnified, since the patterns that will emerge could be capable of painting 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 interacted with" [§356]. Therefore, the UK Government had not "*struck a fair balance… by exempting* [communications data] *in its entirety from the safeguards applicable to the searching and examining of content*" [§357].

115. The First Section was correct, for the reasons it gave. The important safeguards for persons in the UK do not apply to communications data. As the ISC explained:

> "… while the content of UK-to-UK communications incidentally collected by GCHQ attracts special protection and additional safeguards under RIPA, these do not apply to the [communications data] related to those communications. This means that UK-to-UK [related communications data] will be in the pool of Communications Data that GCHQ collect, and may be returned as a result of searches against that pool" [ISC Report §146 **CB2/47**].

116. In addition, for people outside the British Islands, the certification requirement in RIPA s.16 does not apply in any case. Accordingly, communications data can be used and stored by the UKIS in bulk and analysed for any national security, economic well-being or serious crime purpose, without being limited by the narrower purposes specified in any accompanying s.8(4) certificate. Given that the UK relies on the certificate as a limiting factor (albeit overstating the weak limitation it imposes — see paragraph 121 below), it ought at the least to apply to any use of communications data.

Foreseeability – Absence of oversight of selectors and selection of bearers

117. By contrast to *Weber* (Germany prior to 2006) and *Rättvisa* (Sweden), the UK regime does not require selectors to be specified in the warrant or certificate or checked by oversight mechanisms. Nor is there any oversight of the selection of bearers intercepted. See criticisms of the lack of oversight of the "*selectors*" used by GCHQ: ISC Report §§123-125 [**CB2/47**]. There is "*no pre-authorisation or authentication process to select material*": IOCC 2014 Annual Report §6.38 **[CB2/36]**.

118. The First Section (rightly) found the absence of a proper system of oversight of bearers and selectors to be unlawful, for the reasons it gave [§§338, 340, 345-347, 387-388].

119. The absence of effective oversight or approval of the filtering, storage and analysis of intercepted material is reflected in the Third IPT Judgment in June 2015, which found that communications of one of the Applicants – the South African Legal Resources Centre – had not only initially been intercepted, but also extracted, filtered and stored, as the relevant

selection procedure was not followed [§15] [**CB1/16**]. This defect was not discovered by the oversight arrangements and only came to light as a result of litigation in the UK by the Applicants in the present case.

120. A system that requires disclosure of classified material by a whistle-blower in order to identify unlawful conduct does not contain adequate safeguards. At the very least, informed independent judicial authorisation of the bearers intercepted and search terms and selectors used would be necessary to ensure the RIPA system is sufficiently certain.

Foreseeability – Broad scope of s.16 certificate permitted by RIPA

121. The s.16 certificate allegedly constrains intercept data use. But the ISC found it to be "*in very general terms … so generic, it begs the question … whether it need be secret*" [ISC Report §101 **CB2/47**].

122. Some categories in the certificate are not a proper basis for mass interception: they do not correspond to a pressing social need, eg "*strategic environmental issues*" [ISC Report §102]. The ISC said that this category was "*unnecessarily ambiguous and could be misinterpreted*" [ISC Report §103]. The UK regime does not specify, in law and in detail, the purposes for which material may be examined, to prevent arbitrary use of surveillance or use for purposes that could never justify the severe level of intrusion bulk surveillance causes.

Foreseeability – Comparison with Weber and Rättvisa and the subsequent UK regime

123. The UK scheme in RIPA does not compare favourably even with the other bulk surveillance arrangements previously considered by the Court. These regimes demonstrate that alleged difficulties the UK asserts to exist are without foundation.

124. In Sweden, as considered in *Rättvisa*, there is a requirement not to intercept (and to immediately dispose of) internal communications, there is prior judicial authorisation of warrants and search terms or categories of search terms, a procedure for notice, and the involvement of a privacy protection advocate in the judicial authorisation procedure: see paragraph 32 above.

125. In Germany before 2006, as considered in *Weber*:

a) The independent G10 Commission (including a legally qualified President) had to consent in advance to proposed monitoring, on a monthly basis. The Commission had the power to order that individuals subject to monitoring be notified [§25].

b) The exact purposes for which interception was permitted were specified in the G10 Act and thus public [§27]. By contrast, the content of certificates under s.8(4) are always secret.

c) Only wireless communications could be intercepted, which comprised only ten percent of communications (although fixed line communications could be intercepted for the sole purpose of preventing a potential armed attack on Germany).

d) Searches were conducted using approved *"catchwords"*. Each catchword had to be suitable for investigating the dangers in the monitoring order and catchwords had to be listed in the order and thus subject to oversight and supervision [§32].

126. Under the UK Investigatory Powers Act 2016 ("**IPA**"), prior judicial approval is required for bulk interception warrants (but only applying a judicial review standard to the Secretary of State's decision to issue the warrant and without any judicial supervision of selectors or selection for examination), the purposes have been narrowed, the arrangements for oversight have been strengthened and there is provision for notice to be given to victims of serious interception errors (although "*mere*" breach of the Convention is not sufficient). The Applicants do not accept that the IPA bulk interception regime complies with the Convention. Its lawfulness is currently subject to domestic litigation brought by one of the Applicants (Liberty). But just as in *Liberty* §68, these developments show that it was always practicable to have improved safeguards.

127. The First Section relied on the IPA to excuse the absence of judicial authorisation in the RIPA regime [§§380-381]. This is wrong. New (and then uncommenced) legislation cannot justify the previous application of deficient safeguards. The First Section should not have relied on a "*new procedure* [that] *has not yet been implemented*" as a remedy for a complaint about a past breach of the Convention [§380].

Foreseeability – Updating and enhancing Weber

128. The application in *Weber* was filed in 2000 and declared inadmissible (by a majority) in 2006. Since then, there have been "*seismic shifts in digital technology*" (*Carpenter v United States* 585 US _ (2018) at p.15, Roberts CJ [**SB/10**]).

129. It is therefore appropriate to review the principles to ensure that Convention rights remain effective. The same process is ongoing in apex courts across the world. For example, the CJEU has identified extensive minimum safeguards for communications data in *Digital Rights Ireland* [**CB3/54**] and *Tele2/Watson* [**CB3/57**]. In *Carpenter* at p.17, the US Supreme Court (per Roberts CJ) extended the protections of the Fourth Amendment to ensure that the prohibition on unreasonable searches and seizures remains effective in the modern world:

> "… cell phones and the services they provide are '*such a pervasive and insistent part of daily life*' that carrying one is indispensable to participation in modern society ... [A] cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates [communications data], including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data … a comprehensive dossier of his physical movements." [**SB/10**]

130. When the Court identified, in its *Weber* judgment, the minimum safeguards necessary in a regime for the surveillance of communications which is compliant with the Convention, many forms of modern communication were not in existence. Changes in technology, and the development of bulk surveillance, storage and processing capability, mean that the safeguards require updating.

131. **Prior independent judicial authorisation:** Under RIPA, there is no requirement for the prior independent judicial authorisation of s.8(4) warrants, still less of the targets and selectors applied to the bulk data collected. Warrants are issued, in secret, by the Secretary of State, a politician and member of the executive.

132. The Independent Reviewer noted that "*the Secretary of State is rarely if ever held politically accountable for the issue of warrants: contributing factors are RIPA s. 19* [prohibiting disclosure of the fact a warrant has been issued or its content], *NCND* [the 'Neither Confirm nor Deny' policy] *and the fact that intercepted material is not admissible in court*" with the

effect that the lawfulness of the interception cannot be challenged by the defence in any criminal proceedings [AQoT §14.56 **CB2/48**].

133. Even more so in light of the "*rolling*" renewal of the s.8(4) warrants and the very generally worded certificates that accompany them, *ex ante* judicial control of legality, strict necessity and proportionality of warrants, selectors and examination is needed. The UK system of *ex post* oversight is insufficient and in any case has not proven effective, as is best illustrated by the fact that the Commissioners did not identify any of the legal errors found by the IPT or the First Section. The IPT did not identify any problems until after the Snowden revelations and the lodging of complaints about the UK regime.

134. In the IPA, the UK has introduced prior judicial review of the Secretary of State's decision to issue warrants, but this is inadequate as it applies only a judicial review standard and does not require oversight of selectors or examination. Many other states operate prior judicial authorisation procedures, without apparent difficulty. In *Rättvisa*, the warrant had to be approved by a specialist court, and the selectors also had to be identified in the warrant. In *Weber,* a cross-party and independent commission approved surveillance and the selectors. The Court repeated the principles in *Szabó*: "*in this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exceptions, warranting close scrutiny … supervision by a politically responsible member of the executive, such as the Minister for Justice, does not provide the necessary guarantees"* [§77]. The same approach was taken by the Grand Chamber of the CJEU in *Digital Rights Ireland* [§62] and *Tele2/Watson* [§120].

135. The First Section concluded that prior judicial authorisation was "*highly desirable*" but not a "*necessary requirement*" under Article 8 "*in view* [of] *the pre-authorisation scrutiny … extensive post authorisation scrutiny provided by the (independent) Commissioner's office and the IPT and the imminent changes to the impugned regime*" [§§318, 381]. The Grand Chamber is invited to depart from this finding:

    a) Updating and enhancing the minimum safeguards is properly a matter for the Grand Chamber. It is understandable that the First Section limited itself to applying the Court's existing case law.

b) The limited pre-authorisation scrutiny of warrant applications is carried out by the Secretary of State and officials acting on his behalf. They are not independent of the UK Government and the UKIS who will carry out the warrants. This fails to meet the standard in *Zakharov* §258 of authorisation by a non-judicial authority "*provided that that authority is sufficiently independent from the executive*".

c) The First Section rightly found the Commissioner's post-authorisation scrutiny to be inadequate. It held at §347 that there was an "*absence of robust independent oversight of the selectors and search criteria*". Such inadequate oversight cannot remedy the absence of prior judicial authorisation.

d) The IPT does not provide an adequate remedy for the absence of prior judicial authorisation. It may only consider a case referred to it. The Commissioner lacks power to refer a case to the IPT and is not permitted to notify a victim of excessive or unlawful interception. The Independent Reviewer found this "*hard to understand*" [AQoT §14.104 **CB2/48**]. The only means by which the IPT could remedy problems in the initial grant of warrants would be for large numbers of individuals to make speculative claims to the IPT, asserting secret, unknown and undefined problems with the warrant process. The IPT would reject such claims: *Human Rights Watch v Secretary of State for the Foreign and Commonwealth Office* [2016] UKIPTrib15_165-CH **[CB3/56]** §§47-48. This indicates that the First Section was wrong to hold at §379 that "*any person who believes that he or she has been subject to secret surveillance may make an application to*" the IPT. The IPT has now held that there must be some basis for that belief.

e) As recognised by Judges Koskelo and Turković in the First Section, the fact that prior judicial control is not in itself a "*sufficient safeguard*" does not support the conclusion that it should not be considered necessary [§25].

f) The introduction of the IPA does not remedy the defects in the RIPA regime, contrary to the Chamber's reasoning at §§380-381, as explained at paragraphs 126-127 above.

g) The UK has begun to introduce independent approval to consider and authorise state requests for communications data, in response to *Tele2/Watson*. This power has been delegated to a new independent body, the Office for Communications Data

Authorisation, operating under the Investigatory Powers Commissioner, a senior judge. The Applicants do not consider these measures sufficient, but their introduction illustrates the minimum safeguards may practicably be enhanced and updated.

136. **Objective evidence of reasonable suspicion in relation to the persons about whom data is sought:** In *Szabó* the Court noted the requirement of "*a sufficient factual basis for the application of secret intelligence gathering measures … on the basis of an individual suspicion regarding the target person*" as critical for "*the authorising authority to perform an appropriate proportionality test*" [§71]. Similarly, in *Zakharov*, the Grand Chamber held that the authorisation procedure "*must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security*" [§260].

137. The First Section held that "*bulk interception is by definition untargeted, and to require 'reasonable suspicion' would render the operation of such a scheme impossible*" [§317]. Even assuming a bulk interception regime could in principle be compatible with the Convention, this nonetheless incorrectly fails to differentiate between initial interception and subsequent processing or examination of intercept material. For example, selectors could be applied to bulk intercept data at the point of extraction from cables so that masses of irrelevant data of no legitimate intelligence interest are copied but then immediately deleted. Proper grounds will exist for using such a selector only where there are reasonable grounds for suspicion of the person about whom information is sought (see *Zakharov* §260). This test is well understood in the context of search warrants and arrest.

138. It may, in certain circumstances, be technically necessary to access a communications bearer in order to intercept, extract and examine the communications of a legitimate target (approved by an independent judicial authority on the basis of objective evidence of reasonable suspicion). However, the UK Government should then immediately discard the unwanted communications and communications data. This is possible: for example, it occurs, but only for some information, under the Swedish regime considered in *Rättvisa* [§25].

139. **Subsequent notification of the surveillance subject:** Both the Court (in *Szabó* at §86 and *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*, no 62540/00, 28 June 2007, §91) and the CJEU (in *Watson* at §121) recognise the importance of this safeguard, to enable those affected by bulk interception to be aware of the interference with their rights and to seek remedies against any abuse of the relevant surveillance powers.

140. The First Section held that "'*subsequent notification' assumes the existence of clearly defined surveillance targets, which is simply not the case in a bulk interception regime*" [§317]. But again this fails to distinguish between the point of interception and the subsequent storage, processing and use of information. If notification would not cause substantial harm to the public interest, it should be given. Other bulk interception schemes (eg in *Weber* and *Rättvisa*, see paragraphs 32.d), 124 and 125.a) above) do make provision for notification. Further, even the IPA provides for a limited form of notification by the Commissioner in cases of "*serious error*" (see IPA s.231(1)). Further safeguards than those accorded under RIPA are entirely feasible.

(5) Safeguards for journalists' sources and journalistic material under Article 10

141. The gathering of information is an "*essential preparatory step in journalism and an inherent, protected part of press freedom*": *Satakunnan Markkinaporssi Oy v Finland*, no 931/13, 27 June 2017, §128. In this context, the Court has repeatedly emphasised that the protection of journalistic sources and journalistic material is a fundamental guarantee afforded by the right to freedom of expression (see the passage from *Weber* cited at paragraph 71 above). The same principles apply in respect of human rights NGOs engaged in the gathering of information in the public interest (see paragraph 72 above).

142. The concept of journalistic source has been given a very broad definition by the Court (something not reflected in the 2016 Interception Code of Practice). In *Telegraaf Media Nederland Landelijke Media BV v Netherlands*, no 39315/06, 22 November 2012, the Court held that "[a] *journalistic source is any person who provides information to a journalist"* and that *"information identifying a source include*[s]*, as far as they are likely to lead to the identification of a source, both the factual circumstances of acquiring information from a source by a journalist and the unpublished content of the information provided by a source to a journalist*" [§86].

143. The Court has developed well-established relevant safeguards, set out below. In a bulk interception regime, these are particularly relevant at the point at which the UKIS apply selectors and filters, and examine either content or relevant communications data collected. Such selectors can be used to easily identify a journalistic source.

144. The Court "*has always subjected the safeguards for respect of freedom of expression in cases under Article 10 of the Convention to special scrutiny*" and has held that an interference capable of identifying a journalistic source "*cannot be compatible with Article 10 … unless it is justified by an overriding requirement in the public interest*" (*Sanoma* §51 (emphasis added); *Goodwin v United Kingdom*, no 17488/90, 27 March 1996, §39). This requirement is relevant both in the context of evaluating whether a particular measure is prescribed by law (as there must be sufficient safeguards to ensure *ex ante* that surveillance measures imposed are justified by an overriding requirement in the public interest – *Sanoma* §90) and in assessing whether a particular interference is necessary in a democratic society (*Becker v Norway*, no 21272/12, 5 October 2017, §66).

145. Article 10 protection extends not only to protection of journalistic sources but also to journalistic material including "*research material*" (see *Sanoma* §§65-66; *Nordisk Film & TV A/S v Denmark (Admissibility)*, no 40485/02, 8 December 2005). *Sanoma* was itself concerned with access to journalistic material, not measures to identify a journalistic source.

146. The Court has repeatedly held that, given the fundamental importance of press freedom, any interference with journalistic information and, in particular, the right to maintain the confidentiality of sources, "*must be attended with legal procedural safeguards commensurate with the importance of the principle at stake*" (*Sanoma* §88). Accordingly, Article 10 imposes specific and exacting requirements where a measure is capable of identifying journalistic sources and/or revealing journalistic material over and above those that apply under Article 8 and Article 10 generally.

147. Consistent with the Court's case law, the First Section was correct to state that "*the interference* [with Article 10 rights] *will be greater should* [a journalist's] *communications be selected for examination* [following the interception of material under a s 8(4) warrant] *and* [such selection] *will only be 'justified by an overriding requirement in the public interest' if accompanied by sufficient safeguards relating both to the circumstances in which*

they may be selected intentionally for examination, and to the protection of confidentiality where they have been selected, either intentionally or otherwise, for examination" [§492]. The First Section also made clear that special safeguards apply at the least where the material of a journalist is sought or where there may be collateral intrusion [§499]. The Grand Chamber is invited to endorse this approach in relation to journalists and, in addition, other "public watchdog" organisations including human rights NGOs. It is further invited to endorse the First Section's decision that this applies equally to communications data [§499].

148. In *Sanoma*, the Grand Chamber set out minimum safeguards which must be present to ensure that measures whose application is capable of identifying journalistic sources and/or revealing journalistic material are in accordance with the law (the "***Sanoma* Safeguards**"):

a) First, "*is the guarantee of review by a judge or other independent and impartial decision-making body*", which is "*impartial*" and "*separate from the executive and other interested parties*" [§§90, 92]. The authorising body must not be an official or institution "*defending interests potentially incompatible with journalistic source protection*" [§93].

b) Secondly, the review must be *ex ante*, ie, before the relevant measure is implemented [§90]. This is because "*the exercise of any independent review that only takes place subsequently to the handing over of material capable of revealing such sources would undermine the very essence of the right to confidentiality*" [§91]; and see *Telegraaf Media* at §99-102, applying *Sanoma*. The Court's caselaw on the need for *ex ante* independent authorisation is clear.

c) Thirdly, the independent body must be "*invested 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*" [§90] and it must "*be in a position to carry out this weighing 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 properly assessed*" [§92].

d) Fourthly, "*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*" [§92]. The independent body must have power 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 … specifically named in the withheld material*" [§92].

149. The *Sanoma* Safeguards are required where the application of a measure "*could*" lead to identification of a source or "*is capable*" of doing so, not just where the intention is to do so: *Sanoma* §88. As such, the *Sanoma* Safeguards relate to both intentional and incidental intrusions into journalistic materials and sources (see First Section §492).

150. As journalistic sources and material may be identified not only from content but also from communications data, such safeguards apply equally to content and related communications data obtained under the s.8(4) regime. The Grand Chamber is invited expressly so to hold.

151. The importance of the overriding public interest requirement and the *Sanoma* Safeguards is even higher at the stage at which intercept material – content and/or related communications data – is processed or searched (using selectors or otherwise) and in particular where it is selected for examination and analysis with the aim of identifying journalistic material. If the stringent safeguards are required where a targeted surveillance measure (as is the case: see *Telegraaf Media* §97) is capable of identifying journalistic sources or revealing journalistic material, they must apply also to the filtering or other processing and selection for examination of bulk intercept material or communications data.

152. The First Section was therefore right to conclude that the s.8(4) regime breaches Article 10:

> "In the Article 10 context, it is of particular concern that there are no requirements – at least, no "above the waterline" requirements – either circumscribing the intelligence services' power to search for confidential journalistic or other material (for example, by using a journalist's email address as a selector), or requiring analysts, in selecting material for examination, to give any particular consideration to whether such material is or may be involved. Consequently, it would appear that analysts could search and examine without restriction both the content and the related communications data of these intercepted communications" [§493, emphasis added].

153. The overriding public interest requirement (First Section §495) and the other *Sanoma* Safeguards are wholly absent from the s.8(4) regime. No such protections exist in respect of the examination of the content of communications and related communication data gathered

under s.8(4) warrants in circumstances in which the exploitation of such material is capable of identifying journalistic sources or revealing confidential journalistic material.

154. Crucially, the s.8(4) regime does not include any *ex ante* independent, let alone judicial, authorisation at any stage, even where activities authorised are for the purpose of identifying journalistic sources. The absence of this fundamental safeguard is alone sufficient to mean that the regime is not in accordance with the law under Article 10 on existing authorities.

155. To the extent that the 2016 Interception Code **[CB2/33]** contains any relevant (albeit manifestly insufficient) safeguards, it is irrelevant: the First Section was correct to identify these as applying only to targeted interception warrants under RIPA s.8(1) [§493]. They have no application at all to the RIPA s.8(4) regime.

156. In any event, the 2016 Interception Code is flawed and provides no (sufficient) safeguards for the purposes of Article 10 for the following reasons:

    a) It purports to define "*confidential journalistic material*" as "*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*" [§4.3]. To the extent that this provision is intended to define or encompass "journalistic sources" or "information identifying a source", it is inconsistent with the Court's definition of these concepts and excessively narrow (see *Telegraaf Media* at §86, quoted above). Additionally, it omits provision for NGO watchdogs. Further, requiring an undertaking to hold it in confidence incorrectly limits the protection. Journalistic material is often not held on this basis. See, for example, the videos at issue in *Sanoma* at §64.

    b) Even where there is an intention actively to "*acquire*" confidential journalistic material, the 2016 Interception Code goes no further than requiring that "*reasons*" be "*documented*" and stating that the "*specific necessity and proportionality of doing so should be carefully considered*" [§4.28, read with §4.32]. This is inadequate. There is no requirement for an independent *ex ante* decision. The overriding public interest requirement is absent. And there are no "*clear criteria*" governing such decisions (as *Sanoma* at §92 requires), whether by reference to overriding public interest (and circumstances where this might be satisfied), less intrusive alternatives or otherwise.

c) The 2016 Interception Code provides that where selection of confidential journalistic material for examination 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*" [§4.28, read with §4.32]. As set out, the protection Article 10 affords to journalistic sources and information does not depend on any intention to access to such material. If an agency is aware that the use of a measure in particular circumstances could/is capable of leading to identification of a journalistic source or reveal journalistic material, this triggers the full protections required by Article 10, as identified above.

157. The 2016 Interception Code contains no recognition of the fact that the use of related communications data obtained under s.8(4) warrants is capable of identifying journalistic sources and confidential journalistic material (and may be used for such purposes). Often, this data will be all that is required to identify a journalistic source. However, the 2016 Interception Code includes no safeguards at all to protect journalistic sources and journalistic material in respect of related communications data obtained under s.8(4) warrants.

158. In addition, the RIPA s.8(4) regime contains none of the *Sanoma* Safeguards at all for related communications data, that is, communications data attached to intercepted content. The First Section correctly found that "*the intelligence services can search and examine 'related communications data' apparently without restriction*" [§355].

159. That is a particularly striking omission in circumstances where the communications data acquisition regime under Chapter II of RIPA contained some, albeit insufficient, safeguards. The First Section held, correctly, that the Chapter II regime was not in accordance with the law under Article 10 [§§496-499]. This was primarily because relevant safeguards contained in the 2015 Acquisition Code [**CB2/32**] (including for an overriding requirement in the public interest and for independent authorisation via production orders under the Police and Criminal Evidence Act 1984) applied only where communications data was sought to identify a journalistic source. These safeguards did not apply "*in every case where there is a request for the communications data of a journalist, or where such collateral intrusion is likely*" [§499]. (In addition, the First Section rightly held that the Chapter II regime was not

in accordance with EU law.) This shows that the safeguards the Court has developed could be, but were not, applied to relevant communications data.

160. Finally, the relevant safeguards in RIPA s.16 do not provide any additional protection for journalists or journalistic materials. They do not apply to the exploitation of content intercepted under a s.8(4) warrant in a way referable to journalists who are not known to be in the British Islands. Further, the protections afforded by Article 10 attach not only to individual journalists but also to media organisations. Section 16 offers no protection to a media organisation based in the UK if material is selected for examination with reference to one of its journalists located overseas. Further, it offers no protection, for example, from examination of material with reference to individuals overseas who may be sources for and/or in communication with journalists or media organisations in the UK. Examining the content of their communications would plainly be capable of identifying the sources of UK-based journalists and/or revealing their confidential journalistic material. Investigating and gathering information for public interest stories often involves journalists working overseas and media organisations/journalists based in the UK working with persons located abroad.

F ***Intelligence sharing***

161. The Five Eyes group conducts global bulk surveillance. The group – including the UK and the US – shares the fruits of bulk interception reciprocally [King 1/§§71-77 **CB1/5**]. This is the first time the Grand Chamber has considered the Convention compliance of any intelligence sharing regime between states, including those outside the Council of Europe.

162. The First Section found that:

a) the existence of the intelligence sharing arrangements in and of itself is an interference with the Applicants' Article 8 and Article 10 rights [§§394-395];

b) the Applicants were potentially at risk of having their communications requested from a foreign intelligence service and/or obtained by the UKIS, so were victims under Article 34 [§§395-396]; and

c) as the material was the product of intercept, "*those requirements which relate to … storage, examination, use, onward dissemination, erasure and destruction*" must also "*be present*" in the intelligence sharing regime [§§423].

163. The First Section nevertheless concluded that there was no Article 8 violation [§§447-448].

164. This decision is logically inconsistent with the First Section's findings that:

    a) The applicable safeguards must ensure that intelligence sharing is not used "*to circumvent stronger domestic surveillance procedures*". Accordingly "*those requirements which relate to its storage, examination, use, onward dissemination, erasure and destruction must be present*" [§423].

    b) The safeguards for direct surveillance were inadequate. The First Section found that the RIPA s.8(4) regime breached Article 8 because:

        i) there was a lack of oversight of the entire selection process, including the selection of bearers for interception, the selection of search criteria for filtering intercepted communications and the selection of material for examination; and

        ii) the safeguards applicable to the selection of related communications data for examination were inadequate [§§387-388].

165. The First Section identified the correct principles. However, it did not then apply them to the defects it had held to exist under the RIPA s.8(4) bulk interception regime: see [§§431-435]. If the safeguards required are the same for interception and intelligence sharing, it necessarily follows that the breaches in relation to interception apply equally to intelligence sharing. The Grand Chamber is invited to adopt the analysis of Judge Koskelo and Judge Turković in their separate opinion that the "*shortcomings … in the context of the section 8(4) regime also attach the intelligence sharing regime*" [§31].

166. The First Section should also have considered "*unsolicited*" intelligence sharing [§§417, 447]. Even if "*rare*" (a matter on which the Applicants cannot comment), it is expressly contemplated by the intelligence sharing regime. It makes no difference to the interference under Articles 8 and 10 whether provision of bulk intercept material is solicited or not.

167. The flaws in the s.8(4) regime identified by the First Section, and the additional flaws identified above in light of the Applicants' invitation to the Court to enhance the safeguards, render the intelligence sharing regime in violation of Articles 8 and 10.

*(1) **Facts***

168. The US NSA's authority to conduct surveillance of foreign communications is governed by the Foreign Intelligence Surveillance Act ("**FISA**") and Executive Order 12333.

169. Section 702 of FISA permits the US Attorney General and Director of National Surveillance to authorise surveillance within the US by targeting non-US persons "*reasonably believed to be located outside*" the US to acquire foreign intelligence information.

170. PRISM and UPSTREAM are US programmes authorised by FISA s 702:

    a) PRISM allows "*intelligence material (such as communications)*" to be obtained from internet service providers. GCHQ has had access to PRISM since July 2010. GCHQ has acknowledged that it acquired information from the US which had been obtained via PRISM [First Section §§16-17, 395].

    b) UPSTREAM is a "*bulk interception scheme similar to the section 8(4) regime*" which allows the "*collection of content and communications data from fibre-optic cables and infrastructure owned by United States'* [communication service providers]." It has "*broad access to global data, in particular that of non-US citizens, which can then be collected, stored and searched using keywords*" [First Section §§18, 395].

171. In addition, Executive Order 12333 authorises US agencies to collect, retain or disseminate "*information constituting foreign intelligence*", which is defined as "*information relating to the capabilities, intentions and activities of foreign powers, organizations or persons*" [§§2.3, 3.4(d)]. Bulk surveillance is permitted. Presidential Policy Directive 28 on signals intelligence activities, issued 17 January 2014, states that the US must "*collect signals intelligence in bulk in certain circumstances in order to identify … threats*", where "*bulk*" means "*the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (eg specific identifiers, selection terms, etc).*"[18]

---

[18] White House of President Barack Obama, 'Presidential Policy Directive/PPD-28' (17 January 2014), <https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities#_ftnref5>.

172. On 9 October 2014, during the IPT proceedings, the UK Government disclosed a note which confirmed that PRISM and UPSTREAM 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*" [First Section §30]. It stated that, as a matter of administrative practice, the UKIS may make a request for intercepted material where:

    a) the UKIS have a s.8(1) warrant or s.8(4) warrant which would, if the UK had obtained the information, permit it to be intercepted and accessed; or

    b) making a request for the material without a RIPA interception warrant would not amount to deliberate circumvention or otherwise frustrate the objectives of RIPA.

    It was also said that where the UKIS receive "*intercepted communications content or communications data*" from foreign intelligence agencies, irrespective of whether that data is "*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 RIPA regime is, as a matter of administrative practice, applied by analogy (First Section §30).

173. The 1946 UKUSA Agreement, declassified in 2010, explains the extent of intelligence sharing:

> "Such exchange will be unrestricted on all work undertaken except when specifically excluded from the agreement at the request of either party and with the agreement of the other. It is the intention of each party to limit such exceptions to the absolute minimum and to exercise no restrictions other than those reported and mutually agreed upon." [emphasis added] [**SB/11/§3(b)**]

174. All intelligence material is shared between the Five Eyes states by default. The Agreement says in Appendix C paragraph 20 [**SB/11**]: "*As soon as it can be arranged each party will furnish to the other as promptly as practicable without request and as a matter of routine, one copy of every item of raw traffic collected as acquired by its operating agencies, regardless of source.*" [emphasis added]

175. Such routine automatic provision of raw bulk access reportedly includes direct access to US-held bulk communications data and content [10HROs Reply Sep 2016 §77 **BG/18**].

(2) Interference

176. The US operates a number of interception schemes, including arrangements similar to the s.8(4) regime, which allow intelligence material of non-US citizens to be collected, accessed, stored and searched. The Applicants were, at the very least, "*potentially at risk*" of having their communications and associated data requested from a foreign intelligence agency and/or obtained by the UKIS [§§395-396].

177. As is the case for a domestic interception regime, there is an interference with Article 8 rights by the existence of the intelligence sharing regime. Further, there will be an interference each time data is transferred to the UK and copied to GCHQ's computer systems, or made accessible to GCHQ remotely. Further interferences again occur when the data is processed, analysed, selected for examination or read, looked at or listened to by or for GCHQ.

178. In addition, there has been an interference with the Applicants' rights under Article 10(1) of the Convention on account of the intelligence sharing regime, as journalists and other "public watchdog" organisations. There is no difference in the interference with Articles 8 and 10 rights whether the data is intercepted by the UKIS or the same data is intercepted by the NSA and made accessible to the UKIS.

(3) Safeguards for intelligence sharing

179. The First Section endorsed the principle that the minimum safeguards which apply to direct surveillance must apply equally to the intelligence sharing regime [§423-424]:

> 423. … as the material obtained is nevertheless the product of intercept, those requirements which relate to its storage, examination, use, onward dissemination, erasure and destruction must be present … as States could use intelligence sharing to circumvent stronger domestic surveillance procedures and/or any legal limits which their agencies might be subject to as regards domestic intelligence operations, 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 (see paragraph 216 above).
>
> … Consequently, the circumstances in which intercept material can be requested from foreign intelligence services must also be set out in domestic law in order to avoid abuses of power. While the circumstances in which such a request can be made may not be identical to the circumstances in which the State may carry out interception itself … they must nevertheless be circumscribed sufficiently to prevent – insofar as

possible – States from using this power to circumvent either domestic law or their Convention obligations."

180. The First Section's analysis of the law was correct. In *RE v United Kingdom* (2016) 63 EHRR 2 at §130, the Court held that the "*decisive factor*" in determining whether the *Weber* criteria applied *"will be the level of interference with an individual's right to respect for his or her private life and not the technical definition of that interference.*" Thus, the same principles apply where the NSA provides GCHQ with access to intercept material as where GCHQ conducts surveillance itself.

181. The First Section was also correct that, as a minimum, the *Weber* standards, making such limited changes as are necessary for the context, apply. Accordingly:

    a) The defects identified by the First Section in the s.8(4) regime also apply to the intelligence sharing regime (see paragraphs 113-120 above).

    b) The additional defects identified in paragraphs 105-112 and 121-140 above also apply to the intelligence sharing regime. In particular, there must be prior independent judicial authorisation of intelligence sharing and the use of its product, reasonable suspicion, and notification where possible.

182. For the same reasons, the safeguards in place in respect of the intelligence sharing regime are inadequate to provide adequate protection to journalists (or equivalent protection to watchdog organisations) as required by Article 10:

    a) First, the intelligence sharing regime does not contain either the "overriding public interest requirement" or any of the other *Sanoma* Safeguards (see paragraph 148 above). The Applicants' submissions at paragraphs 141-160 above, as regards the incompatibility of the RIPA s.8(4) regime with Article 10 are repeated.

    b) Secondly, no arrangements are in place to provide safeguards where shared information received by the UKIS may have been obtained in disregard of the rights of journalists or sources. The journalistic provenance of shared information may be unclear where provided by a third state, in particular where such information is fragmented or incomplete. The retention and exploitation of such journalistic

information by the receiving state seriously interferes with the journalistic rights under Articles 8 and 10 of the Convention. Despite this:

i) the intelligence sharing agreements themselves afford no guarantees that the parties to the regime will apply appropriate safeguards to journalistic sources and material in the information they share and receive; and

ii) the UK's intelligence sharing "regime" (such as it is) lacks any or any sufficient safeguards to protect journalistic sources and material upon receipt or access by the UKIS against impermissible interferences. In particular, no safeguards exist to prevent intentional or incidental exploitation of journalistic sources or material, alone or in combination with other existing material in the UK's possession. The relevant guidance (such as it is) is wholly deficient. The 2016 Interception Code [**CB2/33**] contains no guidance on the use/exploitation of information shared with the UKIS in circumstances in which Article 10 protections for journalistic sources and journalistic material are engaged.

183. The absence of safeguards to protect journalistic sources and materials means the intelligence sharing regime is not in accordance with the law under Articles 8 and 10.

G The compatibility of the RIPA Part 1 Chapter II regime with the Convention

184. The First Section rightly held that, because it does not comply with EU law, the Part I Chapter II communications data "acquisition" regime is not in accordance with the law [§§465-468]. Part I Chapter II does not comply with EU law insofar as it does not (i) limit access to communications data, where accessed in order to combat crime, to the purpose of preventing "serious crime" and (ii) require access to be approved by an independent court or administrative body (save where access is sought for the purpose of identifying a journalist's source): see generally *Tele2/Watson* **[CB3/57]** and First Section §§232-234. As mentioned, the First Section also held that the regime violated Article 10 as it lacked provision for an overriding requirement in the public interest in communications data acquisition where access could reveal a journalist's sources, including where a journalist's communications data was accessed or collateral intrusion was possible [§§496-499].

185. The Grand Chamber is invited to affirm these findings, which are plainly right. It is not

necessary to consider in further detail requirements in relation to communications data.

186. The First Section declined to address whether the minimum safeguards in the secret surveillance case law apply to communications data access regimes [§352], understandably where the UK regime was not in accordance with domestic law. But if at §§460-464 it suggested otherwise, that is incorrect and the Grand Chamber is invited to affirm that those requirements apply. The First Section rightly held that it was "*not persuaded that the acquisition of related communications data is necessarily less intrusive than the acquisition of content*" [§356]. As *RE* indicates, the decisive factor in whether the minimum safeguards apply and their stringency is the level of interference with private life: see paragraph 180 above. It follows that the minimum safeguards apply, as the IPT held.[19]

187. If the Court wishes to address any further aspect of the Part 1 Chapter II regime (which is not the subject of its questions), the Applicants maintain their submissions below.[20]

H ***Other matters***

188. The First Section concluded at §§237-268 that the Applicants in the first and second of the joined cases satisfied the Article 35 §1 requirement to exhaust effective domestic remedies. Should the UK Government seek to re-argue this point, the Applicants rely upon the reasons at §§169-172 of their Consolidated Submissions to the Chamber.

189. The First Section at §§522-525 awarded the Applicants in the first and second joined cases costs and interest in light of its conclusions as to the violations of Articles 8 and 10 and in recognition of the considerable work the Applicants did. The Grand Chamber is invited to confirm these awards for the same reasons, and to update them (again with interest) to reflect the additional work in relation to its hearing of this application, explained in the Applicants' requests (in all three Applications) and their attachments [**SB/15-17**].

I ***Summary of answers to the Court's questions***

190. The Applicants respond to the Court's questions above. They summarise their answers here.

---

19 First IPT Judgment §114 **[CB1/14]**.

20 App Cons Obs 29 Sep 2017 §§45, 146-160 **[SB/2]**.

1. Has there been an interference with the applicants' rights under Article 8 § 1 of the Convention on account of the operation of the regime under section 8(4) of RIPA?

Having regard to the fact that the regime permits the "bulk interception" of communications, the parties are invited to clarify at which stage(s) the interception and processing of information pursuant to section 8(4) warrants is capable of affecting the rights of concrete individuals or organisations; and to describe the manner in which the individuals or organisations are affected at the stage(s) identified.

191. In accordance with the Court's established case law, an interference occurs as a result of the existence of the RIPA s.8(4) regime (see paragraphs 62-70 above).

192. Interferences with correspondence and private life occur whenever communications are intercepted, copied, stored, subject to automated analysis, retained, read looked at or listened to by a person or further stored.

193. The interference at each stage is significant. The systematic collection, retention and analysis of data about individuals by the state is a significant interference, even if the information is read by machine analysis rather than a person. As noted, technological analysis of communications data enables the state to develop an extraordinarily detailed and intrusive profile of a person's private life, including sexual and political interests, health concerns, movements and social links. Rights are affected by the copying and analysis of private correspondence and communications without consent. This chills communications, especially where content is inherently private or data automatically profiled or analysed.

194. The nature of this interference, and the resulting harm, has been addressed above. In sum:

    a) Technological developments mean that bulk surveillance has become much broader and intrusive than ever before. Governments can now create detailed profiles of intimate aspects of people's private lives (paragraph 12 above).

    b) This is in part attributable to the fact that most online communications and information travel internationally even if the initiator and recipient are in the same locality. The UK Government's expansive definition of "*external*" communications means that this restriction on the application of the RIPA s.8(4) regime is now effectively meaningless (see paragraphs 107-112 above).

    c) It is also due to the role of communications data. The retention of communications data creates a digital trail of an individual, recording their habits, movements, lifestyle,

preferences and social relationships. The data can be used to create a comprehensive profile of the individual concerned and is no less intrusive than the content of those communications (see paragraphs 18 and 58.b)-58.c) above. Journalists and public watchdogs are exposed to particular harm (see paragraph 24 above).

d) In fact, the technological analysis of communications data may lead to an even greater degree of interference with private life than the reading by a human analyst. Communications data is structured in such a way that computers can process and search for patterns in the data faster and more effectively than similar searches through content. Bulk regimes permit the accumulation of data from many bearers and warrants, the building of mass data repositories and the automation – and therefore wide-scale interrogation – of those databases. Moreover, most of the data involved concerns persons of no interest to the intelligence agencies (see paragraph 21 above).

e) The interception and inspection of journalists' and human rights organisations' private communications is particularly serious, and the chilling effect is particularly acute, in light of the important role these organisations play in holding governments to account.

The Government are further invited to provide examples of queries and/or selectors used and to inform the Court about the number (and duration) of interception permissions issued annually.

195. The response to this question is for the UK Government. However, a query may include a number of elements (eg a search for people who read a particular online publication, who send emails in a particular language and whose location data show presence in a particular area or place). A selector may include an email address or other identifier, such as a username or telephone number. Analysts may choose to examine retained material by using a query or by a selector. There is only a very small number of s.8(4) warrants, which provides an indication of their broad scope. Each warrant is subject to regular 'rolling' renewal so that the surveillance authorisations operate continuously. In 2016, only 13 warrants were issued under s.8(4).[21] The Government has never disclosed how many queries or selectors are used.

In addition, the Government are invited to clarify the use which is made of retained material in general and retained communications data in particular. Does material have to be

[21] Interception of Communications Commissioner, *Annual Report for 2016* (HC 297, 2017) p.40 **[SB/14]**.

"selected for examination" by an analyst in order to provide intelligence, or could it simply be subject to complex and comprehensive analysis (by computer)? Could material that is not on an index permitting it to be "selected for examination" by an analyst nevertheless be interrogated, aggregated and subjected to complex analysis by computer in order to provide intelligence? Is a difference made between content and communications data in this regard? On what basis is this retained content and communications data eventually discarded?

196. There is no requirement for communications data to be "*selected for examination*" before it can be read, looked at or listened to: see paragraph 58.a)-58.b) above. The effect is that the certificate does not limit the use of the communications data, and the protections for persons in the British Islands do not apply. And all data (including content) may be subjected to complex and comprehensive automated analysis by computer before it is "*read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant*" under RIPA s.16(1): see paragraphs 58.c)-58.e) above.

197. Raw intercept material that is not on an index may be aggregated and subjected to analysis by computer to provide intelligence. Such material may also be retrieved by an analyst by searching that material using a selector or complex query (see paragraph 58.f) above).

198. Raw intercept material is eventually discarded once a retention period is reached, or GCHQ's systems no longer have technical capacity to store the data: see paragraph 58.g) above.

2. In the event that there has been an interference, was it in accordance with the law and necessary within the meaning of Article 8 § 2?

In particular,

a) To what extent should the standards developed in the Court's case-law on secret measures of surveillance – and, in particular, the interception of communications – apply to the regime permitting the bulk interception and processing of communications and related communications data?

b) Assuming that Article 8 § 2 requires the existence of certain safeguards to avoid abuses of power, to what extent do these safeguards have to be made public? Can they exist "below the waterline" if they are subject to independent oversight?

c) Does Article 8 § 2 also require supervision and review of the impugned activities by an independent body and, if so, what level of independence from the Government is needed? In view of the specific type of analysis in bulk interception, at what stage(s) would it be appropriate for supervision to take place? What type of supervision and review, if any, is required when the surveillance is first ordered, while it is being carried out, and after it has been terminated? Should there be a body entrusted with oversight powers which is capable

of rendering legally binding decisions? If so, at what stage(s)? d) Should the same principles apply to both content and related communications data?

199. The UK bulk interception regime is neither strictly necessary nor proportionate to the interference with Article 8 (and Article 10) rights entailed: see paragraphs 73-92 above.

200. The standards in the Court's caselaw should be updated and enhanced to reflect the intrusiveness and risks to democratic society of modern bulk interception techniques. Those standards apply to regimes permitting bulk interception and processing of communications and communications data: see *Weber*, *Liberty* and *Rättvisa*; paragraphs 128-140 above.

201. Even applying the Court's established case law, the regime is not in accordance with the law nor necessary within the meaning of Article 8(2) (see paragraphs 93-127 above).

202. Sufficient safeguards to make the scheme "foreseeable" must be "*accessible*", within the meaning of that caselaw. This means they must be published. The terminology of "*below the waterline*" is not a useful aid to analysis. Secret provisions cannot contribute to the accessibility and foreseeability of the law: see, eg, *Liberty* §77; paragraphs 98-102 above.

203. Supervision should take place *ex ante* and *ex post*. Prior independent judicial approval ought to be required when the warrant is issued and renewed, and when it is applied, including for approval of selectors and search terms (or classes of them). See paragraphs 131-135 above.

204. There is no basis for any distinction between content and communications data: communications data may be more intrusive, and the risks of automated secret processing are at least as great. The same safeguards should apply to both: paragraph 186 above.

3. Has there been an interference with the applicants' rights under Article 8 § 1 of the Convention on account of the operation of the regime by which the United Kingdom Government are able to request and receive intelligence from foreign Governments? If so, the parties are invited to clarify the manner in which the receipt of intelligence (and the retention and processing of that intelligence) is capable of giving rise to an interference with the rights of concrete individuals or organisations.

205. Yes. By analogy to interception arrangements, the existence of intelligence sharing arrangements is itself an interference under Articles 8 and 10. In addition, when the UK receives a copy (or remote access to) intercept material from a foreign government, there is an interference under Article 8(1). The receipt (and subsequent processing and analysis) is a further significant interference for the reasons set out above in paragraphs 176-178 above.

4. In the event that there has been an interference, was the regime for the requesting and receiving of intelligence from foreign Governments in accordance with the law and necessary within the meaning of Article 8 § 2? To what extent do the standards developed in the Court's case-law on secret measures of surveillance – and, in particular, the interception of communications – apply to this regime?

206. The arrangements are not in accordance with the law, for the reasons set out at paragraphs 179-183 above. The standards in the case law on secret surveillance measures apply here, because there is no difference in principle between the state itself intercepting and receiving the fruits of interception from another state.

Has there been an interference with the applicants' rights under Article 10 § 1 of the Convention on account of the operation of either the regime under section 8(4) of RIPA or the intelligence sharing regime? If so, was it prescribed by law and necessary in a democratic society within the meaning of Article 10 § 2? More particularly, having regard to the risk of intercepting confidential journalistic material and communications capable of identifying journalists' sources, what safeguards are necessary to ensure that these regimes are compatible with Article 10 of the Convention?

207. Yes, there has been an interference under Article 10(1) from both regimes: paragraphs 71-72 above. Neither regime is prescribed by law or necessary in a democratic society under Article 10(2). The required safeguards are set out at paragraphs 141-160 above.

J ***Conclusion***

208. The Grand Chamber is invited to confirm the findings of breach of the Convention made by the First Section and make the additional findings of breach of the Convention set out above.

BEN JAFFEY QC	**HELEN MOUNTFIELD QC**	**GAVIN MILLAR QC**
DAVID HEATON	**RAVI MEHTA**	**CONOR MCCARTHY**
GAYATRI SARATHY	**FLORA ROBERTSON**	**AIDAN WILLS**
For 10 Human Rights NGOs	**For BBW and others**	**For BIJ and others**

3 May 2019

ANNEX: REFERENCES TO APPLICANTS' PREVIOUS SUBMISSIONS

Topic	Key references to previous submissions
The developing case law of the Court	App Cons Obs 29 Sep 2017 §§52-68, 71-74
Summary of the UK's bulk interception regime	BBW App 30 Sep 2013 §§31-40, 53-104 BBW Update 2 Mar 2015 §§6-72 BIJ App 1 Sep 2014 §§22-30, 38-88 10HROs App 31 Mar 2015 §§4-40 10HROs Update 31 Jul 2015 §§3-15 10HROs Reply Sep 2016 §§25-32, 35-61, 82-88, 95-126 App Cons Obs 29 Sep 2017 §§34-51
Summary of the UK's intelligence sharing regime	BBW App 30 Sep 2013 §§18-30 BBW Update 2 Mar 2015 §§73-83 BIJ App 1 Sep 2014 §§31-37 10HROs App 31 Mar 2015 §§5-8 10HROs Reply Sep 2016 §§63-77, 89-94, 226-231 Factual Appendix §§4-19 App Cons Obs 29 Sep 2017 §§88-89
The compatibility of bulk interception under RIPA s.8(4) with the Convention: Facts	BBW App 30 Sep 2013 §§31-40, 53-104 BBW Update 2 Mar 2015 §§6-72 BIJ App 1 Sep 2014 §§22-30, 38-88 10HROs App 31 Mar 2015 §§4-40 10HROs Update 31 Jul 2015 §§3-15 10HROs Reply Sep 2016 §§25-32, 35-61, 82-88, 95-126 App Cons Obs 29 Sep 2017 §§78-87
The compatibility of bulk interception under RIPA s.8(4) with the Convention: Interference with Article 8(1)	BBW App 30 Sep 2013 §§113-116 BIJ App 1 Sep 2014 §§101-102 10HROs App 31 Mar 2015 §42 10HROs Reply Sep 2016 §§127-134
The compatibility of bulk interception under RIPA s.8(4) with the Convention: Interference with Article 10(1)	BIJ App 1 Sep 2014 §§103-104 BIJ Reply §§38-45 10HROs App 31 Mar 2015 §74-75 10HROs Update 31 Jul 2015 §§31-35 App Cons Obs 29 Sep 2017 §§130-137
The compatibility of bulk interception under RIPA s.8(4) with the Convention: Strict necessity and proportionality	BBW App 30 Sep 2013 §§176-178 BIJ App 1 Sep 2014 §§162-165 BIJ Reply §§46-55 10HROs App 31 Mar 2015 §§61-69 10HROs Update 31 Jul 2015 §§16-17, 26-30 10HROs Reply Sep 2016 §§201-220 App Cons Obs 29 Sep 2017 §§159-160

The compatibility of bulk interception under RIPA s.8(4) with the Convention: Not in accordance with the law	BBW App 30 Sep 2013 §§117-118, 140-175 BBW Reply 26 Sep 2016 §§10-29 BIJ App 1 Sep 2014 §§105-156 BIJ Reply §§56-90 10HROs App 31 Mar 2015 §§43-60, 74-81 10HROs Update 31 Jul 2015 §§18-25, 36-39 10HROs Reply Sep 2016 §§135-200, 286-294 App Cons Obs 29 Sep 2017 §§98-129
Intelligence sharing: Facts	BBW App 30 Sep 2013 §§18-30 BBW Update 2 Mar 2015 §§73-83 10HROs App 31 Mar 2015 §§5-8 10HROs Reply Sep 2016 §§33-34, 62-77, 89-94, 226-231 Factual Appendix §§4-19
Intelligence sharing: Interference	BBW App 30 Sep 2013 §§113-116 10HROs Reply Sep 2016 §§221-224 App Cons Obs 29 Sep 2017 §§138-140
Intelligence sharing: Safeguards	BBW App 30 Sep 2013 §§117-118, 119-139 BBW Update 2 Mar 2015 §§84-85 BBW Reply 26 Sep 2016 §§30-37 10HROs App 31 Mar 2015 §§70-73 10HROs Reply Sep 2016 §§232-250 App Cons Obs 29 Sep 2017 §§141-145
The compatibility of Chapter II RIPA with Articles 8 and 10	BIJ App 1 Sep 2014 §§157-161 BIJ Reply §§91-119 App Cons Obs 29 Sep 2017 §§45, 146-160