IN THE EUROPEAN COURT OF HUMAN RIGHTS
BEFORE THE FIRST SECTION
BETWEEN:

BIG BROTHER WATCH
OPEN RIGHTS GROUP
ENGLISH PEN
DR CONSTANZE KURZ

Applicants (App No 58170/13)

BUREAU OF INVESTIGATIVE JOURNALISM
ALICE ROSS

Applicants (App No 62322/14)

10 HUMAN RIGHTS ORGANISATIONS

Applicants (App No 24960/15)

- v -

UNITED KINGDOM

Respondent

APPLICANTS' CONSOLIDATED OBSERVATIONS FOR HEARING ON 7 NOVEMBER 2017

References to the Core Bundle are in the form [CB/Annex No.]; to the Applications are in the form [BBWApp;BIJApp;10OrgApp/para number], to Update Submissions in the form [BBWUpdate;10OrgUpdate/para number] and to Reply Observations in the form [BBWReply;BIJReply;10OrgReply/para number]. References to the Government's Observations are in the form [UKBBWObs;UKBIJObs;UK10OrgObs/para number] and its Further Response to the Applicants' Observations in Reply in the form [UKBBWResponse;UKBIJResponse;UK10OrgResponse/para number]. These Observations summarise the submissions and observations in each of the Applicants' cases.

29 September 2017

For BBW and Ors **Solicitors**: Adam Hundt and Daniel Carey, Deighton Pierce Glynn.
Counsel: Helen Mountfield QC, Tom Hickman and Ravi Mehta.

For BIJ and another **Solicitors**: Rosa Curling, Leigh Day.
Counsel: Gavin Millar QC, Conor McCarthy, and Aidan Wills.

For 10 HRs Organisations
Solicitors: Emma Norton, Liberty; Scarlet Kim, Privacy International; Mark Scott, Bhatt Murphy; Nick Williams, Amnesty International.
Counsel: Dinah Rose QC, Hugh Tomlinson QC, Matthew Ryder QC, Ben Jaffey QC, Eric Metcalfe, Nick Armstrong, Edward Craven; Tamara Jaber.

Table of contents

I. INTRODUCTION & SUMMARY

1. These joined applications concern the privacy of modern forms of communication (including communication covered by journalistic privilege). The UK Government claims the right to intercept and examine, in bulk, any communications that happen to traverse the UK and to store the content of those communications as well as any related communications data. The UK asserts a right to obtain similar bulk access to communications intercepted by the intelligence services of other states. No independent, let alone judicial, authorisation is required in either case.

2. This case has a worldwide reach, as illustrated by the range of Applicants before the Court, resident in different jurisdictions both inside and outside the Council of Europe. If the UK Government's case is correct, then the authorities of every Council

of Europe Member State are free to intercept communications passing through their territory in bulk and to pass it to the authorities of third countries without any legal safeguards against arbitrary use of this power. A single communication could be intercepted dozens of times in the course of its transmission by multiple states, each copying, analysing and storing the communication, as well as its related data.

3. The Applicants challenge the lack of clarity, foreseeability and proportionality in the UK's legal regime for the surveillance of communications by its own Intelligence Services. They similarly challenge the UK's access to and use of the product of such surveillance by the services of other states. The current domestic legal framework was developed in a context where the state's ability to obtain personal information depended mostly on analysis of the content of communications. However, the means by which digital communications are now routed; the expansion in use of digital forms of communication; and vastly increased technical ability to store and analyse communications data on a bulk basis to build intrusive personal profiles of individuals, mean that the legal framework is inadequate to ensure the protection of longstanding Council of Europe standards of respect for private life.

4. The fact that such bulk interception and sharing is even possible reflects rapid technological change. The UK Intelligence Services – the Security Service ("**MI5**"), the Secret Intelligence Service ("**MI6**") and the Government Communications Headquarters ("**GCHQ**") (collectively the "**UKIS**") and the intelligence services of many UK allies, including those outside the Council of Europe – can now intercept, store and analyse vast amounts of internet and telephone communications regardless of any individual ground for reasonable suspicion. This raises novel and important issues of law and principle and the application of established principles to new technology.

5. Council of Europe States face serious security threats and the problem of serious crime. But these threats must be addressed whilst also protecting fundamental rights: the Court has repeatedly reiterated that "*powers of secret surveillance of citizens are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions*" (*Klass and Others v Germany* (1978) 2 EHRR 214 ("*Klass")* at §42; *Rotaru v Romania*, App. No. 28341/95, 4 May 2000 at §47).

6. A potentially valuable power in combating serious crime or terrorism can still be arbitrary, disproportionate and incompatible with the rule of law. In *S and Marper v United Kingdom* (2009) 48 EHRR 50 (*"Marper*") the UK government submitted 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 (at §92). The Grand Chamber nonetheless held that the retention was a "*disproportionate interference*" with those individuals' private lives (at §135). Similarly, in *MK v France,* App 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*." (§13) Rather, it warned that the logic of the French government'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*" (§37).

7. This Court has long recognised the intrusiveness inherent in government interception of the content of communications. In *Klass*, the Court held that "*telephone conversations"* are *"covered by the notions of 'private life' and 'correspondence'"* referred to in Article 8 of the Convention (§41).

8. Since *Klass*, the advent of the internet and advancements in modern technologies have revolutionised the way we communicate. The Court has acknowledged these developments, expanding the scope of Article 8 protection to include "*e-mail communications*" (see *Weber and Saravia v Germany* (2008) 46 EHRR SE5 ("*Weber*"), §77).

9. The world has again moved on. When the Court decided *Weber* in 2006, smartphones did not exist (the iPhone was launched in 2007); Facebook was a website open to university students only; Twitter had not been invented and Gmail was not available in Europe. The understanding of the intrusive power of the mass storage and analysis of large quantities of private data was in its infancy. Technological developments since then mean that governments can now create detailed and intrusive profiles of

intimate aspects of private lives by analysing patterns of communications on a bulk basis.

10. People living in Council of Europe States and beyond now live major parts of their lives online. We use the internet to impart ideas, conduct research, expose human rights abuses, explore our sexuality, seek medical advice and treatment, correspond with lawyers, communicate with friends, colleagues and loved ones and express our political and personal views. We also use the internet to conduct many of our daily activities, such as keeping records, arranging travel and conducting financial transactions. Much of this activity is conducted on mobile digital devices, which are seamlessly integrated into our personal and professional lives. They have replaced and consolidated our fixed-line telephones, filing cabinets, wallets, private diaries, photo albums and address books.

11. The internet has also enabled the creation of greater quantities of personal data about our communications, known as communications data or metadata. Communications data is information about communication and patterns of communication, which may include the sender and recipient, the date and location from where it was sent and at which it was received, the duration and frequency of communication, patterns of communication between associates and the type of device used to send or receive the information and devices linked to it.

12. Communications data is the digital equivalent of having a person trailing a targeted individual at all times, recording where they go and with whom they speak and associate. Communications data will reveal web browsing activities, which reveal medical conditions, religious beliefs and political affiliations. Items purchased, news sites visited, forums joined, books read, movies watched and games played – each of these pieces of communications data gives an insight into a person. Mobile phones continuously generate communications data as they stay in contact with the mobile network, producing a constant record of the location of the phone (and therefore its user) and allowing a person's movements to be tracked and revealing their internet usage on their phone. Communications data produces an intrusive, deep and comprehensive view into a person's private life, revealing identities, relationships, interests, locations and activities.

13. This is of particular concern to journalists and other social "*watchdog*" organisations, such as human rights and other public interest organisations, given the potential for unwarranted intrusion into the right to (journalistic) free expression. The potential for the identification of journalistic sources is plainly a major concern arising from these capabilities. But it is not the only one. As Professor Danezis[1] explains in his expert report **[CB/10]** (§§63–89) modern techniques enable direct or indirect inferences to be drawn in respect of a range of confidential (and sensitive) matters including: a journalist's network of professional sources or contacts; the timing and intensity of contact with those sources; a journalist's lines of enquiry, research agenda or developing stories; the location of the journalist (or his source); his or her movements over time (and those of his sources); and materials or physical sites of interest to the journalist. Without proper regulation, access to these forms of privileged information by the UKIS poses a real threat to the free press and public interest NGO work.

14. Worldwide, Courts are in the process of developing and applying existing principles to these new technologies. In *Riley v California* 134 S.Ct. 2473 (2014); 573 US (2014) ("*Riley*") **[CB/52]**, Chief Justice Roberts of the United States Supreme Court noted that "[t]*he term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers*." The consequence is that there is a "*digital record of nearly every aspect of their lives*". This is "*qualitatively different*" from the recent past. Modern communications 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." (pp.19-20)

---

[1] Professor of Security and Privacy Engineering, University College London.

15. The costs of storing and collating data have decreased drastically, and continue to do so every year. Most importantly, the technical means of analysing data have advanced so rapidly that what were previously considered meaningless or incoherent types and amounts of data can now produce revelatory analyses. Communications data is structured in such a way that computers can search through it for patterns faster and more effectively than similar searches through content. Indeed, access to content is often unnecessary: as the RUSI Committee (which included the former heads of the UKIS) put it:

> "[a]ggregating 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."[2]

16. Such interferences with privacy require strong legal safeguards. This is no more than to apply long-standing principles to new technology. As Roberts CJ put it in *Riley:*

> "Privacy comes at a cost… 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… Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life," … The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant."

17. In the UK Supreme Court, Lord Sumption identified the same phenomenon in *R. (on the application of Catt) v Association of Chief Police Officers of England, Wales and Northern Ireland* [2015] A.C. 1065 **[CB/55]**, p.1077F-G at [2]:

> "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

---

[2] Royal United Services Institute ("RUSI"), *A Democratic Licence to Operate: Report of the Independent Surveillance Review* (13 July 2015), available at https://rusi.org/publication/whitehall-reports/democratic-licence-operate-report-independentsurveillance-review ("RUSI Report") **[CB/49]** §2.14.

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."

18. Nevertheless, the legal response in the UK has been limited and hesitant. As Lord Sumption put it "*the concept of a legal right of privacy whether broadly or narrowly defined fell on stony ground in England. Its reception here has been relatively recent and almost entirely due to the incorporation into domestic law of the European Convention on Human Rights*" (p.1077H, ibid).

19. These applications are the latest in a series of cases about the failure of the UKIS to give proper effect to the right to privacy. This Court, over the last three decades, has repeatedly found the UK to have violated Article 8 of the Convention e.g. *Malone v UK* (1985) 7 EHRR 14 ("*Malone")*; *Hewitt & Harman v UK* (1992) 14 EHRR 657; *Halford v UK* (1997) 24 EHRR 523; *Khan v UK* (2001) 31 EHRR 45 ("*Khan*"); and *Liberty v UK* (2009) 48 EHRR 1 ("*Liberty")*. The response to the Court's judgments has sometimes been minimal including through the introduction of a bare legislative framework which obfuscates the true extent of the surveillance taking place.

20. Despite its submissions to this Court, the Snowden documents indicate that when speaking privately, the UKIS have expressed their pleasure at the minimal UK legal regime that permits bulk interception. GCHQ describes the UK legal regime as a *""selling point" for the Americans*." GCHQ is "*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*."[3] In a briefing, one of GCHQ's senior legal advisers noted "*we have a light oversight regime compared with the US."* The United Kingdom Investigatory Powers Tribunal has "*so far always found in our favour"*.[4]

---

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 Ewan MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, "*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

21. The UK's former bulk surveillance regime under the Interception of Communications Act 1985 ("**ICA**") was found to be unlawful by this Court in *Liberty*. This case concerns the replacement scheme under the Regulation of Investigatory Powers Act 2000 ("**RIPA**") **[CB/22]**, which has lesser safeguards despite rapid technological change and increased ability for the state to build personal profiles of individuals using data about their online activity. Indeed, by way of contrast with the German "*strategic monitoring*" scheme analysed by the Court in *Weber*:

21.1. The independent G10 Commission (including a legally qualified President) had to consent in advance to proposed monitoring, on a monthly basis. There was therefore independent, detailed and continuous scrutiny of the precise surveillance measures used. The Commission had the power to order that individuals subject to monitoring be notified (*Weber*, §25). By contrast, RIPA prohibits a person from knowing he or she has been subject to a section 8(4) warrant. There is also no requirement for prior judicial or independent authorisation of surveillance activities.

21.2. 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, even if they are generally worded and disclosure of their content would itself not pose a real risk to national security.[5]

21.3. The categories under the G10 Act were very tightly defined (an armed attack on Germany, the commission of a terrorist attack in Germany, international arms trafficking, illegal importation of drugs into Germany, counterfeiting (but only when committed abroad) or money laundering (but only when it threatened the monetary stability of Germany)). By contrast, a s.8(4)

---

[5] For instance, on 3 June 2014, *The Register* reported that "*Miliband's first 2009 warrant for TEMPORA authorised GCHQ to collect information about the "political intentions of foreign powers", terrorism, proliferation, mercenaries and private military companies, and serious financial fraud*", The Register, *Revealed: Beyond top secret British Intelligence Middle-East internet spy base*, 3 June 2014, http://www.theregister.co.uk/Print/2014/06/03/revealed_beyond_top_secret_british_intelligence_middleeast_internet_spy_base/

certificate can cover any purpose within the far wider rubric of "*national security*", "*serious crime"* or the economic well-being of the UK.

21.4. 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). In practice at that time, interception could only cover some satellite communications because interception only took place in Germany and satellites focused their "*downlink*" on very narrow areas (§31). By contrast, as noted below, under the s.8(4) RIPA regime, a substantial volume of communications may be – and is – intercepted alongside related communications data.

21.5. 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). By contrast, there is no equivalent requirement for Secretary of State (still less judicial) approval of selectors used under RIPA. Profiling of entire populations is permitted.

21.6. There were stringent requirements on how information could be used. It could only be employed for the purpose of preventing, investigating and prosecuting specified, extremely serious, criminal offences (§§33-44). Transmission or further use had to be approved by a staff member with the qualifications to hold judicial office. By contrast, s.8(4) information may be used for any of the much more broadly defined functions of the UKIS, as well as being transferred domestically or abroad.

22. The limited safeguards against bulk surveillance in the UK have become ineffective as technology has developed over the last decade. For example, a traditional interception warrant under s.8(1) of RIPA (of the kind considered by the Court in *Kennedy v UK* (2011) 52 EHRR 4 ("*Kennedy*") requires the specification of a particular person or set of premises to be targeted. It was in that context that the Court observed that "[i]*ndiscriminate capturing of vast amounts of communications is not permitted under the internal communications provisions of RIPA*" (§160)). By contrast, a bulk communications warrant under s.8(4) goes much further. It need not

focus on particular people or premises: rather, an entire communications link can be targeted and all communications transmitted by it can be captured. Thus, under s8.4, bulk interception, storage and analysis is permitted for material within the scope of a (secret) certificate issued by the Secretary of State.

23. The legislation provides that a s.8(4) warrant must be primarily targeted at "*external*" not "*internal*" communications. However, as a result of technological changes in the way data is transmitted, the distinction drawn in national law between the legal regimes governing "*external*" and "*internal*" communications has become meaningless in practice. This is for two reasons. First, where a person in the UK communicates with a webpage, or email portal, which is hosted abroad, this will be classified as an *"external"* communication. Second, it is now routine for "*internal*" communications, such as an email between persons in the UK 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 the former has effectively become subject to the bulk interception powers as *"incidental"* product of bulk surveillance of *"external"* communications.

24. This means that the world has also changed dramatically from the position considered by this Court in *Liberty*. That case concerned the bulk surveillance only of telephone calls between the UK and the Republic of Ireland, and solely for counter-terrorism purposes. There, 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 Facebook messages between two Londoners will be routed via California and are likely to be intercepted by bulk surveillance techniques and subjected to automated profiling and analysis. The notional legal safeguards for "*internal*" communications have failed to keep up with the development of technology. This is incompatible with the quality of law requirement inherent in Article 8.

25. For example, assume a group of friends in London are arranging a meeting:

25.1. In 1990, they would have phoned or written to each other and perhaps left messages on answerphones to arrange a time. 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.

25.2. In 2000, 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 subject to any bulk surveillance.

25.3. In 2010, the friends would have used email, probably provided by an international provider such as Gmail. Such communications may have been collected under a bulk warrant.

25.4. By 2017, 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 are likely to leave the UK during transmission, and so be treated as 'external' and subject to bulk interception, filtering and storage.

26. The combination of changes to the technological means of transmission of data, the vastly expanded capacities of the UKIS to intercept data and to draw up a picture of a person's private life (see §§90, 116 below) and the exponential growth in use of electronic media to conduct private life; mean that the legislative distinction between "*internal*" and "*external*" communications (which is reflected in the Court's judgment in *Weber*) no longer provides any meaningful protection against arbitrary or disproportionate State intrusion into private life and correspondence.

27. The UK Government seeks to downplay the significance of interception when it states *[UKBBWIntResponse/3]* that "*the interception of a communication as it flows through a fibre optic cable, does not entail a substantial invasion of privacy…unless that communication is selected for examination: in other words unless a human examines it or may potentially examine it*". The Applicants do not accept that the interception, storage and subsequent searching of individuals' communications is a negligible, or lesser invasion of privacy. To the contrary, the interception, retention of, and repeated and sophisticated algorithmic searching of their communications

and ability to combine many sources of data to draw up patterns of communication is potentially an even more substantial interference with the right to private life and consequently create an even greater "*need for* […] *safeguards*".

28. In Joined Cases C-203/15 *Tele2 Sverige AB* and C-698/15 *Watson and Others* (ECLI:EU:C:2016:970) ("*Watson*") **[CB/57]**, the Court of Justice of the European Union ("**CJEU**") emphasised that communications data retained on a routine basis by commercial operators, "*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*" (at §§98-99). The RUSI panel (including the former heads of each of the UKIS) took a similar view (see §15 above). As noted above, for journalists and NGOs dealing with human rights abuses, other public interest information and confidential sources, the effect of retention of communications data is especially serious.

29. The UKIS recognise the power of communications data. Their approach is straightforward: GCHQ "*keep the entirety of all the communications data that comes into the building*…".[6] This includes location data for mobile telephones, websites visited, and who we have communicated with, and what we have read or looked at online. Nevertheless, bulk interception, filtering, storage and analysis of communications data (even for persons in the UK) requires no warrant or any other form of prior authorisation.

30. The position is made worse because of the complexity and obscurity of the UK legal regime. It is notable that the United Kingdom's observations in this case extend to well over 200 pages, including 38 pages on "*Domestic Law and Practice*". The UK Independent Reviewer of Terrorism Legislation, David Anderson QC (the "**Independent Reviewer**"), when asked to review the RIPA regime, concluded that

---

6 Summary Filenote: Visit of Sir Anthony May, Interception of Communications Commissioner, 15 May 2013, p. 2 **[CB/40]**.

its provisions were "*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*" **[CB/48]**.[7] Such a situation falls short of the minimum requirements of the Court's case-law concerning the requirement that law be accessible.

31. The Applicants submit that such a position is incompatible with Articles 8 and 10. The Court has repeatedly emphasised that, "[t]*he protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention* […and] *the need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned*" (*Marper at* §103; *MK v France* at §35). The law must provide, but in the UK no longer provides, adequate safeguards to ensure the continued enjoyment of these fundamental rights in the face of rapid technological changes.

Summary

32. In these submissions, the Applicants:

    32.1. Recall the key features of the legal framework applicable in the UK at the material time, including by reference to the Statement of Facts, as well as significant recent developments (**Section II**);

    32.2. Identify the relevant legal framework under the Convention (**Section III**);

    32.3. Set out the factual context and background to the Applications, by reference to the Statement of Facts produced by the Court for each application along with relevant updated information (**Section IV**);

    32.4. Address Question 3 of the Court's letter dated 10 July 2017, in relation to the compatibility with the "*in accordance with the law*" and "*necessary in a*

---

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

democratic society" requirements of Article 8 and/or Article 10 of the Convention, of the acts of the UKIS (**Section V**); and

32.5. Address the remainder of the Court's questions (**Section VI**).

II. RELEVANT DOMESTIC LAW AND PRACTICE

See [BBWApp/53-112]; [BIJApp/38-88]; [10OrgApp/(additional submissions)/30-40]

33. The Statement of Facts contains extracts of the relevant legislation and other relevant features of UK law. The Applicants briefly restate the key provisions for consideration by the Court.

A Relevant UK legislation

(1) Relevant functions of the UKIS

34. Section 1(2), 3(2) of the Intelligence Services Act 1994 ("**ISA**") **[CB/25]**, and s.1(2)-(4) of the Security Service Act 1989 ("**SSA**") **[CB/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 "*in support of the prevention or detection of serious crime*." The functions of the UKIS are not limited to responding to threats to national security.

(2) Key provisions of the Regulation of Investigatory Powers Act 2000 ("*RIPA*")

35. The domestic law regulating the interception of communications is principally set out in RIPA. The "*main purpose*" of RIPA, as stated in the accompanying Explanatory Notes to that Act, is to "*ensure that the relevant investigatory powers are used in accordance with human rights*".

Part I, Chapter I RIPA

36. The scope *rationae materiae* of Chapter I **[CB/22]** is set out in three provisions. Section 1(1) RIPA provides:

> "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."

37. Section 2(2) defines "*interception*" in the following terms:

> "a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he –
>
> (a) so modifies or interferes with the system, or its operation,
> (b) so monitors transmissions made by means of the system, or
> (c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system,
>
> as to make some or all of the contents of the communication available, while being transited, to a person other than the sender or intended recipient of the communication".

38. Interception of communications is not unlawful if it is 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 shall not issue an interception warrant unless he believes that the warrant is necessary, inter alia, 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 that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

39. Section 5(6) makes clear that conduct authorised by a warrant extends to "*related communications data*" as well as to the content of communications. In addition, s. 5(6)(a) permits so-called "*incidental*" collection of "*internal*" communications collected when engaging in bulk interception of an entire communications link:

> "**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."

40. Section 8 sets out the requirements of 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.

(2) The provisions of an interception warrant describing communications the interception of which is authorised or required by the warrant must comprise one or more schedules setting out the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications that may be or are to be intercepted.

…

(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." (emphasis added)

41. For the purposes of s.8(4), "*communications*" – and therefore the scope of that which is permitted by virtue of a 'bulk' warrant - can be very widely described, including by reference to their means of transmission. They need not be described by reference to a particular individual or premises. The effect of ss.8(4) and (5) of RIPA coupled with s.5(6) is that the limitations and safeguards on the ambit of an interception warrant for interception of "*internal*" communications, which satisfied this Court in *Kennedy*, do not apply, either to interception of "*external*" communications, or to the incidental interception of '*internal'* communications and "*related communications data"*. Read with the broad definition of "*external*" communications, this removes a very significant sphere of electronic communication from the scope of the safeguards of s.8(1)-(2) RIPA.

42. Section 15 RIPA imposes a requirement on the Secretary of State to put in place arrangements for securing the "*general safeguards*" set out in that section regarding the use of intercepted material, in particular restrictions on the storage, destruction, and extent of disclosure of that material.

43. One of the safeguards is that a bulk warrant under s.8(4) can only be issued if the Secretary of State has issued a certificate describing the intercepted material which he regards it as necessary to "*examine*". Section 16 RIPA provides that "*intercepted material*" may only be selected for such examination if it is not material which is "*referable to an individual*" in the UK or "*ha[s] as its purpose, or one of its purposes, the identification of material contained in communications sent by him, or intended by him*" unless the Secretary of State certifies such examination to be necessary for the statutory purposes. However, this provision:

    43.1. 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 communications data; and

    43.2. Applies only where it is <u>known</u> that the relevant individual is present in the UK. So if it were known that person A is in Manchester, a certificate would be required to permit the selection for examination of the content of that person's communications. By contrast, if it is not known where person A is located (because he or she is travelling on holiday), then no such certificate is required.

44. The existence or otherwise of a warrant is not a public fact. Section 17 restricts the disclosure of the existence or content of warrants granted under Chapter I.

Part I, Chapter II RIPA

45. Chapter II of RIPA **[CB/22]** provides for the obtaining of communications data by public authorities in the UK, including law enforcement agencies and the UKIS. Section 22 empowers a person designated by that public authority in accordance with s.25(2) of RIPA ("**a Designated Person**") to require a telecommunications company to obtain and disclose communications data. The Designated Person may make such an order where "*he believes it is necessary*" on a ground falling within s.22(2) of

RIPA. These grounds include, *inter alia*: national security; the prevention of disorder or the detection of crime; "*public safety*" or "*public health*". There is no requirement that communications data obtained pursuant to s.22 be targeted in respect of a particular person or premises.

Scrutiny of Investigatory Powers under RIPA

46. RIPA provides for the appointment of an "*Interception of Communications Commissioner*", charged with supervising the exercise of functions under – inter alia - Chapters I and II of the Act, and notifying the Prime Minister by a report if he identifies any contraventions of the Act (s.58). The Prime Minister must place such reports before the Houses of Parliament (s.58(6)) although she may redact information which she considers sensitive (s.58(7)).

47. Section 59 RIPA provides for the appointment of an "*Intelligence Services Commissioner*", charged with supervising the exercise of functions of the UKIS under ISA. The Commissioner must also provide reports to the Prime Minister (s.60), who must place such reports before the Houses of Parliament (s.60(4)), which may also be redacted (s.60(5)).

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

(3) Other legislation

49. The Justice and Security Act 2013 **[CB/29]** regulates the Intelligence and Security Committee of Parliament ("**ISC**"), the parliamentary committee which oversees the work of the UKIS. Section 1 provides for the appointment of its members drawn from, and appointed by the Houses of Parliament, after nomination by the Prime Minister. The ISC is not a full-time body and has only six permanent members of staff. Its functions consist of the oversight and examination of the activities of the UKIS, on which it reports annually to Parliament and the Prime Minister (ss.2-3). The Prime Minister may direct the exclusion of matters contained in any such report, prior to its delivery to Parliament, "*if prejudicial to the continued discharge of the functions*" of the UKIS (ss. 3-4).

50. The Data Protection Act 1998 ("**DPA**") **[CB/27]** provides a series of protections relating to the "*processing*" of "*personal data*" of "*data subjects*". However, s.28(1) provides an exemption for personal data from the data protection principles in the context of national security matters, "*if the exemption from that provision is required for the purpose of safeguarding national security*". Pursuant to s.28(2) the relevant Minister has certified that such exemption is required in relation to personal data processed by the UKIS in the performance of their functions **[CB/27]** *[UKBBWObs/2.19]*, in relation to six of the eight data protection principles, including the prohibition on transfer of data outside the European Union.

B Codes of Practice

51. Section 71 RIPA **[CB/22]** requires the Secretary of State to issue Codes of Practice relating to the exercise and performance of the powers and duties under, inter alia, Chapters I and II of the Act. These Codes shall be taken into account by persons exercising the powers under the Act or by Commissioners or the IPT (s.72). The Secretary of State has issued such codes, including the Interception of Communications: Code of Practice (as amended in January 2016) ("**the 2016 Interception Code**") **[CB/33]** and the Acquisition and Disclosure of Communications Data: Code of Practice (as amended in March 2015) ("**the 2015 Acquisition Code**") **[CB/32]**.

III. THE COURT'S CASE LAW

A. Article 8 of the Convention

Interferences with Article 8

52. The Applicants identify two discrete categories of interference with their rights under Article 8 of the Convention.

53. First, the state's systematic interception and storage, in bulk, of information about an individual or NGO, is an interference with private life. Storage of communications constitutes an interference with Article 8 whether or not such information is used at a later stage (see *Rotaru*, §46; *Bouchacourt v France* App. No 5335/06 (17 December 2009), §57; and *Marper*, §§77 and 86). The interception and

retention of communications data is also an interference (see *Malone* at §84 (in relation to the practice of 'metering') and *Amann v Switzerland* (2000) 30 EHRR 843, §65 – especially on a searchable database) as is its transmission to other authorities (*Weber* at §79). This constitutes a "*separate interference with the applicants' rights under Art.8*" (e.g. *Weber*, at §78; see also the CJEU in *Watson §§100-101*).

54. Second, the Government's access to content and communications data intercepted by other countries' intelligence agencies, as well as its storage, analysis, use and dissemination also constitutes an interference with an individual's private life: e.g. *Hewitt & Harman* at §§34-35; *Liberty* at §56.

General principles established in the Court's case-law

55. The requirement that any interference with private life must be in "*accordance with the law*" under Article 8(2) will only be met where three conditions are satisfied: (i) the measure must have some basis in domestic law (ii) the domestic law must be compatible with the rule of law, i.e. the law must have a sufficient quality such as to be accessible and foreseeable to affected persons and (iii) there must be adequate and effective guarantees against abuse (*Klass*, §§43-44 and 50; *Malone*, §66; *Weber*, §84; *Gillan and Quinton v UK* (2010) 50 EHRR 45, §§76-77).

Sufficient basis in domestic law

56. Article 8 requires that a measure which intrudes on privacy is permitted by domestic law: *Malone*, §§66, 68 and 79 (see also *Liberty*, §59; *Kennedy* §151). In *MM v United Kingdom*, App. No. 24029/07 13 November 2012 at §194, the Court recognised that in *Khan*, Article 8 had been violated *"because there existed no statutory system to regulate the use* [of covert listening devices] *and the guidelines applicable at the relevant time were neither legally binding nor directly publicly accessible".*

Quality of the law: accessibility and foreseeability

57. The Court has identified two particular requirements as to the quality of the law: the law must be "*accessible to the person concerned and foreseeable as to its effects*" (*Zakharov v Russia*, App. No. 47143/06, 4 December 2015 *("Zakharov")*, §228). In *Telegraaf Media Nederland Landelijke Media BV and others v Netherlands*

("Telegraaf Media"), App. No. 39315/06, 22 November 2012 (at §90), the Court clarified that for the law to be accessible to the person(s) concerned, it

> "must indicate the scope of any … discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference"

See also, *Weber*, §§93-95 and 145; *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, §76, ECHR 2006-VII; *Liberty*, §§62-63; *Kennedy*, §152.

58. In *Liberty*, the Court considered the analogous provision to s.8(4) RIPA, under s.3(2) ICA relating to "*external*" communications which applied before RIPA came into effect (described in the Court's judgment at §§22-27). Those provisions were in materially identical terms to RIPA and in two respects were more protective.[8]

59. The Court nonetheless held that the provisions of the ICA relating to interception of "*external*" communications were insufficient to comply with Article 8. It noted that the power to intercept "*external*" communications contained in s.3(2) (now RIPA s.8(4)) "*allowed the executive an extremely broad discretion*" (at §§64-65). Thus, any person who sent or received any form of telecommunication outside the British Islands could have such communication intercepted. The discretion granted was, therefore, "*virtually unfettered*". The same reasoning applies to the defects in s.8(4) RIPA.

60. As to foreseeability, the Court has clarified that in this context, this goes to the foreseeability of the system of rules and the scope of the discretion which they confer:

> "in the special context of secret measures of surveillance, such as the interception of communications, [this] cannot mean that an individual should be

---

[8] Section 3(3) ICA provided that an external interception warrant could not specify an address in the British Islands for the purposes of including communications to or from that address in the certified material, unless,

"*(a) [T]he Secretary of State considers that the examination of communications sent to or from that address is necessary for the purpose of preventing or detecting acts of terrorism; and*

(b) communications sent to or from that address are included in the certified material only in so far as they are sent within such a period, not exceeding three months, as is specified in the certificate."

The maximum period that such material could be examined was three months (rather than six months) in national security cases.

> able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly […] However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident […such that it is] essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated.
>
> […]
>
> it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference"

(*Weber* at §§93-94. See also *Liberty* at §62; *Zakharov* at §229).

61. In *Liberty*, the Court emphasised that these principles apply to "*general programmes of surveillance*" in the same way as to measures of surveillance "*targeted at specific individuals or addresses*" (at §63). In finding a violation of Article 8, it held that:

> "66. … According to the Government … there were at the relevant time internal regulations, manuals and instructions applying to the processes of selection for examination, dissemination and storage of intercepted material, which provided a safeguard against abuse of power. The Court observes, however, that details of these "arrangements" made under section 6 were not contained in legislation or otherwise made available to the public.
>
> 67. […] the Court recalls its above case-law to the effect that 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."

Quality of law: Guarantees against abuse

62. The Court has developed the following "*minimum standards*" that should be set out in "*statute law*" as "*clear, detailed rules*", rather than internal or other forms of law in order to ensure that the law provides sufficient guarantees against abuse; (i) the nature of the offences which may give rise to an interception should be identified; (ii) the law should provide a definition of the categories of people liable to have their communications intercepted; (iii) there should be a limit on the duration of interception; (iv) the procedure to be followed for examining, using and storing the data obtained; (v) the precautions to be taken when communicating the data to other parties; and (vi) the circumstances in which communications must be destroyed must satisfy the quality of law requirements. See *Weber* at §§92 and 95. See also *Huvig v*

France (1990) 12 EHRR 528; *Amann* §§56-59 and 76-80; *MM v United Kingdom* §195.

63. In *Zakharov*, the Grand Chamber of the ECtHR recently re-iterated its well-established case-law regarding surveillance measures (§§227-232). It held that the security interests on which the State could rely under national law were too wide, rendering the legal framework unforeseeable (§§246-248), and identified the risk of "*automatic storage of clearly irrelevant data*" (at §§255 and 302).

64. In *Szabó and Vissy v Hungary (App. No. 37138/14)*, the Court also raised concerns about the use of widespread surveillance operations, which could amount to "*unfettered executive power intruding into citizens' private spheres*" (at §68). The Fourth Section noted the "*remarkable progress*" in the scale and sophistication of surveillance technology in recent years, which have "*reached a level of sophistication which is hardly conceivable for the average citizen, especially when automated and systemic data collection is technically possible and becomes widespread*" (§68). It called for the "*simultaneous development of legal safeguards securing respect for citizens' Convention rights*", making specific reference to the case-law of the CJEU and the views of the European Parliament (§§68 and 70).

Judicial oversight

65. The Court reaffirmed in *Telegraaf Media* (at §98) that, "*[i]n a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge*". Similarly, in *Kopp v Switzerland* (1998) 27 EHRR 91, the Court expressed its astonishment that the tapping of a lawyer's telephone was "*assigned to an official of the Post Office's legal department… a member of the executive, without supervision by an independent judge, especially in this sensitive area of the confidential relations between a lawyer and his clients, which directly concern the rights of defence*" (at §§73-75).

66. In *Zakharov*, it emphasised that "*it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure*", provided the scope of that control was wide

enough and effective to provide scrutiny of the relevant powers (at §§233, 249 and 258-261; see also *Szabó*, §§75-79).

Additional safeguards

67. In *Zakharov,* the Grand Chamber emphasised that the authority responsible for authorising interception "*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 and 263).

68. In *Szabó,* the Court identified the requirement for "*subsequent notification of surveillance measures*" to the person affected as *"inextricably linked to the effectiveness of remedies and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for any recourse by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their justification retrospectively*" (§86) (see also the CJEU in *Watson,* §121).

B. Article 6 of the Convention

69. The Court has stressed that the concept of "*civil rights and obligations*" bears an autonomous meaning, which "*should not be construed too technically*" and "*should be given a substantive rather than a formal meaning*" (*Le Compte, Van Leuve and De Meyere v. Belgium*, 23 June 1981, Series A no. 43, §45). In this regard, "*the character of the legislation which governs how the matter is to be determined (civil, commercial, administrative law and so on) and that of the authority which is invested with jurisdiction in the matter (ordinary court, administrative body and so forth) are therefore of little consequence*" (*Micallef v. Malta* [GC], App. No. 17056/06, §74).

70. In assessing the scope of Article 6(1) it is "*incumbent on the Court to review whether, in the light of changed attitudes in society as to the legal protection that falls to be accorded to individuals in their relations with the State, the scope of Article 6§1 should not be extended*" to cover new categories of legal disputes against public authorities (*Ferazzini v Italy,* App. No. 44759/98, §26). The need for a progressive

interpretation of the scope of Article 6(1) is particularly important where, as here, major advances in surveillance technology and the corresponding change in public attitudes to state surveillance both increase the need for independent and impartial judicial scrutiny of disputes concerning interferences with protected privacy interests. To engage the civil limb of Article 6(1), there must be a "*genuine and serious*" dispute about the existence, scope or manner of exercise of a right recognised under domestic law, and the proceedings must be "*directly decisive for the right*" (see *Mennito v. Italy* [GC], App. No. 33804/96, §23).

C. Article 10 of the Convention

71. Where an NGO is involved in matters of public interest it is exercising a role as a public watchdog of similar importance to that of the press, and therefore warrants similar protections to those afforded to the press. As the Court itself has noted:

> "The function of the press includes the creation of forums for public debate. However, the realisation of this function is not limited to the media or professional journalists. In the present case, the preparation of the forum of public debate was conducted by a non-governmental organisation. The purpose of the applicant's activities can therefore be said to have been an essential element of informed public debate. The Court has repeatedly recognised civil society's important contribution to the discussion of public affairs (see, for example, Steel and Morris v. the United Kingdom (no. 68416/01, § 89, ECHR 2005-II). The applicant is an association involved in human rights litigation with various objectives, including the protection of freedom of information. It may therefore be characterised, like the press, as a social "watchdog" (see Riolo v. Italy, no. 42211/07, § 63, 17 July 2008; Vides Aizsardzības Klubs v. Latvia, no. 57829/00, § 42, 27 May 2004). In these circumstances, the Court is satisfied that its activities warrant similar Convention protection to that afforded to the press." (*Társaság A Szabadságjogokért Hungary*, 37374/05, 14 April 2009, §27. See also *Guseva v Bulgaria* App. No. 6987/07, 17 Feb 2015, §38; *Animal Defenders International v. the United Kingdom*, no. 48876/08, 22 April 2013, § 103)"

72. The Court has repeatedly emphasised that the protection of journalistic sources and confidential journalistic material is an important guarantee afforded by the right to free expression. In the specific context of secret state surveillance of journalists, the Court reaffirmed in *Weber*, §143 that:

> "[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 Utigevers BV v Netherlands* [GC] (2010) 51 EHRR 31 at §50) [9]

73. The concept of a journalistic source material has been given a very broad definition by the Court (something not reflected in the applicable Codes of Practice currently in force in the United Kingdom as explained below). In *Telegraaf Media* (at §86) 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*"".

74. Article 10 imposes additional and more exacting requirements where an interference gives rise to a significant risk of revealing journalistic sources or confidential journalistic material (see the submissions below). However, it suffices to note that (a) surveillance measures which run a significant risk of identifying journalistic source information must be justified by an "*overriding public interest*" (*Goodwin v United Kingdom* (1996) 22 EHRR. 123 at §39; *Sanoma* (§§51 and 90)); (b) in such cases, authorisation can only be granted by a judge or other independent adjudicative body, which must be independent of the executive and any other interested party (*Sanoma,* §90–91). Authorisation must be *ex ante*, and full information must be disclosed to the adjudicative body to enable it to weight and balance the interests at stake (*ibid.*, §92). "*Clear criteria*" must govern the exercise of the adjudicative body's discretion, ***including*** whether there are "*less restrictive means*" of pursuing the "*overriding public interest in question*". The Judge must be empowered to refuse or limit the order sought. Information barriers are required to protect privileged information when obtained **and** where (exceptionally) such information is retained

---

[9] The Applicants note that the role played by human rights organisations – such as the Applicants – is similar to the watchdog role of the press. (*Társaság a Szabadságjogokért* v. Hungary (2011) 53 EHRR 3, §27). See further and more recently the decision of the Grand Chamber in *Magyar Helsinki Bizottság v. Hungary* [GC], App. No. 18030/11, 8 November 2016, §§166-167.

(*ibid*. See, by analogy, *Wieser and Bicos Beteiligungen GmbH v. Austria*, (2008) 46 EHRR 54 (§§62-65)).

D. Article 14 of the Convention

75. Article 14 prohibits both direct and indirect discrimination on various grounds including nationality and "*other status*". Discrimination based on whether or not a person is located in a particular jurisdiction is likely to lead to indirect discrimination on grounds of nationality. Differential treatment based on place of residence is in any event discrimination on the ground of "*other status*", subject to justification (*Carson v United Kingdom*, App. No. 42184/05, §70).

76. Discrimination "*means treating differently, without an objective and reasonable justification, persons in relevantly similar situations*." Discrimination does not need to be intentional in order to engage Article 14 since "*a general policy or measure that has disproportionately prejudicial effects on a particular group may be considered discriminatory notwithstanding that it is not specifically aimed at that group*." (*D.H. and Others v Czech Republic*, App. No. 57325/00, §175).

77. A difference of treatment will violate Article 14 if it has no objective and reasonable justification; in other words, if it does not pursue a legitimate aim or if there is not a reasonable relationship of proportionality between the means employed and the aim sought to be realised. (*J.M. v United Kingdom*, App. No 37060/06, §54). Once a relevant difference of treatment has been established, the burden is on the respondent Government to demonstrate that the measure giving rise to the differential treatment is justified (*Oršuš and others v Croatia* [GC], App. No. 15766/03, §150).

IV. FACTS

78. These Applications arise from disclosures to the press by Edward Snowden, the former contractor for the United States ("**US**") National Security Agency ("**NSA**"), and express public avowals of the relevant surveillance programmes.[10]

[10] See *[BBWApp/19]; [BIJApp/21]; [10OrgApp/(additional submissions/5)]*.

79. Since the preparation of the Statement of Facts in each of the three Applications, new factual information has been published. This is summarised in the Factual Appendix to the 10Org Reply to the UK's Observations **[CB/51]**, to which the Applicants refer the Court.

80. In summary:

80.1. The UK Government intercepts communications and communications data passing along submarine fibre-optic cables passing through, into and out of the UK. Given the UK's geographical position, much internet data from across the world passes through the UK. The Intelligence and Security Committee of Parliament ("**ISC**") has confirmed that "*GCHQ* […] *has access to communications as they move over the internet via major internet cables*."[11]

80.2. The US Government carries out similar operations and shares data obtained through those operations with the UK.

81. The intercepted data is then processed and stored. The techniques used are powerful and intrusive:

81.1. 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"*.

81.2. Black Hole is a repository, which contains internet data "*collected by GCHQ as part of bulk 'unselected' surveillance*." 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

---

11 Report published on 25 November 2014 into the distinct issue of the murder of Fusilier Lee Rigby **[CB/46]**.

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*."

81.3. A 2011 GCHQ PowerPoint presentation further describes GCHQ's development of "*unprecedented' techniques to perform… 'population-scale' data mining, monitoring all communications across entire countries in an effort to detect patterns or behaviours deemed suspicious*." *[Factual appendix to 10OrgReply/7]*.

81.4. 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 to 10OrgReply/8]*.

81.5. By 2011, GCHQ also operated a rolling buffer, known as TEMPORA, which stored the bulk data it intercepted, regardless of whether there was any ground for suspicion ("*We keep the full sessions for 3 working days and the metadata for 30 days for you to query")*. In effect, everyone's data transmitted on the internet was stored, to enable GCHQ to go back and review it.

81.6. Under the programme OPTIC NERVE, GCHQ collected and stored an image from every Yahoo! Chat user's webcam every 5 minutes ("*does not select but simply collects in bulk, and as a trade-off only collects an image every 5 minutes*"). 1.8 million Yahoo! users were affected. GCHQ's internal documents record that around 7% of the images were intimate and explicit.

82. The technical process of 'bulk interception' can be divided into stages. At each stage, there is a substantial interference with the privacy of communications and private life, which must be justified under Article 8(2) and to which the minimum safeguards identified in the Court's case law apply:

82.1. **Interception** – The first step is to obtain a signal from a source and to transmit it to a GCHQ processing facility. Fibre optic cables are tapped and all of the data flowing over the cables are copied to GCHQ's computers.

82.2. **Extraction** – The intercepted signals are then converted into a digital stream so that the data can be reconstructed into an intelligible format.

82.3. **Filtering** – The data can then be filtered, usually near real-time or shortly after interception. Some low value internet traffic may be discarded, such as the content of video streaming from commercial providers. Information of potential interest may be selected at this stage through the use of a database of identifiers or selectors.

82.4. **Storage** – Information is retained in a database for potential future analysis or dissemination. The documents disclosed by Edward Snowden, indicate that the majority of the information stored is not of any legitimate intelligence interest, but rather data are stored in bulk (see the discussion of TEMPORA, KARMA POLICE, BLACK HOLE and OPTIC NERVE above and *[Factual appendix to 10OrgReply/4-9]*).

82.5. **Analysis** – Once held in databases, there can then be further querying, examining or data-mining of the information.

82.6. **Dissemination** – The product of the intercept may then be shared with or distributed to other persons, organisations or agencies. Sharing can also occur in earlier stages of the interception process, for example, by providing foreign agencies access to entire databases, which may store raw intercept material.

Storage of data – arrangements and duration

83. As to storage of data from intercept, the UK Government's disclosure has provided some information to the Court as to arrangements and duration:

83.1. The UKIS who receive "*intercepted material*" and related communications data under a s.8(4) warrant "*have internal "arrangements" that require a record to be created, explaining why access to the analysed intercepted material is required*" before a person is able to access the "*intercepted material*" pursuant to s.16 RIPA. However, the internal "*arrangements"* only impose a requirement to keep a record of some kind: they do not specify what must be recorded as to the use made of such material. There is no requirement for any judicial or independent authorisation. These "*arrangements"* only

apply before a person can gain access to "*intercepted material"*. But in domestic law, "*intercepted material*" is not all material intercepted under a s.8(4) warrant: it 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 supplied). The internal arrangements therefore do not apply if what is to be examined is communications data, including e.g. information about the identity of a person making a communication and who received it, the location of the communication, information about the device used, its operating system and hardware, or the identity of websites visited (etc) (all of which is not content data).[12]

83.2. The "*internal "arrangements"*" specify, or require to be determined, maximum retention periods for different categories of data – including both "*intercepted material*" (content) and communications data – in order to "*reflect the nature and intrusiveness of the particular data at issue*". However, the internal arrangements, the retention periods and the criteria of intrusiveness are not disclosed; save that the retention periods are said to be "*normally no longer*" than a maximum of 2 years and "*may be*" significantly shorter. The effect of these "*arrangements*" is that everyone's data may be intercepted in bulk and held by the UKIS for a substantial period, apparently two years in most cases.

A Bulk interception and collection of "internal" communications

84. The Interception of Communications Code of Practice (2007) **[CB/30]** states at §5.1 that "*external*" communications, *"do not include communications both sent and received in the British Islands, even if they pass outside the British Islands en route"*. [13] But this assurance given to Parliament makes no practical difference when applied to modern internet communications. Section 5(6)(a) of RIPA permits conduct "*necessary to undertake in order to do what is expressly authorised or required by the warrant*". It is not possible to distinguish between "*internal*" and "*external*" communications at the point of interception.

---

13 The same statement is also included in the amended the 2016 Interception Code at §6.5.

Expansive definition of "external communications"

85. In his evidence to the IPT, Mr Charles Farr (the Director General of the Office for Security and Counter Terrorism of the UK Home Office) explained for the first time, that the UK Government and its intelligence agencies and law enforcement bodies also adopt a very broad understanding of "*external communications*" **[CB/9]**. Such communications are treated as the legitimate object of a s.8(4) warrant by the UK Government, thus expanding the potential scope of such warrants and rendering the notional protections for internal communications in s.8(1) and (2) effectively meaningless (see §§23-26 above & §§101, 110 below).

86. Mr Farr sets out the UK Government's view that a person in the UK engages in an "*external*" communication when they conduct a Google search on their internet browser, use YouTube, post an item on a Facebook page (including their own) or use Twitter. The reason for this, he states, is that such actions are in substance communications between the user and the web servers of those companies, and they will constitute "*external*" communications when such companies' servers are based overseas.

87. This explanation reinforces the Applicants' submission that the scope of the UK's bulk interception regime is far further reaching than had previously been appreciated, even by expert commentators.[14]

B Intelligence Sharing

See [BBWApp/31-40]; [BBWUpdate/34-64]; [10OrgApp/(additional submissions)/70-73]; [10OrgReply/63-77, 226-227]

88. The UKIS is able to, and does, access substantial intelligence obtained by intercept from security services in other States.

89. The UK's most important intelligence sharing relationship is with the so-called "*Five Eyes*" countries: the USA, UK, Canada, Australia and New Zealand. The "*Five*

[14] See the Witness Statement of Dr Ian Brown in the IPT proceedings, §4 **[CB/4]**.

Eyes" agreement envisages and provides for the broad and reciprocal access to the fruits of the surveillance of communications by each member of the group.

C Other developments concerning bulk interception

90. The Applicants also emphasise the range of international and regional bodies (often specifically responsible for enforcing international privacy standards), which have expressed concern regarding the acts of the UKIS which are the subject of these Applications. Many have also concluded that the indiscriminate and vast nature of the UKIS' surveillance is not justified or proportionate:

90.1. On 18 December 2013, the UN General Assembly ("**UNGA**") adopted Resolution 68/167 (A/RES/68/167) on the right to privacy in the digital age[15], which expressed deep concern for "*the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights*"

90.2. Similarly, on 12 March 2014, the EU Parliament adopted a resolution on US surveillance programmes[16], surveillance bodies in various Member States and their impact on EU citizens' fundamental rights as well as on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)). The Parliament identified the UK programme as a "[…] *far-reaching, complex and highly technologically advanced system* […] *to collect, store and analyse communication data, including content data, location data and metadata of all citizens around the world, on an unprecedented scale and in an indiscriminate and non-suspicion-based manner*" which was "*incompatible*

---

15 UNGA Resolution, *The right to privacy in the digital age*, 21 January 2014 A/RES/68/167 http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167. See also UN Human Rights Committee Resolution A/C.3/69/L.26/Rev.1 dated 26.11.14, *The right to privacy in the digital age*.

16 European Parliament Resolution 2013/2188(INI), *US NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*, 12 March 2014, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0230&language=EN&ring=A7-2014-0139#ref_1_7

with the principles of necessity and proportionality in a democratic society" (Main Findings §§1, 4 and 5).

90.3. On 10 April 2014, an EU Data Protection Working Party, set up under Article 29 of EU Directive 95/46/EC as an independent European advisory body on data protection and privacy ("**the EU Working Party**"), published its "*Opinion 2014 on surveillance of electronic communications for intelligence and national security purposes*"[17], stating inter alia that: "*the Working Party concludes that secret, massive and indiscriminate surveillance programs are incompatible with our fundamental laws and cannot be justified by the fight against terrorism or other important threats to national security. Restrictions to the fundamental rights of all citizens could only be accepted if the measure is strictly necessary and proportionate in a democratic society*" (p.1).

90.4. At the request of the UNGA (UN GA Res. 68/167), the Office of the UN High Commissioner for Human Rights ("**UNHCHR"**) reported on these matters in a report published on 30 June 2014 (*"The right to privacy in the digital age*" A/HRC/37) **[CB/45]**. The UNHCHR noted that "*the onus is on the Government to demonstrate that interference is both necessary and proportionate to the specific risk being addressed. Mass or "bulk" surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. In other words, it will not be enough that the measures are targeted to find certain needles in a haystack; the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate*" (at §25, p.9).

90.5. The UN Special Rapporteur on Terrorism shared this view. In his fourth annual report dated 23 September 2014 (A/69/397)[18], he noted that "[t]*he communications of literally every Internet user are potentially open for*

---

17 Article 29 Data Protection Working Party, *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*, 10 April 2014, http://statewatch.org/news/2014/apr/eu-art-29-dp-wp-215.pdf

18 *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, 23 September 2014 A/69/397, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement

inspection by intelligence and law enforcement agencies in the States concerned. This amounts to a systematic interference with the right to respect for the privacy of communications, and requires a correspondingly compelling justification" (at §9, p.4). The Special Rapporteur concluded that "[t]*he hard truth is that the use of mass surveillance technology effectively does away with the right to privacy of communications on the Internet altogether*" (at §12, p.5). In short, "*mass surveillance of digital content and communications data presents a serious challenge to an established norm of international law*" (at §18, p.7). He also emphasised that "[s]*ince there is no opportunity for an individualized proportionality assessment to be undertaken prior to these measures being employed, such programmes also appear to undermine the very essence of the right to privacy*." (at §52, p.19)

90.6. In December 2014, the Council of Europe's Commissioner for Human Rights ("**the CoE Commissioner**") published an Issues paper ("*The rule of law on the internet and in the wider digital world*")[19], in which he concluded that "[u]*ntil the rules are known under which the agencies and services operate – domestically, extraterritorially or in co-operation with each other – their activities cannot be said to be in accordance with the rule of law. Another matter of serious concern is the manifest ineffectiveness of many supervisory systems*. (p.19)

90.7. On 21 April 2015, the Parliamentary Assembly of the Council of Europe passed Resolution 2045[20] which called upon member states, *inter alia* to ensure that "*their national laws only allow for the collection and analysis of personal data (including so-called metadata) with the consent of the person concerned or following a court order granted on the basis of reasonable suspicion of the target being involved in criminal activity*" (§19.1).

---

19 Council of Europe Commissioner for Human Rights, Issue Paper, *The rule of law on the internet and in the wider digital world*, December 2014, https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/70114_Rule%20of%20Law%20on%20the%20Internet_web.pdf

20 Parliamentary Assembly, Council of Europe, Resolution 2045, *Mass Surveillance*, 21 April 2015, http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=21692

V. Q3: BULK INTERCEPTION & INTELLIGENCE SHARING BREACHES THE CONVENTION

Question 3 from the Court:

In the event that the application is not inadmissible on grounds of non-exhaustion of domestic remedies, are the acts of the United Kingdom intelligence services in relation to:

a. the soliciting, receipt, search, analysis, dissemination, storage and destruction of interception data obtained by the intelligence services of other States;

b. their own interception, search, analysis, dissemination, storage and destruction of interception data in respect of "external" communications (where at least one party is outside the British Isles); and/or

c. their own interception, search, analysis, dissemination, storage and destruction of interception data in respect of "communications data"

"in accordance with the law" and "necessary in a democratic society" within the meaning of Article 8 and/or Article 10 of the Convention?

A Summary

91. In relation to bulk interception of content and communications data:

91.1. The *Weber* safeguards are the minimum required of any surveillance regime, including one which concerns the bulk or general interception of communications.

91.2. When the BBW and BIJ applications were made, the RIPA section 8(4) regime did not meet these requirements, because it did not provide a legal framework for the interception, storage and analysis of communications in ways which interfere with private life which is sufficiently clear and foreseeable to provide protection against conduct which is arbitrary or disproportionate. Notwithstanding what is now known by virtue of disclosures by the UKIS in the IPT process, these concerns remain; and s.16 RIPA does not assuage these concerns because it is insufficient and also applies only to analysis of content and not the building of detailed 'personal profiles' of individuals by intercepting, filtering, storing and analysing communications data.

91.3. In addition to the *Weber* safeguards, in the face of the substantial recent technological developments and capabilities of the UKIS, a regime such as that in RIPA s.8(4) must include (i) a requirement for objective evidence of

reasonable suspicion of a serious crime or conduct amounting to a specific threat to national security in relation to the persons for whom data is being sought (ii) prior independent judicial authorisation and (iii) notification to enable the affected persons to exercise their right to challenge the interception.

92. In relation to intelligence sharing:

92.1. As a minimum, the *Weber* safeguards which apply to direct surveillance also apply to intelligence sharing, and require oversight of any such access to, storage and use of data;[21]

92.2. Prior to the Disclosure in the IPT proceedings, the UK's legal regime did not sufficiently explain or identify the standards and arrangements which apply to the UKIS' receipt of the fruit of surveillance by foreign intelligence services. There was therefore no sufficient basis in law for the accessing, storing, analysing, disseminating or destroying of communications and communications data obtained by the intelligence services of other States;

92.3. Following that Disclosure, there are no provisions *in law* which govern the sharing of communications or communications data between the UKIS and foreign intelligence services. The only protections available are set out in a document, whose status is open to question and which may be altered by the UK Government at any time;

92.4. Further, in the face of the substantial recent technological developments and capabilities of intelligence services, the regime applied by the UKIS by analogy to the access to intelligence from foreign intelligence services must include (i) a requirement for objective evidence of reasonable suspicion of commission of a serious crime or conduct amounting to a specific threat to national security in relation to the persons for whom data is being sought; (ii) prior independent judicial authorisation; and (iii) notification to enable the affected persons to exercise their right to challenge the interference.

93. In the section below, the Applicants primarily address the Court's question in relation to the "*in accordance with law*" requirement of Articles 8 and 10 ECHR. However, for the reasons set out below, they also submit that the interferences with these rights caused by the UK regime are not "*necessary in a democratic society*", and do not satisfy the test of "*strict necessity*" recognised in the Court's case-law (*Klass*, §42; *Szabó* at §73).

B Q3(b)-(c): Bulk interception

See [BBWApp/140-178]; [BBWUpdate/6-72]; [BBWReply/10-29]; [BIJApp/109-125, 141-156 and 162-165] [BIJReply/26-37 and 46-90]; [10OrgApp/(additional submissions)/42-69]; [10OrgUpdate/1(2)-(3)]; [10OrgReply/127-220]

94. As noted above, Article 8 of the Convention requires that:

94.1. there be a sufficient basis in law for any interference with the right to private and family life ("**basis in law**");

94.2. domestic law should satisfy the "quality requirements" identified in the Court's case law, namely *accessibility and foreseeability* ("**quality of the law**"); and

94.3. there should be sufficient protections against arbitrariness, particularly in the context of secret surveillance regimes ("**guarantees against abuse**").

95. These requirements exist because secret surveillance is liable to lead to be abuse (*Klass*, §49; *Weber*, §§94-95; *Zakharov*, §229). The Independent Reviewer explained the importance of both safeguards and firm limits on the use of mass surveillance technology in his 2015 report **[CB/48]**:

> "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…" (A Question of Trust, §§13.18-13.21)

96. The Independent Reviewer's "*red lines*", as traced in the Court's case-law, have traditionally been the six minimum safeguards set out in *Weber*. In the modern world, these are necessary, but not sufficient to reflect the practical realities the Applicants

have highlighted above, or the scale of surveillance possible as increasingly mechanized tools are at the disposal of the UKIS.

97. Whether taken separately or together, for the reasons set out below the Applicants submit that the UK's statutory regime that applies to "*external"* communications is not compliant with Article 8 and 10. Faced with the technological realities in the present day, the traditional defects of the UK surveillance regimes reviewed by this Court are still present, and amplified in their potential impact on persons present within and outside Council of Europe States.

(1) Basis in Law

98. The Applicants accept that bulk interception by the UKIS has a legal basis in domestic law, but it, lacks the quality of law, because it is obscure and lacks sufficient guarantees against abuse. It has been variously described by:

98.1. the ISC as "*unnecessarily complicated*", "*difficult to understand*", and "*unnecessarily secretive*";[22]

98.2. the Independent Reviewer, as "*complex, fragmented and opaque*", and "*extraordinarily difficult to understand and apply*";[23] and

98.3. by RUSI as "*unclear*" and failing to "*serve either the government or members of the public satisfactorily*."[24]

99. This may be contrasted with the regime for intelligence sharing, which – as set out below – historically contained no provisions set out in the law, and currently relies only upon "*internal arrangements*" disclosed to the IPT in domestic proceedings.

---

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

23 A Question of Trust **[CB/48]**, §12.20

24 RUSI Report **[CB/49]** pp.xi-xii.

(2) Quality of the Law

100. The Applicants submit that the UK regime for bulk interception does not meet the quality of law requirements identified in the Court's case-law (set out at §§62-68 above) and repeatedly held to be absent from the UK's surveillance regime:

100.1. For instance, in *Malone,* the Court identified a violation of Article 8 because provisions in the legislation governing the Post Office were too "*obscure*", "*open to differing interpretations*" and lacking in clarity as to the "*scope and manner of exercise of the relevant discretion conferred on the public authorities"* (§79). This led to the introduction of the ICA in 1985.

100.2. In *Liberty,* the Court concluded that the basic legal framework established by the ICA remained too skeletal and allowed the executive a wide discretion as to the capture, listening and reading of communications (§§64-65 and 69). The Government also relied upon "*arrangements*" which were not contained in legislation or "*otherwise made available to the public*" (§66).

101. RIPA suffers from the same defects. As set out above, the universal view shared by domestic expert bodies is that it is so complex as to be inaccessible to the public and to the government. In particular, the Applicants identify three principal features of the regime which do not meet the quality of law requirements: (i) the reliance upon "*arrangements*" substantially "*below the waterline*" rather than clear and binding legal guidelines as to what is permitted; (ii) the combination of a lack of clear or principled definition of "*internal"* and "*external"* communications and the continuation of a notional distinction between them in the legislation, in the face of modern technological developments which render the distinction meaningless and (iii) reference to widely framed purposes for the granting of bulk interception warrants, in particular where this is said to be "*in the interests of national security*".

102. First, the key "*arrangements*" in relation to what are said to be safeguards against misuse of intercepted data under ss.15 and 16 remain secret and unavailable to the public. The UK Government relies upon a "*summary of the evidence*" of internal "*arrangements…below the waterline*" which were referred to only in a secret closed session of the IPT's proceedings, from which the public, the applicants and the

applicants' representatives were all excluded.[25] Such a concept has no basis in the Court's case law, and is analogous to the undisclosed "*arrangements*" criticised by the Court in *Liberty*. In that case, the Court went on to note (at §77) that:

> "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."

103. Disclosure to the tribunal only in closed proceedings before the IPT cannot contribute to the accessibility and foreseeability of the law for the public (and the government). Instead, the detail relating to the safeguards in the UK regime remains inaccessible. The Applicants emphasise that a statutory Code of Practice is substantially different from secret "*arrangements*" such as those on which the UK Government relies. As the Court noted in *Liberty* (at §§40 and 60), such a Code is a public, and it must be subject to consultation and approved by both Houses of the UK Parliament (s.71(9) RIPA).

104. In *Liberty*, the Court also pointed to the practice of publication of details concerning the operation of a scheme of external surveillance by the German authorities under the G10 Act and the UK authorities under RIPA as evidence that the quality of the law could be improved "*without compromising national security*" (§68). Indeed, since these proceedings started, and since the UK decided voluntarily to disclose some of UKIS's "*arrangements*" for handling data, relevant Codes of Practice have been revised. The Applicants do not accept that these revisions are sufficient to have the quality of law; but this does illustrate that the Codes at the relevant time were less accessible and foreseeable than they could have been.

105. There is an absence of legal safeguards on the transfer of data out of the UK or European Union by the UKIS. As noted above, the Government has issued certificates under s.28 of the DPA which exempt the UKIS from the eighth data

---

[25] The Applicants address the compatibility of this procedure with Article 6 of the Convention in response to QQ4-5 from the Court at §§173-197 below.

protection principle, which prevents the transfer of data outside the EEA without an adequate and equivalent level of protection on the use, storage and destruction of that data. In place of the statutory protections, internal documents apply to the transfer of such data which are unenforceable and open to amendment or repeal by the agency concerned.

106. Second, the distinction between "*internal*" and "*external*" communications in the RIPA scheme is unacceptably vague and has been overtaken by changing methods of communication since the introduction of that legislation:

106.1. Both the Government's statements during parliamentary debates on RIPA, and the relevant Code of Practice had expressly identified that (email) communications between persons in the UK but routed outside of the British Islands would be treated as "*internal*" communications;[26]

106.2. Members of the public were entitled to rely upon such statements regarding the scope of s.8(4) warrants.

107. However, during the course of the IPT proceedings, the Government made a contradictory statement as to what it regards as *"internal"* and "*external*" communication. It now says that the use of platforms that rely on servers outside the UK, including Facebook, Google or YouTube – even for communications between two persons present in the UK – is *"external"* not "*internal"* communication, so interception of it does not attract the protections of s.8(1) and (2) RIPA; it is permitted under a generic s.8(4) warrant *[UKBBWObs/6.73]*. This fundamentally alters the application and scope of the domestic legislation. 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.

108. This expansive interpretation is not accessible. At the same time, it remains unclear what other online services falls within the Government's definition of an "*external*" communication. For instance, the term "*platform*" appears nowhere in RIPA or in the Code of Practice.

---

[26] See Hansard, House of Lords Debates, 12 July 2000, Col 323 (Lord Bassam of Brighton) **[CB/39]**.

109. The UK's oversight bodies, such as the ISC, have 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*" (Annex A §O,p.113, ISC Report **[CB/47]**).

110. The Government rejects these conclusions. It submits to this Court that "*when a communication…is placed on a web-based platform such as Facebook or Twitter, the communications will be external if the server in question…is outside the British Islands*." *[UK10OrgObs/4.69]* But this is a meaningless distinction. Emails are placed on servers in the course of transmission and telephone calls are routed through exchanges. These are in principle no different from a modern communications "*platform*". Moreover, it was not until the proceedings before the IPT that the Government even publicly disclosed such a distinction – indeed, it is significant that the Government itself relies simply on its witness evidence in the IPT proceedings to describe the regime (e.g. *[UKBBWObs./1.42]*).

111. The Government also attempts to dismiss any confusion as irrelevant on the grounds that any distinction between "*internal*" and "*external*" is "*macro level*" guidance for the UKIS on which cables to tap *[UK10OrgObs/4.71-4.72]*. In other words, the Government asserts that such guidance is not meant to assist individuals in determining if their communications might be intercepted. Yet, the whole purpose of the foreseeability requirement is to allow the individual, who may be the subject of surveillance, to understand the conditions under which the Government may act to intercept communications. The legal rules must be "*sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered*" to intercept their communications (*Zakharov*, §229).

112. In response, the Government further asserts that clarification would be both "*impractical*" and "*pointless*" *[UK10OrgObs/4.69, note 140]*. It explains that, "[t]*he difficulty…is*…[that] *each time a new form of internet communication is invented, or at least popularised, the Code would need to be amended, published in draft, and*

laid before both House of Parliament, in order specifically to explain how the distinction applied to the particular type of communication at issue". The Government's response is contrary to the view of the ISC and demonstrates apparent indifference towards the importance of ensuring that there is a clear and accessible regime for interception. Convenience is not a good reason for an absence of foreseeability in a surveillance regime.

113. Third, whilst the Secretary of State is required to certify that he considers the examination of the material necessary for the purposes set out in s.5(3) RIPA, these purposes are extremely broad and provide only the most minimal restrictions: "*in the interests of national security*", for the "*purpose of preventing or detecting serious crime*", "*for the purpose of safeguarding the economic well-being of the United Kingdom*" or for preventing or detecting serious crime pursuant to an international mutual assistance agreement: s.8(4)(b)(ii). The concept of "*national security*", which is especially relevant to these Applications, is vague and unforeseeable in scope, particularly in light of recent developments in the threats posed to Council of Europe States:

113.1. The Applicants emphasise that the UK Government's conception of what constitutes a threat to national security has considerably broadened over time and includes, for instance, action taken to combat pandemics and energy security. For instance, the former Director General of the Security Service, Baroness Manningham-Buller, during recent parliamentary debates on the Justice and Security Bill noted that "*national security meant to us something pretty narrow following the Attlee instructions at the end of the war to the intelligence community* [...but more recently the Government had developed] *a national security strategy which was much broader and included things such as pandemics and added cyberthreats, energy security and so on and* […]*now ha*[d] *quite a long national security strategy that covers a wide range of issues*" *[BBWApplication, §111]*;

113.2. The UK courts have described the concept of national security as "*protean*" (*SSHD v Rehman* [2003] 1 A.C. 153, p.166G at §35 per Lord Woolf MR (Court of Appeal)). They have held that it overlaps with foreign policy and that there is a very large area of discretion for the Government to determine

what constitutes action that is in the interests of national security (ibid, p.192H-193B at §53 per Lord Hoffmann).

113.3. Likewise, the concept of *"terrorism"*, which is part of the concept of *"national security"* in domestic law (e.g. SSA 1998 s.1(2)), is itself extremely broad. It has no accepted definition in international law and the UK Supreme Court held that the concept in UK law[27] includes nationalist groups or freedom fighters engaged in lawful armed conflict, or even UK troops themselves (*R v Gul* [2014] AC 1260, pp.1288D-H §§59-62). Registering concerns at the breadth of the definition, the Supreme Court noted that it afforded *"what appears to be very broad discretion"* to police and immigration authorities bestowed with "*terrorism"* powers. The observation applies equally to the UKIS and the Secretaries of State exercising powers under RIPA: *"the fact that the powers are so unrestricted and the definition of "terrorism" is so wide means that such powers are probably of even more concern than the prosecutorial powers to which the [Terrorism] Act give rise"* (p. 1289A-B at §63). The breadth of powers legitimately exercised for terrorism purposes is vividly illustrated by the fact that the Court of Appeal upheld the stop, search and seizure powers exercised over David Miranda[28] for the purposes of determining whether he was or had been concerned in the *"commission, preparation or instigation of acts of terrorism"* (*R (Miranda)) v Home Secretary* [2016] 1 WLR 1505 **[CB/53]**). It was held that the power could legitimately be exercised on the basis that the basis that the confidential documents he possessed could have endangered life and that he may have been seeking to do so for a political and ideological cause. Such examples illustrate the striking breadth of the powers under RIPA that are exercisable for objectives of *"national security"*, including prevention of terrorism, and the chilling effect on journalistic activity.

---

27 Set out in s.1 of the Terrorism Act 2000.

28 Mr Miranda was the partner of the journalist Glenn Greenwald, responsible for a number of the Guardian newspaper stories based on the Snowden material.

113.4. Thus, the concept of national security as a matter of UK law is obscure, not defined in law or in policy, and its scope and application are vague and unforeseeable. In *Kennedy*, the Court held that the term "*national security*" had an understood meaning and, for instance, was used in the Convention itself. The Court relied upon on a definition of "*national security*" offered by the Interception of Communications Commissioner in his Annual Report for 1986 (at §33). However, the Communications Commissioner's definition (i) is not authoritative or binding and, (ii) is out of date and (iii) does not reflect the breadth of the concept as understood by the UK courts and government.

113.5. Although the concept of *"national security"* might not be capable of a comprehensive definition (*Esbester v United Kingdom* (1994) 18 EHHR CD72), it is nonetheless possible to define with far greater precision than is currently the case in RIPA the legitimate grounds for exercising different coercive surveillance powers. Given the breadth of the language used in the certificates accompanying s.8(4) pursuant to s.16 (as to which, see below), in practice no specificity is provided for under the UK regime. By contrast, in *Weber* §27, the Court noted the specific list of identified objectives for which surveillance powers could be exercised under German law (see §21 above).

113.6. The wide discretion that is afforded to public officials in determining whether the exercise of powers can be justified on grounds of national security also powerfully reinforces the need for protections against abuse, including *ex ante* judicial oversight of the use of the powers.

(3) Guarantees against Abuse

114. The Applicants also submit that the existing safeguards in the UK regime for bulk interception have become ineffective and are insufficient to guard against abuse, or to ensure that the interception of communications is proportionate in light of technological developments. These have led to both a difference in the scale and in the nature of the interception carried out by the UKIS:

114.1. Communications which would traditionally have been "*internal*" are now transmitted externally, outside the UK, based on technological developments rather than the intention or conduct of the user. No attempt is made to remove this material from the interception of "*external*" communications or to apply the regime and requirements for "*internal*" communications in such situations: to the contrary, the Government asserts that it must be collected in bulk under the "*external*" communications regime *[UKBBWObs/1.39-1.41]*; and

114.2. Although the intention behind the scheme of RIPA was not to "*authorise the interception of any internal communications beyond the irreducible minimum*" and the selection for examination of the content of communications was not "*in practice likely to catch many internal communications*",[29] this is no longer the case. As noted above, unlike in the *Weber* case, the bulk interception powers of the UKIS are liable to affect potentially all persons who use the internet. GCHQ not only has considerable resources but has also deployed them to, for example, create detailed profiles of individuals by cross-referencing pieces of communications data, such as IP addresses, user IDs and email addresses using the KARMA POLICE, Black Hole and MUTANT BROTH programmes (see *[Factual appendix to 10OrgReply/4-9]*).

115. Moreover, no protection is offered at all for the collection of communications data, despite the growing importance of this information. This has two particular features:

115.1. First, the certification requirement in s.16 RIPA does not apply to such data by virtue of the narrow definition of the concept of "*intercepted material*" in s.20 RIPA. Accordingly, communications data can be used and stored by the UKIS in bulk and analysed for any purpose, without being limited by the purposes in s.3 RIPA as specified in any accompanying s.8(4) certificates;

---

[29] See the written Parliamentary answer by Lord Bassam to Lord Phillips of Sudbury given on 4 July 2000 **[CB/39]** as to the operation of (what became) s.16(3) of RIPA.

115.2. Second, the additional safeguards for persons in the UK do not apply to communications data.

116. However, the picture which can be painted through the modern use of communications data is much richer and more intrusive than previous forms of interception: indeed, the ISC has recorded that it is the primary purpose of bulk intercept by the UKIS. In *Szabó*, the Court specifically noted 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*", which must "*be subjected to very close scrutiny both on the domestic level and under the Convention*" (at §70). The UNHCHR has stressed[30] that the distinction between the seriousness of interception of metadata and content is "*not persuasive*" and "*any capture of communications data is potentially an interference with privacy* […] *whether or not those data are subsequently consulted or used*". The mere fact of such capture may indeed have a "*potential chilling effect on rights, including those to free expression and association*" (§26, at p.9).[31] Finally, as noted above, in *Watson* the CJEU emphasised that communications data "*is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained"* (at §§98-99).

117. Despite the significance of this interference with private life, the safeguards against abuse applicable to "*internal*" communications are not extended to communications data.

118. The Applicants further submit that (a) even the *Weber* safeguards are not satisfied by the s.8(4) regime and (b) in any event, the vast technological changes and expanded interception capacity since *Weber* was decided mean that additional legal safeguards over the bulk interception and use of communications data are needed to ensure continued respect and protection for the privacy interests protected by Article 8 of the Convention.

---

30 In its report published on 30 June 2014, *"The right to privacy in the digital age*" (A/HRC/37) **[CB/45]**.

31 See also the report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson QC, UN doc. (A/69/397) at §55.

Absence of the Weber safeguards in the RIPA regime for interception of 'external' communications under s.8(4).

119. The Applicants consider each of the *Weber* safeguards in turn, below.

120. *Weber #1*: Nature of offences: As set out above, the purposes for which bulk interception is permitted (such as "*national security*" or the "*economic well-being of the UK")* are unacceptably vague, particularly in the context of bulk surveillance, and do not provide a reasonably clear limit on the scope of the UKIS' activities. Indeed, the ISC has reported that the Secretary of State has only ever issued a single certificate under s.16 RIPA, which is "*expressed in very general terms*" which is "*unnecessarily ambiguous*" and liable to "*be misinterpreted*". For example, the categories of information which GCHQ is authorised to obtain under bulk interception powers includes the undefined "*strategic environmental issues*". By contrast, in *Weber* the list identified in the German legislation was much more specific.

121. *Weber #2*: Categories of persons affected: any person is liable to have their communications intercepted under s.8(4), in particular as a result of the failure of the distinction between "*internal*" and "*external*" communications. The Government admits that the s.8(4) Regime "*may in principle authorise the interception of internal communications insofar as that is necessary in order to intercept the external communications*." *[UKBBWObs/33(2)]*. Whilst the Secretary of State is required to provide "*the descriptions of material the examination of which he considers necessary*" (s.8(4)(b)(i)), the ISC has reported that s.8(4) warrants are framed in generic terms. In effect, this means that a very high proportion of communications are being intercepted. Again, by contrast, the regime in *Weber* was clearer and focused on persons using "*catchwords capable of triggering an investigation into the dangers listed*" or "*foreign nationals or companies whose telephone connections could be monitored deliberately in order to avoid such dangers*" (§97).

122. *Weber #3*: Limits on duration: In practice, a s.8(4) warrant may continue indefinitely, under a system of rolling warrant renewals. By virtue of s.9(1)(a) and 9(6)(ab) RIPA, a standard warrant endorsed under the hand of the Secretary of State with a statement

"*that the issue of the warrant is believed to be necessary on grounds falling within section 5(3)(a) or (c)*", lasts for a period of six months. Without such a statement, it lasts 3 months (s.9(6)(c)). This can be renewed for further periods of six months (s.9(1)(b)) so long as the Secretary of State certifies that the warrant remains necessary. In reality, this is no control on bulk interception warrants under s. 8(4), which will always be renewed as they are not based on any particular individuals and specific threat, but rather on general threats to national security etc., and there is no limit to the number of times a warrant may be renewed.[32] As in the case of *Gillan* (at §81) the alleged statutory temporal restriction has failed, so that a "*rolling programme*" of indefinite authorisation is effectively in place.

123. *Weber #4*: examination, usage and storage of data: The procedure for filtering, storing and analysing intercepted material lacks adequate safeguards and gives rise to an unacceptable risk of arbitrary or disproportionate interference with Articles 8 and 10, for a number of reasons:

123.1. First, as reported by the ISC (see ISC Report §§145-146), the protections in s.16 extend only to the content of communications data, and do not extend to filtering, storage or analysis of "*related communications data*", which is itself capable of creating serious government intrusion into private life.

123.2. Second, the only s.16 certificate ever issued (noted at §120 above) purports to limit the use which could be made of content. However, the breadth of its terminology means that the certificate places no effective constraint on the scope of filtering and analysis of data.

123.3. Third, the safeguards in s.16 apply only to a limited range of persons: they apply only if a person to whom intercepted material is referable is known to be in UK and if the interception is directed at that person (rather than to the other side of communications, such as his/her associates). They do not apply to persons who are or even may be permanently or temporarily outside UK.

---

[32] See Statement of Dr Ian Brown §53 **[CB/4]**.

123.4. Fourth, the procedure makes no provision for the *ex post facto* notification of a surveillance subject of the fact of surveillance. Indeed, there is a statutory prohibition on disclosure that a person has been subject to interception.

123.5. Fifth, the s.16(3) procedure – which permits the Secretary of State to modify the safeguards of s.16 - is not equivalent to that which applies to a targeted, s.8(1) warrant. No guidance is given as to how the Secretary of State will assess the "*necessity*" of examination of material, and the ISC Report makes clear that the information provided by GCHQ to the Secretary of State for instance *"do*[es] *not cover all the categories of information that an 8(1) application would cover (for example, any expected collateral intrusion into the privacy of others, or why the intelligence sought cannot be obtained by less intrusive means)"* (ISC Report, §114).[33] By contrast to *Weber*, the UK regime applies no requirements for selectors to be specified in the certificate, or to be checked by oversight mechanisms (see the criticisms of the lack of oversight by Ministers or Commissioners of the "*selectors"* used by GCHQ in the ISC Report §§123-125).

124. The absence of effective oversight or approval of the filtering, storage and analysis of intercepted material is reflected by the third IPT judgment in June 2015 **[CB/16]**, which found that communications of one of the Applicants – the South African Legal Resources Centre – had initially been intercepted, extracted, filtered and stored as the relevant selection procedure was not followed (§15) **[CB/16]**. This would never have been discovered by audit or oversight if the Applicant had not brought a claim.

125. *Weber #5*: precautions for the communication of intercepted material: The Secretary of State is required to ensure that disclosure of material intercepted under s.8(4) RIPA "*is limited to the minimum that is necessary for the authorised purposes*" by virtue of s.15(2) RIPA. However, this is an ineffective safeguard. The authorised purposes, which are enumerated in s.15(4), are extremely wide and include situations where the information is or "*is likely to become*" necessary for any of the purposes

---

[33] See also the examples given by Dr Brown at §§40-42 and 52-55 of his statement **[CB/4]**, e.g. that the relevant descriptor could be that of "*all traffic passing along a specified cable running between the UK and the US*".

specified in s.5(3). Section 15 permits dissemination of intercepted material where there is a "*reasonable suspicion*" that an individual has committed or is likely to commit any criminal offence or to pose any sort of threat to national security (which is itself very widely defined).

126. Moreover, the s.15(2) limitation does not apply to dissemination of intercepted material to foreign authorities (s15(6)). The Independent Reviewer has noted, in this respect, that there is "*no statute or Code of Practice governing how exchanges [to foreign authorities] should be authorised or take place*" (A Question of Trust, §7.66 **[CB/48]**). In *Weber*, by contrast, the transfer of intercepted personal data to other authorities (e.g. public prosecutors, police etc.) under the G10 Act was only permitted if (a) it served the protection of an important legal interest; and (b) there was a "*sufficient factual basis*" for suspecting that criminal offences had been committed. In this respect, it was necessary to establish that "*specific facts aroused suspicion that offences listed in s. 3(3) had been committed*" (§§40, 44). In addition, decisions to transmit data to other authorities could only be taken by a staff member of the Federal Intelligence Service who was qualified to hold judicial office (§§37, 128). These requirements ensured that the person taking the decision "*was particularly well trained to verify whether the conditions for transmission were met*" (§§37, 128).

127. *Weber #6*: erasure and destruction of data – There are no effective or binding safeguards against disproportionate retention of intercepted data. The Government points to provisions in the Code of Practice which specify that retention periods "*should normally be no longer than 2 years*" *[UK10OrgObs/4.54]*. Yet the lack of effective safeguards to ensure the prompt destruction of intercepted material is reflected in facts disclosed – for the first time – in the Third IPT judgment **[CB/16]**. This recorded that the communications of another Applicant, Amnesty International, had been stored without the appropriate (automated) deletion procedures being followed (§14). Neither the UKIS themselves, nor the oversight and audit mechanisms under RIPA had detected this issue, and the affected person had not been notified of this breach of its rights. Indeed, Amnesty International – and no doubt other affected victims – would never have discovered that its data had been

retained at all, let alone for longer than the Code of Practice regarded as '*normal',* but for its litigation of the issue.

Additional safeguards: updating Weber

128. As noted above (§§60, 64), the Court has regularly recognised the need to adapt its jurisprudence to shifting realities and to technological advances. Technological changes to ways in which government *can* access and use private data mean that new legal safeguards are needed to ensure genuine and effective protection of Article 8 rights online. 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. In its *Kennedy* judgment the Court emphasised that the regime for "*internal*" communications under RIPA did not allow the "[i]*ndiscriminate capturing of vast amounts of communications*" (§160). The changes since *Kennedy* as to that which is now regarded by the government as "*external"* communication, and changes to bulk surveillance capability mean that the domestic regime as interpreted by the government *does* now permit the indiscriminate capture and analysis of vast amount of communications.

129. It is clear that the *Weber* safeguards are therefore now insufficient to ensure that communications surveillance regime is compatible with Article 8 and Article 10. The Applicants have identified a number of additional safeguards that are necessary to ensure that any legal framework for communications surveillance regime complies with the protections of the Convention:

129.1. The absence of any requirement for objective evidence of <u>reasonable suspicion</u> in relation to the persons for whom data is being sought, is incompatible with the requirements established in the Court's recent case law. In particular:

(a) Permitting bulk interception of communications without reasonable suspicion would be inconsistent with the Court's established case-law, including the maintenance of national databases of intimate personal data (as in *S and Marper* or in *MK v France*);

(b) The Grand Chamber has emphasised the importance of verification of a reasonable suspicion in *Zakharov* (at §§260 and 263). Similarly, in *Szabó,* albeit in reference to the necessity and proportionality evaluation, 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).

(c) In *Watson*, the CJEU proposed the need for "*objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities*" before it could be intercepted and used (§119).

In this context, the Court should be particularly mindful of the need to adopt a consistent and principled approach across all Council of Europe States: should it be compatible with the Convention for the UK to adopt such a broad surveillance regime, permitting it to intercept, store and analyse communications without individual suspicion, there is nothing to stop all Member States from doing so, effectively removing the private life protected by Article 8 throughout the Member States. Indeed, in light of the modern movement of communications, the same communication could be caught up in more than one secret surveillance regime.

129.2. Prior independent judicial authorisation: Only prior independent judicial authorisation of interception warrants could satisfy Article 8. At present, the approval of such warrants is a matter that is entirely within the province of the executive. In light of the "*rolling*" nature of the s.8(4) warrants and their reliance upon very general terminology, any oversight by the Secretary of State is of limited efficacy, and in any event, could not replace the critical role of the judge in deciding on the legality, strict necessity and proportionality of warrant requests. Moreover, as noted above, the ISC has reported that there is no control over the addition of new selectors or the obtaining of communications data, even in relation to persons in the UK, or

even where a specific target has been identified. The absence of prior judicial approval has received the disapproval of:

(a) This Court in *Szabó* (§§77 and 80) and *Zakharov* (§§249 and 266-267);

(b) The CJEU in *Watson* **[CB/57]** (§120); and

(c) A range of international and regional human rights bodies (set out in Section IV(C) above).

129.3. The existing oversight mechanisms are ineffective, as is best illustrated by the fact that they did not identify even the legal errors found by the IPT, or properly investigate any of the issues set out in these Applications until domestic proceedings were brought in the form of complaints about the UK regime.

129.4. Subsequent notification of the surveillance subject. Both this Court (in *Szabó* at §86) and the CJEU (in *Watson* at §121) have recognised the importance of this safeguard, to enable those persons 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. Such a system also has the support of international and national bodies.[34] It is of particular importance where – as under RIPA – no other effective remedies are provided. For instance, the IOCCO has no power to refer a case to the IPT for a remedy, and he is not permitted to notify the victim of any excessive or unlawful interception.

---

[34] See, e.g. the report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression in April 2013 (UN Doc. A/HRC/23/40 at §82; the CoE Commissioner's May 2016 Memorandum, CommDH (2016)20 at §25 and the Independent Reviewer's conclusions in "*A Question of Trust*" **[CB/48]**, §14.104.

(4) Additional considerations relevant to Article 10 ECHR

*See [BIJReply/38-45 and 82-90]; [10OrgApp/74-81]**;** **[**10OrgUpdate/31-35]; [10OrgReply/286-294]*

130. As noted above, where an NGO is involved in matters of public interest it is exercising a role as public watchdog of similar importance to that of the press and warrant similar protections to those afforded to the press (*Társaság A Szabadságjogokért Hungary*, 37374/05, 14 April 2009, para 27).[35]; see also the *OSCE Guidelines on the Protection of Human Rights Defenders:*

> "In addition to recognizing the particular professional needs of human rights defenders who are journalists or lawyers, participating States should also acknowledge the specific needs of other human rights defenders as regards the protection of their privacy rights, including the confidentiality of their communications, in order to protect their sources or the people whose rights they defend. This is particularly important for those whose sources, including witnesses and whistleblowers, face particular risks for providing information to them, as well as for those who work with people, including victims of trafficking or individuals leaving violent criminal or extremist groups, who are at heightened risk of attacks as a result of turning to human rights defenders for assistance."[36]

131. The protection afforded by Article 10 is therefore of critical importance to all the Applicants in this case. In circumstances in which the Applicants are in daily communication with sources, some of whom risk their lives by so communicating, the failure of the relevant legal framework to provide sufficient indication as to how their confidential material is liable to be treated by the intelligence services constitutes an additional respect in which the s8(4) regime is not in accordance with the law (see 10OrgReply/286-294).

132. The Applicants submit that the subjection of journalists' and human rights NGOs' privileged information to s8(4) surveillance or intelligence sharing is neither a necessary nor a proportionate restriction on their Article 10 rights. Both regimes put their respective public watchdog role and functions at risk by exerting a chilling

---

35 See also *Guseva v Bulgaria* App. No. 6987/07, 17 Feb 2015, §38; *Animal Defenders International v. the United Kingdom*, no. 48876/08, 22 April 2013, § 103.

36 §257, available at http://www.osce.org/odihr/guidelines-on-the-protection-of-human-rights-defenders?download=true

effect on them and those with whom they communicate. It also raises risks to the safety, well-being and life of victims of serious human rights violations that work with human rights NGOs and journalists.

133. The covert interception and inspection of journalists' and human rights organisations' private communications is particularly serious in light of the important role those organisations play in holding governments to account, including investigating human rights abuses, and providing confidential advice and support to the most marginalised and vulnerable groups in society. The chilling effect of such surveillance is therefore particularly acute.

134. As set out above (§§72-74), Article 10 imposes supplementary safeguards where there is a significant risk that surveillance measures may reveal confidential journalistic material, including the identity of sources (and, by analogy, other organisations playing a social "*watchdog*" function). The interception of material gathered through bulk surveillance under s.8(4) warrants is not attended by those required safeguards.

135. First, the scope of protection afforded to journalistic material by the Code of Practice on the Interception of Communications (and, as a result, the attendant safeguards) is much too narrow. The Code defines confidential journalistic material as including "*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*" (at §4.3). To the extent that this provision is intended to define journalistic sources or information identifying a source, it is clearly inconsistent with the Court's much broader definition of these concepts and the additional safeguards required (see *Telegraaf* at §86). As such the Code (even if followed) offers insufficient protection to journalistic material to comply with Article 10 ECHR.

136. Second, the regime does not, remotely, comply with the other strict requirements of Article 10 set out above (§§72-74) where surveillance measures may reveal journalistic source material.

137. Third, judicial authorisation is not required. The authorising official is not independent of the executive. Moreover, authorisation (as explained above) is not governed by clear criteria. In particular, there is no requirement in the 2016 Interception Code that journalistic source material may only be obtained where this would be in the overriding public interest.

C Q3(a): Intelligence sharing

See [BBWApp/119-139]; [BBWUpdate/73-85]; [BBWReply/30-37]; [10OrgApp/70-73]; [10OrgReply/221-250]

138. In its first judgment, the IPT concluded that prior to the disclosure made to it in those proceedings, the UK regime for intelligence sharing was unlawful, due to its lack of foreseeability. The UK Government now submits that following the publication of the Disclosure, the intelligence sharing regime is "*in accordance with law*" *[UKBBWObs/5.14-5.32]*. But even after the disclosure of internal "*arrangements below the waterline*" by the UKIS, there remains no basis in law for the intelligence sharing carried out by the UKIS, and certainly no regime which satisfies the Court's quality of law requirements.

139. The UK government submits that the *Weber* safeguards need only apply to interception by the respondent State itself *[UKBBWObs/5.39-5.40]*, apparently on the basis that interception by a third country constitutes a lesser interference with the private life of affected persons (see also *[UK10OrgObs/3.32]*).

140. However, the interference with the rights protected by Article 8 and/ Article 10 of the Convention is no less serious when a third State shares the intelligence with the respondent State than when the respondent State conducts the surveillance itself. A similar argument made by the UK was rejected by the Court in *R.E v UK*, Application no. 62498/11, (27 October 2015), when it held that "*the decisive factor 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*" (§130). If the degree of interference with privacy is similar to interception, it should be irrelevant how the interference with a person's private life has been technologically achieved: the *Weber* safeguards set out minimum requirements, to be enhanced as necessary in

light of *Szabó* and the development of modern surveillance practices. Indeed, as noted above, the UN Special Rapporteur (Terrorism) and the UN General Assembly's Third Committee appear to treat the *Weber* criteria as the relevant reference point.

(1) Basis in law

141. The access to, analysis, use and storage of data intercepted by foreign intelligence agencies do not have an adequate basis in UK law. As the Independent Reviewer put it, there is "*no statute or Code of Practice governing how exchanges* [to foreign authorities] *should be authorised or take place*" (A Question of Trust **[CB/48]**, §7.66).

142. In his statement to Parliament on 10 June 2013, the Foreign Secretary asserted that such a legal basis exists in domestic law. He said that "*any data obtained*" from third countries relating to UK nationals was subject to "*statutory controls and safeguards*", namely ss.15 and 16 of RIPA; the Human Rights Act 1998 ("**HRA**") **[CB/26]** and the ISA.

143. However, that statement was wrong. No domestic legislation in fact provides any adequate basis for the regulation of the exchange of information between intelligence agencies:

143.1. Sections 15 and 16 of RIPA have no application to data shared with foreign partners.

143.2. The SIS, GCHQ and the Security Service are afforded statutory powers by s.1 and s.3 ISA and s.1 SSA respectively to "*obtain and provide*" information, including to and from foreign intelligence services. However, the legal safeguards which attend those powers are very limited. There is no direct legal control on the purposes for which they may be used other than that the heads of the agencies are under duties to ensure that there are arrangements for securing that no information is obtained except insofar as "*necessary*" for purposes specified in s2(2)(a) and s4(2)(a) ISA and s.2 SSA respectively. This is a bare statutory power of a kind found to be inadequate in this context in *Malone* and *Liberty*. These purposes are so widely defined

as to place no meaningful limitation on the breadth of these powers and do not provide foreseeability as to the scope of the regime.

143.3. In short, safeguards relating to the access to foreign intelligence, are not statutory, and are relegated to unenforceable internal 'guidance'.

(2) Quality of the law

144. Further and in any event, the "*internal arrangements*" disclosed do not have the character or quality of law for the purposes of the Convention. They have all the defects of the s8(4) regime identified above:

144.1. As noted above, the concept of "*arrangements below the waterline*" is not one known to the Court's jurisprudence. Such arrangements are (i) established by the executive agency in question and are not democratically or independently established, (ii) a matter of internal policy and thus subject to change and a lower standard of enforceability through the courts, and (iii) not published or accessible, especially where - as here - only "*gists*" are supplied.

144.2. They were only disclosed as a result of this litigation: it is unclear whether the note of these arrangements is the actual policy, part of a policy, a summary of a policy or a summary of submissions made by the Government to the IPT in closed proceedings. It is also unclear whether it is binding or is simply a description of desirable practices. Finally, it is unclear who drafted or adopted the note (and under what legal authority) or who has the power to amend it.

144.3. Given the scale and seriousness of the potential interference with Convention rights through such intelligence sharing, it is notable that the "*arrangements*" are not binding. While this Court has previously given weight to Codes of Practice or to administrative practices which are sufficiently established and accessible (*Silver v United Kingdom* (1983) 5 E.H.R.R. 347 at §§88–89; *Kennedy* at §156), in the context of a bulk interception regime leading to "*indiscriminate capturing of vast amounts of communications*" the absence of binding rules adversely affects the quality of the law.

144.4. The note for the IPT is obscurely drafted. It speaks of the UK Intelligence Services making a "*request*" for "*intercepted communications (and associated communications data)*" or circumstances where they "*receive intercepted communications content or communications data.*" It is unclear, however, whether "*request*" or "*receipt*" cover all the scenarios where the UKIS may access material intercepted by foreign intelligence agencies, such as to raw initial intercept material that they may then extract, filter, store and analyse or to databases of intercept material that has already been extracted, filtered, stored and/or analysed by the foreign intelligence agency. In addition, the concepts of "*analysed*" and "*unanalysed*" are not defined or explained, and do not derive from statute.

144.5. The arrangements appear to provide no protection at all for communications data.

145. The inadequacy of the previous arrangements is made clear by the revision of the Code of Practice in January 2016. The publication of the revised Code confirms that there was no good national security 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. In any event, publication of the revised Code was insufficient to address the flaws in the UK regime, given that it applied the inadequate RIPA regime to the obtaining of data intercepted by a foreign government.

D Q3(a): BIJ's Challenge to Section 22 RIPA

See [BIJ Application/126-138, 157-161 and 162-165]; [BIJReply/91-119]

146. BIJ also challenges the regime enabling the obtaining of communications data by the UKIS via s.22, RIPA. This is permitted in a wide range of ill-defined circumstances and without proper safeguards for journalistically privileged information, in contravention of the requirements of Articles 8 and 10, ECHR. This is an issue of fundamental concern to BIJ and the UK's national media, as reflected in the interventions of the National Union of Journalists ("**NUJ**") and the Media Lawyers Association (whose members include all the major press and media outlets in the United Kingdom). Two examples will suffice:

146.1. The Metropolitan Police has admitted viewing the call records of journalists at *The Sun* newspaper to identify and punish sources (see NUJ Intervention (§21)). The IPT considered this case in *NGN Ltd v. Commissioner of Police for the Metropolis* [2015] UKIPTrib 14_176-H where it found (§111-112) that the s.22 regime did not contain effective safeguards to protect Article 10 rights where authorisation was granted to identify a journalist's sources. The IPT lacked power under s.8 HRA to grant a remedy to the applicants notwithstanding its finding that Article 10 had been contravened (§126).[37]

146.2. Communications data obtained under Chapter II RIPA was used to identify a journalist's source for a *Mail on Sunday* report of an offence committed by a member of Parliament (*see* NUJ Intervention (§21)).

147. The safeguards presently in place regarding the use of s. 22 by the UKIS are the same as those found to be ineffective by the IPT in *NGN* in respect of the police. Yet, given the secrecy with which they necessarily operate, it is all the more important that the UKIS's activities are properly regulated.

(1) The degree of interference through interception of communications data

148. Chapter II RIPA's legal framework (and attendant safeguards) are informed by a fundamental (but erroneous) premise: that the interception or obtaining of communications data is necessarily *less intrusive* than the interception of content. The UK adopts this position to justify the lack of safeguards in the s.22 regime *[UKBIJObs/274 and 281]*. This premise is, however, fundamentally misconceived insofar as journalism is concerned, for reasons explained at *[BIJReply//96–98]*. A single piece of communications data could reveal the identity of a journalist's source, his location and the institution to which he or she is attached. As explained above (and in the expert report of Professor Danezis **[CB/10]**), when aggregated and subject to modern data-mining technology, communications data can, by "jig-saw identification", reveal an enormous range of journalistically privileged information.

---

[37] As regards one of the applicants, the IPT found that s.22 itself had been contravened (as opposed to the Convention rights protected by the HRA) and so it was able to grant a declaratory remedy. Compensation was refused.

In *Watson*, the CJEU recognized that such data may be "*no less sensitive, having regard to the right to privacy, than the actual content of communications*" (§99).

(2) Quality of Law/Protection Against Arbitrariness

149. 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 cannot be compatible with Article 10 …unless it is justified by an overriding requirement in the public interest*" (*Sanoma*, §51). Importantly, the protection afforded by Article 10 does not merely extend to information which may tend to reveal a journalist's sources, but to other forms of journalistically confidential material (see *Nordisk Film & TV A/S*, Admissibility, Application no. 40485/02; *Telegraaf*, §86). The Court has repeatedly held that, given the fundamental importance of press freedom, any interference with journalistically privileged information and, in particular, the right to protect sources "*must be attended with legal procedural safeguards commensurate with the importance of the principle at stake*" (*Sanoma,* §88).

Absence of judicial authorisation / effective oversight

150. Communications data may be obtained by the UKIS pursuant to Chapter II without any form of judicial or quasi-judicial authorisation, even where the purpose or effect of this may be to reveal a journalistic source or other form of privileged information. In *Sanoma*, the Grand Chamber emphasised the "*vital importance*" of press freedom in a democratic society and that "[f]*irst and foremost among these safeguards is the guarantee of review by a judge or other independent and impartial decision-making body*" (§88). As noted above, it identified certain key requirements:

    150.1. First, a review must be *ex ante*: he Court regarded it as "*clear*" that "*an independent review that only takes place subsequent to the handing over of material capable of revealing such sources would undermine the very essence of the right to confidentiality*" (§91).

    150.2. Second, "[t]*he requisite review should be carried out* by a body separate from the executive and other interested parties, *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, emphasis added). In addition, the authorising body must not be an official or institution "*defending interests potentially incompatible with journalistic source protection*…" (§93). Self-certification by the UKIS is therefore impermissible.

150.3. Third, in reaching a decision, "*the full picture should be before the court*" (§90), which must "*be in a position to carry out* [the] *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*" (§92).

150.4. Fourth, 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).

150.5. Fifth, the additional safeguards identified in *Sanoma* are required in circumstances where information is obtained which "could" lead to the identification of a source (not merely where the intention is to obtain such information) (see e.g. §88, ("*could lead to their identification*"). Thus, *Sanoma* relates to both intentional *and* incidental intrusions into journalistic privilege.

151. The safeguards set out in Chapter II and the accompanying Code of Practice do not comply with these standards. Insofar as the UKIS are concerned, authorisation is not provided by a court. As an official within the UKIS, the Designated Person is not independent of the executive (or even the executive agency requesting the disclosure - the UKIS). The Designated Person's role will involve that official defending or pursuing interests potentially incompatible with the protection of journalistic sources. More problematic still is that, in various cases, the Code of Practice envisages that the Designated Person need not even be operationally independent of those officials who seek the information in the first instance, for instance, in situations of urgency or where required on national security grounds (see the 2015 Acquisition Code §3.12-3.13). Furthermore, even insofar as the Code requires the police to follow procedures set out in the Police and Criminal Evidence Act 1984,

this guidance only applies to applications made "*in order to identify the journalist's source*" (§3.78). These safeguards do not apply in respect of the incidental identification of a journalist's source.

Insufficiency of statutory safeguards

152. First, the scope of protection afforded to journalistically privileged information by the 2015 Acquisition Code is too narrow. That Code fails to recognize that communications data may be privileged, advising decision-makers as follows "*communications data is not subject to any form of professional privilege – the fact a communication took place does not disclose what was discussed, considered or advised*" (§3.72).

153. This is not accurate. As explained above, it is readily possible to infer a range of privileged matters from communications data using modern methods of data exploitation such as the subject-matter of a story under development, the role and expertise of persons being consulted in respect of the investigation (and the likely subject matter of discussions occurring). The potential for information to be used in this way is accentuated by the very broad definition of "*communications data*" adopted for purposes of RIPA (see the 2015 Acquisition Code **[CB/32]** §§2.14–2.23). Such data includes: the address or email address or the originator or recipient of a communication; both party's location as well as the frequency and duration of contacts. The failure of the Code of Practice to define the proper scope of journalistic privilege undermines the (limited) protection afforded.

154. Second, (and relatedly) given the risk of communications data being aggregated or exploited in a manner which may reveal information which is journalistically privileged, rigorous safeguards are necessary in respect of the handling and exploitation of such information. In particular, information barriers are essential to ensure that privileged information is, where necessary, identified and destroyed (or, separated and retention exceptionally authorized in accordance with proper procedures). The Court has recognized the need for such procedural safeguards (including information barriers or "Chinese Walls") to protect professional secrecy in other contexts:

154.1. By analogy, in *Wieser*, §§62-65, the Court found a violation of Article 8 where police searched documentary and electronic records of a law firm, failing to put in place arrangements to identify and isolate information which was professionally privileged.

154.2. The Grand Chamber adopted the same approach in respect of journalistic privilege in *Sanoma* (§92), observing that where privileged information was unavoidably obtained (in cases of urgency) "*a procedure should exist to identify and isolate, prior to the exploitation of the material by the authorities, information that could lead to the identification of sources from information that carries no such risk*".

155. Yet, neither the 2015 Acquisition Code nor the 2015 Code for the Retention of Communications Data (not in existence at the time of BIJ's original application) provides safeguards for the identification, isolation (and destruction) of journalistically privileged information inadvertently or incidentally obtained by the UKIS.

156. Third, Chapter II provides little by way of limitation as to the basis on which communications data can be obtained. Pursuant to s.22, a Designated Person may authorise obtaining an unspecified volume communications data (subject to an overall requirement of proportionality) where "*that person believes it is necessary*" on a broad range of grounds ranging from national security and the preventing disorder to "*the interests of public safety*" and "*public health*". Further:

156.1. As noted above, neither the "*general safeguards*" in s.15 nor the "*extra safeguards*" in s.16 apply to communications data obtained, including data obtained pursuant to s.22.

156.2. The requirements of s.6 RIPA, that an interception warrant must describe "*one person as the interception subject*" or a single set of premises as the subject (at least in respect of "*internal*" communications also do not apply to the s.22 regime. This increases the scope of privileged communications being incidentally obtained.

156.3. As regards the requirement of proportionality, this cannot compensate for a regime which lacks procedural safeguards which are required to protect against arbitrariness. Even proportionate obtaining of communications data will be unlawful where insufficient safeguards are in place to protect against misuse.

157. Finally, safeguards in respect of the handling and exploitation of communications data obtained under Chapter II are also unsatisfactory insofar as journalistically privileged information is concerned, not least given the increasingly sophisticated means of exploitation which now exist. In particular: (a) information barriers are absent, as described; (b) although a Designated Person should be informed of the overall "*purpose*" of acquisition under the 2015 Acquisition Code, there is no requirement that he or she be informed of the ***manner*** in which it is intended to exploit data. This inhibits his or her ability to reach an informed and independent view as to the risks of such use and the proportionality of this (especially given the modern techniques of exploitation discussed earlier and the degree of intrusion they potentially involve). This approach runs counter to that adopted in *Sanoma* (§90) which requires the "*full picture*" to be placed before the adjudicative body, when reaching a decision on whether to obtain data which may compromise journalistically privileged material; (c) once communications data is obtained there is little to prevent it being aggregated (with other similarly obtained data) and exploited in a manner which compromises the privileged status of information. This is particularly problematic in view of the broad bases on which authorisation for acquisition may be granted. Yet it is an issue not addressed in the 2015 Acquisition Code. There are no special safeguards for retained privileged information or as to how it may be used.

158. Taken collectively: the unduly narrow scope of protection afforded to journalistic confidentiality; the threadbare safeguards available fail to comply with Article 10.

(3) Lack of proportionality

159. The Chapter II regime permits disproportionate acquisition and retention of journalistically confidential information and disproportionately interferes with free

expression. The regime grants the UKIS access to journalists' communications data, with few limits or safeguards. The following features of the regime illustrate this:

159.1. The absence of a requirement for authorisation by a judge with guarantees of independence from the executive agencies seeking to obtain information which may reveal a journalistic source or other confidential information;

159.2. The very broadly-defined bases on which communications data can be obtained, taken with the absence of safeguards analogous to those set out in ss.8(1) and 8(2) RIPA. As a result, substantial volumes of communications data may be obtained, not meaningfully tailored to a specific purpose, including privileged information;

159.3. The absence of safeguards in respect of the incidental interception of journalistically privileged information and arrangements to ensure that its destruction;

159.4. The absence of additional safeguards in respect of the obtaining or retention of privileged information, including, information barriers;

159.5. The absence of precise criteria for indicating when communications data will be ***further analysed***. This does not ensure that communications data will be used only for targeted and sufficiently important purposes, in circumstances where any interferences with journalistic free expression is rigorously justified;

159.6. The absence of a requirement that the Designated Person be informed not merely of the "*purpose*" for which communications data is sought but as the manner in which such data will be exploited. Without this information, it will not be possible for the authorising official to independently determine the risk of confidential journalistic information being obtained and/or misused throughout the time the information is held, given the wide range of means by which such data can now be exploited.

160. Potential sources can have little confidence that they can communicate freely and confidentiality with a journalist, without the UKIS (or, indeed, other law

enforcement agencies) being able to identify them. Journalists themselves can have little confidence that their inquiries will remain confidential, until such time as they are published. These are vital confidences for a free press.

VI. OTHER QUESTIONS POSED BY THE COURT

In this Section, the Applicants expressly address the remaining questions posed by the Court in its letter dated 10 July 2017.

A. Q1: VICTIM STATUS

Question 1 from the Court: Can the applicants claim to be victims, within the meaning of Article 34 of the Convention, of the alleged violations?

See [BBWApp/10-17 and 115-116]; [BBWReply/43-44]; [BIJApp/11-20]; [BIJReply/24]; [10OrgApp/(additional submissions)/4]; [10OrgReply/78-81; 251-261]

161. The Applicants recall the Court's well-established case-law in the field of challenges to secret surveillance programmes. As the Court expressly stated in *Kennedy* (at §119, emphasis added):

> "… in recognition of the particular features of secret surveillance measures and the importance of ensuring effective control and supervision of them, the Court has permitted general challenges to the relevant legislative regime".

The Applicants do not therefore need to establish that their communications have actually been the subject of interception or that their information has otherwise been obtained by agencies of the UK Government. The Applicants also bring this claim on behalf of others affected by the surveillance of which they complain.

162. In the recent decision of the Grand Chamber in *Zakharov*, the Court emphasised the possibility of general challenges being be brought before the court in this context, subject to (i) the scope of the legislation in question being such that an applicant "*can possibly be affected by it*" and (ii) taking into account "*the availability of remedies at the national level*" (§§170-171).

163. The Applicants are clearly within the scope of the legislation given their activities. It is - at the lowest - possible that they may in fact have had their communications intercepted.[38]

164. Indeed, as the Court has acknowledged in Application Number 24960/15 (see Summary of Facts in Application 24960/15, §A(3)(d), p.9), the IPT has confirmed that two of the Applicants in that case have in fact had their communications unlawfully intercepted *[UKBBWObs/1.52; 10OrgUpdate/14-15; 10OrgReply/251-261]*.

B. Q2: EXHAUSTION OF DOMESTIC REMEDIES

Question 2 from the Court: If the applicants did not raise their Convention complaints before the Investigatory Powers Tribunal, have they done all that is required of them to exhaust domestic remedies?

See [BBWApp/179-190]; [BBWUpdate/86-88]; [BBWReply/38-42]; [BIJApp/7-10]; [BIJReply/20-23]

165. The Applicants in the 10 Human Rights NGOs application exhausted their domestic remedies before the IPT. This question is therefore academic and the Court can resolve the substantive issues before it without needing to consider this issue.

166. The Applicants in the BBW and BIJ applications did not file complaints before the IPT prior to lodging applications before this Court.[39] They did so in reliance upon this Court's case-law concluding that at the relevant time a claim before the IPT was not necessary in order for a general challenge to be brought against the UK's surveillance framework (*Kennedy* at §§109-110). The short answer to the Court's question is therefore that the BBW/BIJ Applicants did "*all that was required of them*" in terms of domestic remedies. What was required of them was spelt out by this Court in *Kennedy*. It will of course always be open to this court to reconsider

---

38 The Court is also referred to the witness statement of Ms. Ross **[CB/7]** and Mr Bochenek **[CB/6]**.

39 The first two Applicants in Application Number 58170/13 sought to bring a claim in relation to the receipt and use of information from foreign intelligence partners before the Administrative Court of England and Wales **[CB/41]**. The UK Government responded that the Applicants could not bring any complaint before the UK courts alleging a violation of Article 8 ECHR because the effect of s.65(2) of RIPA is to exclude the High Court's jurisdiction to hear complaints against UKIS under the HRA **[CB/44]**.

whether a domestic avenue of complaint provides an effective remedy, but it should do so only prospectively not retrospectively, and not to the detriment of applicants having relied upon its jurisprudence.

167. The BBW and BIJ applicants also relied upon the domestic case-law at the time identifying the shortcomings of the procedure before the IPT (see, e.g. *AJA & Ors v Commissioner of Police for the Metropolis & Ors* [2013] EWCA Civ 1342 at §§54 and 56-57). The IPT rarely gives an open judgment on points of law (see the Applicants' submissions on Article 6 below). They further submit that, in any event, there has been no change of circumstances such as to make the IPT an effective remedy.

168. First, in the unusual circumstances of this case, this Court can be confident that the outcome of the posited alternative remedy would not have provided the Applicants with a remedy for the violation found – for all the reasons set out in answer to questions 4-6 below.[40]

169. Second, it is clear from s.4(5) HRA, that the IPT is not included on the list of bodies that can make such a declaration of incompatibility of UK law with the Convention. Such a declaration does not in any event result in the invalidation of the legislation in question, and this Court has held that it therefore does not constitute an effective remedy: *Burden v United Kingdom* (2008) 47 EHRR 38, confirmed in *Malik v United Kingdom* (Application no.32968/11) (2013) ECHR 794 (28 May 2013). *Burden* remains good law. It is telling that in relation to the faults found with the intelligence sharing regime before further disclosures were made by the Government in the IPT proceedings, the IPT did no more than grant a (non-statutory) declaration that the regime had not been compliant with Article 8.

170. Third, in any event, even if the court were to change the position set out in *Kennedy* prospectively and to find that the IPT does constitute an effective remedy, that should not lead to the applications being held inadmissible. The BBW and BIJ

---

[40] Indeed, in its letter dated 26 July 2013 **[CB/44]**, the UK Government pointed out that the IPT has previously considered s.8(4) of RIPA and in an open ruling in the *British Irish Rights Watch* case dated 9 December 2004 (IPT/01/77) has expressed the view that it is compatible with the Convention.

Applicants were entitled to rely on the ruling in *Kennedy*. The Court has held that it will only consider that an applicant is required to make use of a remedy which has developed since the Application was made if (a) the applicant can still make use of this remedy and (b) it would not be "*unjust*" to declare the application inadmissible at such a late stage (J. Simor QC and B. Emmerson QC, *Human Rights Practice*, §20.007; *Campbell and Fell v United Kingdom* (1985) 7 EHRR 165 at §§58-63; *Baumann v France* (2002) 34 EHRR 44 at §47). In this case, the Applicants cannot now be expected to complain to the IPT since the issues are general issues of law, not specific issues of fact relating to the Applicants, which have now been determined by the IPT. Furthermore, this Court is considering the applications on the merits, on the basis of evidence and submissions filed by the BBW and BIJ Applicants (which are similar but not identical to those relied upon by 10 Human Rights Organisations) following extensive engagement with the Court over a four-year period.

171. In addition to these points, the Applicants also refer to their detailed submissions regarding the compatibility of the IPT's procedure with Article 6(1) ECHR below. They note that the disclosures made in the course of the IPT proceedings were made voluntarily and in respect of both its findings on the bulk interception and intelligence sharing regime, the IPT relied materially on closed material that it had considered which was not disclosed to the claimants.

172. In the circumstances, the Applicants have done all that was required of them.

C. Q4: DETERMINATION OF "CIVIL RIGHTS AND OBLIGATIONS"

Question 4 from the Court: "If the applicants brought proceedings before the Investigatory Powers Tribunal, did those proceedings involve the determination of "civil rights and obligations" within the meaning of Article 6 §1 of the Convention?"

See [10OrgReply/272-279]

173. The applicants in Application Number 24960/15 brought proceedings before the IPT challenging the compatibility of the bulk interception and intelligence-sharing regimes with their rights under Articles 8 and 10 ECHR. They also challenged the specific application of those regimes to the interception, extraction, filtering, storage,

analysis and dissemination of the applicants' own private and confidential electronic communications (and related communications data). In so doing, those Applicants invoked the only mechanism under UK law that enables a person to challenge unlawful interferences with their private law confidentiality and privacy rights by the UKIS exercising surveillance powers under RIPA. The proceedings before the IPT therefore undeniably involved the determination of "*civil rights and obligations*" within the meaning of Article 6(1) of the Convention.

174. All of the conditions for the engagement of the civil limb of Article 6(1) are met in respect of the proceedings brought by the Applicants before the IPT.

175. The IPT itself has previously held that legal challenges of this nature engage Article 6(1). In *Kennedy* (IPT01/62 and IPT/01/77) the IPT held that, "*Article 6 applies to a person's claims under section 65(2)(a) and to his complaints under section 65(2)(b) of RIPA, as each of them involves "the determination of his civil rights" by the Tribunal within the meaning of Article 6(1)*"[41] (§85). Moreover, the IPT's determinations "*have a sufficiently decisive impact on the private law rights of individuals and organisations to attract the application of Article 6*" (§99). In reaching this conclusion, the Tribunal explained that:

> "100. The jurisdiction of the Tribunal is invoked by the initiation of claims and complaints by persons wishing to protect, and to obtain redress for alleged infringements of, their underlying rights of confidentiality and of privacy for person, property and communications. There is a broad measure of protection for such rights in English private law in the torts of trespass to person and property, in the tort of nuisance, in the tort of misfeasance in a public office, in the statutory protection from harassment and in the developing equitable doctrine of breach of confidence …
>
> 101. Since 2 October 2000 there has been added statutory protection for invasion of Article 8 rights by public authorities. This follows from the duties imposed on public authorities by section 6 and the rights conferred on victims by section 7 of the [Human Rights Act]. The concept of 'civil rights and obligations' is a fair and reasonable description of those common law and statutory rights and obligations, which form the legal foundation of a person's right to bring claims and make complaints by virtue of section 65."

---

41 Section 65(2)(a)-(b) **[CB/22]** provides that the IPT is the only appropriate tribunal (i.e. it has exclusive jurisdiction) to hear claims alleging violations of ECHR rights against UKIS.

176. In this regard, the IPT added that: "[t]*he fact that the alleged infringements of those rights is by public authorities in purported discretionary exercise of administrative investigatory powers does not detract from the 'civil' nature of the rights and obligations in issue*" (§102). The IPT therefore concluded that, "*viewing the concept of determination of "civil rights" in the round and in the light of the Strasbourg decisions, the Tribunal conclude that RIPA, which puts all interception, surveillance and similar intelligence gathering powers on a statutory footing confers, as part of that special framework, additional 'civil rights' on persons affected by the unlawful exercise of those power*s" (at §108).

177. This Court subsequently noted in *Kennedy* that, "*the IPT was satisfied that rights of confidentiality and of privacy for person, property and communications enjoyed a broad level of protection in English private law and that the proceedings therefore involved the determination of 'civil rights' within the meaning of Article 6 § 1*." (at §179). Although the Court formally left open the question of "*whether Article 6 applies to proceedings of this nature*", it nevertheless proceeded to examine the merits of the alleged violation of Article 6 in that case.

178. In adjudicating the Applicants' claims in the present case, the specific findings of fact and law which the IPT was required to make included:

> "Whether in fact there has been…soliciting, receiving, storing and transmitting by UK authorities of private communications of the Claimants which have been obtained by the US authorities pursuant to Prism and/or Upstream in contravention of Articles 8 and/or 10 ECHR" and
>
> "Whether in fact the Claimants' communications have been intercepted pursuant to s.8(1) or s.8(4) of RIPA, and intercepted, viewed, stored or transmitted so as to amount to unlawful conduct and/or in contravention of and, not justified by, Articles 8 and/or 10 ECHR."[42]

179. In determining those issues, the IPT had to reach specific determinations regarding whether the Applicants' individual rights were violated by intrusive surveillance targeted against the Applicants' own private and confidential communications. The alleged conduct in question – namely the unlawful interception, extraction, filtering,

---

42 IPT third judgment, 22 June 2015 **[CB/16]** §2.

storage, analysis and dissemination of the Applicants' electronic communications (and related communications data) – entailed a direct, serious and far-reaching interference with the Applicants' rights to privacy and confidentiality under English private law.

180. There is no reason to depart from the IPT's position in *Kennedy* that proceedings before the Tribunal involve the determination of civil rights and obligations. There was a genuine and serious dispute between the Applicants and the Respondent as to the scope of those rights, the extent to which they had been interfered with, and the lawfulness of such interference. The IPT's determination of those issues was directly decisive of the Applicants' civil rights. The proceedings therefore involved the determination of "*civil rights and obligations*" and were required to satisfy the requirements of fairness, independence and impartiality established by Article 6(1).

D. Q5: COMPATIBILITY OF IPT PROCEEDINGS WITH ARTICLE 6 ECHR

Question 5 from the Court: "If so, were the limitations inherent in the IPT proceedings, taken as a whole, disproportionate or did they impair the very essence of the applicants' right to a fair trial?"

See [10OrgApp/86; 10OrgUpdate/1-40; 10OrgReply/280-285]; [BBWReply/39]

181. The limitations inherent in the IPT proceedings were disproportionate and impaired the very essence of the applicants' right to a fair trial protected under Article 6. In particular:

    181.1. Secret meeting and secret protocol between the IPT and the Security Service – As explained at §§182-187 below, the proceedings before the IPT were conducted without the Applicants being informed about a secret meeting between members of the IPT and the Security Service at which a secret protocol was explained and endorsed. The secret meeting and protocol (a) demonstrate a lack of independence and impartiality on the part of the IPT; and (b) made it impossible in practical terms for the IPT to undertake a meaningful assessment of the necessity and proportionality of any interception, extraction, filtering, storage and dissemination of the Applicants' communications and/or communications data.

181.2. Reliance on secret arrangements in support of conclusion that interception regime was in accordance with the law – In finding that the existing interception regime was in accordance with the law, the IPT placed significant reliance on secret "*arrangements below the waterline*" which were not disclosed to the Applicants and on which the Respondents were permitted to make submissions during closed proceedings.

181.3. Applicants were not effectively represented in the closed proceedings – The IPT held a closed hearing from which the Applicants were excluded. The IPT failed to take adequate steps to ensure that the Applicants were effectively represented in the closed proceedings.[43]

181.4. Failure to require defendants to disclose key internal guidance – The IPT declined to direct the UKIS to disclose any of their internal guidance concerning the treatment of confidential material of non-governmental organisations under Article 10. As a result, the Applicants were required to advance their challenge under Article 10 in ignorance of relevant material that could have been disclosed without posing any risk to national security.

181.5. Determination in favour of wrong party – At the conclusion of the proceedings, the IPT made a determination in favour of the wrong Applicant. This error went undetected for a significant period of time and indicates a lack of care and rigour during the judicial process before the IPT.

A summary of the Applicants' Article 6 objections to the IPT process is as follows:

(1) Secret meeting and secret protocol between IPT and Security Service

182. In July 2016 (i.e. after the Applicants' proceedings before the IPT had concluded) it emerged in the course of separate proceedings before the IPT that in November 2007

---

[43] The IPT appointed Counsel to the Tribunal, who produced a written protocol explaining that his role in the secret part of the procedure was to advance the points that could properly be made on behalf of the Applicants. However, there was no formal procedure for liaison between the Applicants and the Counsel to the Tribunal; and the ad hoc protocol voluntarily adopted by Counsel to the Tribunal did not come close to ensuring that the Applicants were effectively represented during the hearings from which they were excluded.

judicial members of the IPT attended a secret meeting with senior MI5 officials at MI5's headquarters.[44] At that meeting MI5 discussed a protocol concerning how MI5 would search its data holdings, and how it would report the outcome of those searches to the IPT, whenever a person lodged a complaint to the IPT. Under the protocol, MI5 would not search or disclose any bulk data holdings relating to a complainant before the IPT. It would only search its records of persons specifically targeted. In consequence, if bulk intercept material had been retained for too long, or if material had been wrongfully retained about a person not of intelligence interest, this would not be detected.

183. The existence of this secret meeting and resultant secret protocol was not known until it was disclosed in other proceedings. None of the Applicants was informed about the existence of the meeting or the protocol. Nor were they informed that one of the judges who sat on the IPT in this case (Mr Robert Seabrook QC) had previously attended the meeting with officials from one of the UKIS, defendants to the proceedings.

184. It is striking that the IPT, which is a judicial body with jurisdiction over a wide range of litigation against the Security Service, willingly attended a secret meeting with the Security Service to discuss the Security Service's approach to its disclosure obligations in future litigation before that judicial body. It is even more striking that:

    184.1. The IPT apparently agreed to the operation of a protocol whereby the Security Service would neither search for nor inform the IPT about the existence of any communications or communications data relating to a complainant in an MI5 bulk data holding.

    184.2. The IPT did not consider it inappropriate to withhold from the Applicants all information concerning the existence of the meeting and the protocol, notwithstanding the obvious relevance of both to the issues in the proceedings and the fact that the Security Service was a defendant to the proceedings.

---

44 *[10OrgReply/Reply Annex, no. 34]*.

185. The Applicants submit that:

185.1. the secret meeting between the IPT and the Security Service;

185.2. the existence and apparent endorsement by the IPT of a secret protocol limiting the scope of the Security Service's obligation to search for, and make disclosure to the IPT of, relevant holdings of material in MI5 databases; and

185.3. the failure to inform the Applicants about either the existence of the secret meeting or the existence of the secret protocol;

each demonstrate a lack of independence and impartiality on the part of the IPT as well as a breach of the requirement of equality of arms between the Applicants and the Respondents.

186. Furthermore, quite apart from the points above, assuming that the secret protocol was applied in the present case then it was impossible for the IPT to determine whether the Applicants' communications had been intercepted, extracted, filtered, stored or disseminated and, if so, whether that was necessary and proportionate. The secret protocol disabled the IPT from discovering whether there were bulk data holdings about each of the Applicants, and whether there had been any unlawful conduct in relation to such holdings.

187. As a result of the application of a secret protocol, the IPT would never be told about the retention of the Applicants' communications in bulk data holdings, the nature and volume of data contained in those holdings, the period of time those holdings were retained for, and whether those holdings were disseminated. A potentially vast volume of the Applicants' sensitive private communications (and related communications data) could therefore have been intercepted, extracted, filtered and stored for years (and potentially in contravention of any internal time limits) without the IPT ever being aware of this or detecting the unlawful conduct. In those circumstances, it is impossible to see how the IPT could have reached a fair determination about the necessity and proportionality of any interception, extraction, filtering, storage and dissemination of the Applicants' communications (and related communications data).

(2) Reliance on secret arrangements in support of conclusion that interception regime was in accordance with the law

188. When determining issues of law based on hypothetical facts, the IPT held a closed hearing at which the respondents relied on secret "*arrangements below the waterline*"[45] concerning the conduct of the s.8(4) interception regime. The IPT concluded that those secret arrangements meant that the s .8(4) regime was "*in accordance with the law*". By founding its conclusions on relevant material that was deliberately withheld from the Applicants – and by taking no meaningful steps to mitigate the substantial disadvantage that this caused the Applicants – the IPT violated the principle of equality of arms.

(3) The Applicants were not effectively represented in the closed proceedings

189. The IPT did not ensure that the Applicants were effectively represented in the closed proceedings. Indeed, while Counsel to the Tribunal ("**CttT**") participated in the closed hearing the Applicants were not represented by representatives of their choice to whom they could give effective instructions based on genuinely adequate disclosure. While the IPT stated that it would expect CttT to advance submissions from the perspective of the Applicants' interests, the IPT in its judgment described CttT's role as "*neutral*" and there was no mechanism for the Applicants to be involved in the appointment and instruction of CttT.[46] The role of the CttT, moreover, was not provided by legislation and the CttT was answerable only to the IPT in respect of the discharge of its functions[47]

190. The absence of effective representation for the Applicants was particularly significant since, as explained above, the IPT's analysis of the Applicants' complaints under Articles 8 and 10 drew heavily on secret arrangements on which the respondents made submissions in closed.

---

45 This was the expression used by the respondents' legal representative, as recorded at §47 of the IPT's first judgment, 5 December 2014 **[CB/14]**.

46 IPT's first judgment, 5 December 2014 **[CB/14]**, §9.

47 The objection in *Kennedy*, at §187 of the Court's judgment falls away, since the IPT determined the matter on the basis of agreed hypothetical facts, and since the fact of interception in two cases was ultimately disclosed to the Applicants.

(4) Failure to require the defendants to disclose key internal guidance

191. The IPT declined to direct the UKIS to disclose any of their internal guidance concerning the treatment of confidential material of non-governmental organisations under Article 10. The IPT decided not to require this material to be disclosed notwithstanding that:

    191.1. the UKIS had maintained for almost a year that Article 10 did not apply to non-governmental organisations;

    191.2. the IPT directed disclosure of similar material in *Belhaj and others v Security Service and others* (IPT/13/132-9/H) without apparent prejudice to national security; and

    191.3. the Applicants had requested disclosure of such material from the outset.

192. As a result, the Applicants were prevented from advancing their case under Article 10 by reference to the applicable guidance that governed how the UKIS approached the interception, extraction, filtering, storage, analysis and dissemination of confidential material of non-governmental organisations. Article 10 confers enhanced protections on the communications of non-governmental organisations (see §§71-74, 130 above). Since the content of any guidance is relevant to the question of whether interferences with the communications of such organisations are "*in accordance with the law*", the Applicants' ability to advance their case under Article 10 was significantly and unnecessarily prejudiced by the IPT's failure to require disclosure of that guidance. This constituted a further violation of the requirement of equality of arms.

(5) The IPT's fundamental error about identity of applicant whose rights were violated

193. Almost two weeks after the IPT circulated its third judgment to the Applicants – and more than a week after it was publicly handed down and reported worldwide – the IPT notified the Applicants that the judgment had erroneously identified the Egyptian Initiative for Personal Rights, rather than Amnesty International Ltd, as the

party whose rights were violated as a result of the excessively long retention of their intercepted email communications.

194. The fact that the Tribunal made such a fundamental error in relation to the identity of the party whose rights had been violated, and that the error remained uncorrected until over a week after the judgment was published, indicates a lack of rigour during the judicial processes that led up to the third judgment.

195. At that stage in the proceedings, the IPT was undertaking an assessment of the necessity and proportionality of the interference with each of the Applicants' rights. The identity of each Applicant was self-evidently relevant to that assessment, which could only be fairly carried out on the basis of an accurate understanding of the identity of the person whose intercepted communications were being examined.

196. The fact that the IPT confused the Egyptian Initiative for Personal Rights with Amnesty International gives rise to a serious and legitimate concern about the manner in which the IPT determined the Applicants' claims.

Conclusion

197. For the reasons set out above and in *[10OrgApp/86; 10OrgUpdate/1-40; 10OrgReply/280-285]*, the restrictions inherent in the limitation of the proceedings before the IPT were disproportionate and impaired the essence of the Applicants' right to a fair hearing under Article 6(1).

E. Q6: VIOLATION OF ARTICLE 14 ECHR

Question 6 from the Court: "Has there been a violation of Article 14, taken together with Article 8 and/or Article 10, on account of the fact that section 16 of the Regulation of Investigatory Powers Act 2000 grants additional safeguards to people known to be in the British Islands?"

See [10OrgApp/(additional submissions)/82-85] [10OrgReply/262-271]

198. The s.8(4) Regime is indirectly discriminatory on grounds of nationality and "*other status*" because of the additional safeguards granted to those known to be in the

British Islands but denied to those abroad under s.16 RIPA. There is no justification for this differential treatment, which violates Article 14 of the Convention.

199. The discriminatory impact of the differential treatment is exacerbated by the IPT's ruling in *Human Rights Watch v Secretary of State for the Foreign and Commonwealth Office* [2016] UKIPTrib15/165/Ch **[CB/56]** that, "*a contracting state owes no obligation under Article 8 to persons both of whom are situated outside its territory in respect of electronic communications between them which pass through that state*" (§60). As a result, persons outside the United Kingdom whose communications are nevertheless intercepted by the Government in the UK are not only denied the protection of a safeguard concerning the treatment of that intercepted material (s.16 of RIPA) but also the protection of the Convention altogether (Article 8).

(1) The effect of s. 16 of RIPA

200. The s.8(4) framework expressly confers additional safeguards upon individuals who are known to be in the British Islands. In particular, under s.16(2) when intercepted material is selected for examination, it may not be selected on the basis of a factor which is "*referable to an individual who is known to be for the time being in the British Islands*", unless the Secretary of State certifies that this is necessary under s.16(3).

201. As a result, in the absence of such certification, material intercepted under a s.8(4) warrant may not be selected for examination using factors that relate to individuals known to be in the British Islands. No equivalent restriction applies to individuals who are situated outside the British Islands

(2) The facts are within the ambit of Articles 8 and 10

202. It is not disputed that the facts in issue fall within the ambit of Articles 8 and 10.

(3) Indirect discrimination on grounds of nationality and other status

203. A British person is substantially more likely to be present in the British Islands than a non-British person. Similarly, a person who is resident in the United Kingdom is

substantially more likely to be present in the British Islands than a person who is resident in another country. Section 16 of RIPA therefore constitutes indirect discrimination on grounds of nationality and "other status", since the safeguards and search restrictions established under that provision:

203.1. are substantially less likely to be enjoyed by non-British nationals than by British nationals; and

203.2. are substantially less likely to be enjoyed by persons resident outside the British Islands than by persons resident in the British Islands.

204. In the proceedings before the IPT, the Government "*accept[ed] that there is an arguable distinction based upon location, and thus, by reference to the claimants' arguments, on a ground by reference to national origin*" (First IPT Judgment **[CB/14]**, §147).

(4) Absence of justification for differential treatment

205. Persons outside the United Kingdom are entitled to the same protection for the privacy of their electronic communications as persons inside the United Kingdom. However, the protection afforded to persons outside the UK under s. 16 is substantially weaker than the protection afforded to persons inside the UK. If UKIS wishes to select the intercepted communications of a NGO in the UK for examination, a certificate under s. 16(1) would be required. Accordingly, the Secretary of State would need to be satisfied that there was a proper basis for reading, looking at or listening to, the NGO's communications. But if UKIS wish to read, look at or listen to the communications of a foreign NGO (the communications of a foreign office of a UK NGO or of a UK NGO staff member on mission abroad) then this would not require a s. 16(1) certificate, even if the evidential basis was exactly the same. RIPA requires certification (which must be supported by a proper case and the personal approval of the Secretary of State) for a person in the UK, but not for a person in an otherwise identical position abroad. There is no good reason for this differential treatment.

206. The nature and extent of this differential treatment is serious and the Government has advanced no proper justification for it. In essence, the Government contends that:

206.1. The Government enjoys a wide margin of appreciation since the impugned measure concerns the field of national security;

206.2. The Government has more powers at its disposal to investigate individuals who are in the British Islands than individuals based outside the British Islands. Accordingly, it is reasonable to restrict certain safeguards to persons who are known to be in the British Islands; and

206.3. The IPT considered that a requirement for a s.16(3) certificate in every case would undermine the efficacy of the s.8(4) regime.

None of these points provides an adequate justification for the significant indirect discrimination that inevitably results from the operation of s.16.

207. In relation to §206.1 above, while the Court has recognised that States enjoy a margin of appreciation in relation to the justification of indirectly discriminatory measures, States do not enjoy untrammelled discretion and they continue to bear the burden of establishing the necessity and proportionality of the measure giving rise to the discriminatory consequences. The Court retains ultimate responsibility for determining whether the requirements of Article 14 have been satisfied (*Biao v Denmark*, GC, App. no. 38590/10, 24 May 2016, §93).

208. In this regard, the Government's reliance on the case of *Stec v UK*, App. No. 65731/01, 12 April 2006, which adopted a "*manifestly without reasonable foundation*" test, is misplaced. *Stec* was a welfare benefits case concerning an upper limit of eligibility that had been tied into other benefits (and so severing them would have a number of complex financial implications). It was therefore a classic economic or social strategy case where a wider margin of appreciation is often afforded by the Court.

209. The types of issues in *Stec* are far removed from the present case. The Applicants' claims do not concern economic or financial issues; nor do they involve sensitive

value judgments in the sphere of social policy or welfare. Instead, they concern intrusive surveillance programmes that engage the privacy interests of large numbers of individuals in multiple countries. In view of the sheer volume of communications (and related communications data) intercepted under the bulk interception regime, s.16 has substantial and direct implications for the privacy rights of non-British persons. The differential treatment therefore requires a logical and evidence-based justification.

210. In relation to §206.2 above, while the ability of the Government to investigate individuals who are in the British Islands may be greater in some cases than its ability to investigate individuals in other countries, this does not justify a sweeping denial of the s.16 safeguards to all persons who are outside the British Islands. In particular, it is arbitrary to apply a one-size-fits-all denial of a safeguard without any reference to the particular country where a person is known to be and the Government's ability to obtain information about that person through criminal and intelligence sharing relationships with the authorities in that country.

211. In relation to §206.3 above, the IPT accepted the Government's argument that it would be unworkable to require a s.16(3) certificate every time that the UKIS wish to select for examination intercepted material. However, no evidence was presented to the IPT in open in support of that proposition. Nor is there any suggestion in the IPT's judgment that any such evidence was presented in closed. On the contrary, the IPT merely accepted a submission that it was "*obvious*" that this would not be possible. The IPT did not provide any reasons or explanation in its judgment of the factors and evidence on which that conclusion was based. The IPT's unreasoned assertion stands in contrast to the position in *Weber v Germany* (App. No. 54934/00), where the Court noted that the G10 Commission supervised all 'catchword' selectors.

212. The distinction drawn by s.16 is arbitrary. The applicability of the safeguards in s.16 depends upon whether the UKIS know that a person is present somewhere in the British Islands. As soon as a person leaves the British Islands, the UKIS are free to select for examination any intercepted material that is referable to that particular person. As a result:

212.1. If the UKIS wish to select for examination intercepted material using the name of an individual who they know is about to board a flight from London to Paris, they must obtain ministerial authorisation to do so. However, if the UKIS wish to intercepted material for examination using the name of the same individual when that person is about to board a flight from Paris to London, there is no such requirement. The position is then inverted when the person reaches their destination. There is no logical reason for providing different levels of protection in these two situations.

212.2. Similarly, if GCHQ wishes to target an NGO's London office they would need a warrant or s.16(3) certificate. But if they wish to target the same NGO's German office the communications of one of its London staff member abroad, they would not need to do so. Again, this distinction lacks any rational basis.

212.3. The extent of the UKIS' knowledge about the whereabouts of a person of interest does not necessarily bear any correlation to the applicability of the s.16 safeguards. For example, even if the UKIS know the exact location of a person in a foreign country and have placed that person under direct visual surveillance, they may nevertheless select for examination intercepted material referable to that person without a ministerial certificate. By contrast, if the UKIS merely know that a person is somewhere in the British Islands, but have no idea exactly where, they are precluded from selecting for examination that person's communications (and related communications data) unless they obtain a s.16(3) certificate. It may be much easier for the UKIS to investigate the former, yet that person enjoys significantly less protection than the latter. This is inconsistent with the Respondent's ostensible rationale for the distinction drawn in s. 16, namely that greater safeguards should be reserved for those persons who can be more easily investigated by other means

VII. CONCLUSION

213. The interferences with Convention rights identified in these Applications are unprecedented and potentially affect the entire populations of the Council of Europe States and beyond. Moreover, the Court's acceptance of a wide-ranging regime for

bulk surveillance of communications and communications data would set a remarkable precedent for all other Contracting Parties to the Convention, undermining the Court's case-law on secret surveillance measures.

214. For all the reasons set out above, in their Applications, their Update Submissions and their Reply Submissions, the Applicants respectfully invite the Court to uphold their Applications and declare the UK in breach of Articles 6, 8, 10 and 14 of the Convention.

29 September 2017