IN THE EUROPEAN COURT OF HUMAN RIGHTS APP. NO. 24960/15

BETWEEN:

10 HUMAN RIGHTS ORGANISATIONS

Applicants

-v-

THE UNITED KINGDOM

Respondent Government

APPLICANTS' REPLY TO OBSERVATIONS OF THE GOVERNMENT OF THE UNITED KINGDOM

TABLE OF CONTENTS

PART 2: APPLICANTS' REPLY TO THE GOVERNMENT'S OBSERVATIONS

PART 1: CURRENT CONTEXT OF PARTIES' SUBMISSIONS

I. INTRODUCTION AND SUMMARY

Modern forms of communication

1. The context of this case is of critical importance to the privacy of modern forms of communication used by billions of people around the world and hundreds of millions of people communicating to or from persons residing in Europe.

2. The Government of the United Kingdom claims the right to intercept in bulk any communications that happen to traverse the UK, including those of both UK citizens and others across the world. Additionally, in relation to communications that the UK Government does not obtain by directly intercepting them, it asserts an almost unfettered right to obtain those which have been intercepted by the intelligence services of other states, including the National Security Agency ("NSA") of the United States of America.

3. 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") – can now intercept, store and analyse vast amounts of internet and telephone communications regardless of any individual ground for reasonable suspicion.

The risk of state abuse of overbroad powers that infringe privacy

4. Council of Europe states face serious security threats and the problem of serious crime. But these threats are to be addressed whilst also protecting fundamental rights. In his published Opinion in *Tele2 Sverige AB v Post-och telestyrelsen (C-203/15) and Secretary of State for the Home Department v Tom Watson, Peter Brice, Geoffrey Lewis (C-698/15) Interveners: Open Rights Group, Privacy International, The Law Society of England and Wales Joined Cases C-203/15 and C-698/15 (Watson & Others)*, Advocate General Saugmandsgaard Øe cited James Madison writing in 1788 to explain the essential principles. Privacy is a qualified right, but one which must be protected by the law to ensure that wide state powers are not abused. The risk of abuse can occur in any state, including those in the Council of Europe:

> If men were angels, no government would be necessary. If angels were to govern men, neither internal nor external controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself.

5. As the Independent Reviewer of Terrorism Legislation, David Anderson QC (the "Independent Reviewer") put it in "*A Question of Trust: Report of the Investigatory Powers Review*":

> The moral is not that threats ought to be ignored: on the contrary, any credible threat should be guarded against. The point is, rather, that claims of exceptional or unprecedented threat levels – particularly if relied upon for the purposes of curbing well established liberties – should be approached with scepticism. (§3.6)

6. This application raises novel and important issues of law and principle: it is the first time this Court has been called upon to address directly the question of whether surveillance on the scale now taking place should be

permitted and the minimum safeguards that are needed to meet the standards required by the Convention in an age of digital communication. The Applicants contend that the scheme of bulk interception and intelligence sharing operated by the UK is incompatible with the rights to privacy and freedom of expression guaranteed by Articles 8 and 10 of the European Convention on Human Rights.

Lack of safeguards

7. Further, the safeguards put in place by the UK were and are entirely inadequate. The UK system lacks:

(1) A clear statement on the nature of the offences which may give rise to the surveillance at issue;
(2) A requirement of individual reasonable suspicion;
(3) Defined categories of people who may be subject to surveillance;
(4) Temporal limits on the duration of surveillance;
(5) Adequate procedures for the examination, analysis, and storage of the data obtained;
(6) Precautions when disseminating data to other parties;
(7) *Ex-ante* independent authorisation for and *ex-post* effective review of the interception and/or sharing of individuals' communications; and
(8) Notification to subjects of surveillance.

Simple focus of this application

8. Before proceeding, the Applicants wish to note that the extremely lengthy response by the Government, making many assertions on the history and context of the relevant domestic legislative provisions combined with reliance on a large number of long reports, necessitates a lengthy response from the Applicants to ensure that the Court is aware that many of the

assertions made by the Government are in dispute. However, the Applicants also wish to emphasise that this unfortunate lengthening of the material before the Court should not distract or detract from the relatively simple focus of this application.[1]

The s8(4) Regime

9. These submissions begin by addressing the United Kingdom bulk interception powers under section 8(4) of the Regulation of Investigatory Powers Act 2000 ("RIPA") (the "s8(4) Regime"). RIPA will be familiar to the Court, as it was the subject of the Court's consideration in *Kennedy v United Kingdom* (2011) 52 EHRR 4. But in *Kennedy*, the Court assessed whether so-called targeted interception under RIPA section 8(1) (the "s8(1) Regime"), which requires the identification of a specific person or location as the subject of the interception, violated Article 8. The Court found the RIPA s8(1) regime did not breach Article 8 because, as the Court noted in *Szabó and Vissy v Hungary* 63 (2016) EHRR 3, "*the impugned legislation did not allow for indiscriminate capturing of vast amounts of communications*" (§69). The s8(4) Regime, however, authorises the very "*so-called strategic, large-scale interception*" that the Court dubbed "*a matter for serious concern*" in *Szabó* (§69).

10. For that reason, the Court is invited to consider the s8(4) Regime with care. On examination, it neither meets the requirements for being "in accordance with law" nor is it necessary or proportionate.

11. First, the s8(4) Regime is opaque. It was not until Edward Snowden disclosed the extent of the UK Government's bulk surveillance operations

[1] In March 2015, the Applicants submitted their applications to this Court, setting out violations of Articles 8, 10, 6 and 14 of the Convention. The document setting out their submissions, in compliance with the Court's rules, is 20 pages long. In a document dated 18 April 2016, the Government of the United Kingdom ('the Government') set out its *'Observations on the Merits'* in response. The Government's document is 200 pages long. Additionally, it attached 64 separate annexes, totalling an additional several hundred pages.

– in particular, its bulk interception programme code-named "Tempora" – that the public first understood the true scope of the s8(4) Regime. The confusing and obscure nature of RIPA and related surveillance legislation in the UK has now been almost universally recognised, including by multiple independent committees and reviewers tasked with assessing the legislation following the Snowden disclosures.

12. Second, the s8(4) Regime fails to meet the minimum safeguards for communications surveillance identified in *Weber and Saravia v Germany* (2008) 46 EHRR SE5. Furthermore, in its recent case law, the Court has made clear that significant technological developments in electronic communications and covert surveillance capabilities must be matched by commensurate developments in the minimum legal safeguards applicable to a state's use of covert surveillance powers. As the Court declared in *Szabó*, "[*t]he guarantees required by the extant case-law on interceptions need to be enhanced so as to address the issue of such surveillance practices*." (§70).

13. The Applicants also contend that the recent jurisprudence of this Court and the Court of Justice of the European Union ("CJEU") have identified these enhanced safeguards – and the s8(4) Regime fails to satisfy any of them. The s8(4) Regime does not require: (1) individual reasonable suspicion regarding the target of the interception; (2) prior independent authorisation of the interception; or (3) subsequent notification of the interception measures.

14. The Applicants place significance on the way UK law treats intercepted communications data. While there are inadequate safeguards for both content and communications data, in relation to the latter the lack of safeguards is particularly serious. For this reason, the UK Government is forced to argue that this difference in safeguards reflects a significant difference in the infringement of privacy caused by state interception,

retention and examination of the content and state interception, examination and retention of the communications data associated with such communications. That distinction is now largely discredited. It is well accepted – both through expert evidence and in the CJEU's decisions – that interference with communications data, including its examination and retention, is a significant interference with privacy. The Government's position in this case in seeking to defend the lack of legal safeguards connected with communications data by elevating a distinction between content and communications data is simply untenable.

15. For all of these reasons, interferences with privacy and freedom of expression authorised under the s8(4) Regime are not in accordance with law.

16. Bulk interception is also neither necessary nor proportionate. The Government maintains that, "*the information and intelligence obtained under both the Intelligence Sharing Regime and the s8(4) Regime have been and remain critical to the proper protection of national security, notably against the serious threat of terrorism*" (Observations, §2). The Applicants agree that the UK faces serious security risks and that properly targeted and authorised surveillance measures can assist in the prevention and prosecution of serious crimes. The Applicants further recall the Government's similar claim in *S and Marper v United Kingdom* (2009) 48 EHRR 50 that DNA material taken from persons who had not been convicted of any criminal offence was "*of inestimable value in the fight against crime and terrorism and the detection of the guilty*" (§91). In that case, the Grand Chamber unanimously concluded that the "*blanket and indiscriminate"* nature of the Government's retention of personal data "*fail[ed] to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard*" (§25).

17. The Applicants submit the same is true of the present case. The blanket and indiscriminate nature of the s8(4) Regime fails to strike a fair balance between public and private interests and similarly oversteps any acceptable margin of appreciation. As the Grand Chamber held in *Klass v Germany* (1978) 2 EHRR 214: "*The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate*" (§49).[2]

The Intelligence Sharing Regime

18. The Government's access to data intercepted by other countries' intelligence agencies, including the NSA, raises similar concerns. Until very recently, and only after this case was initiated before the UK Investigatory Powers Tribunal ("IPT"), the UK had no publicly accessible regime governing intelligence sharing. Even now, that regime remains highly deficient.

19. The Government argues that such intelligence sharing should not be subject to the same safeguards as its own interception powers. But its reasoning is faulty. Just because another country is conducting the interception does not lessen the intrusion. Accordingly, whether the Government intercepts communications and communications data itself or obtains the same flow of data from another intelligence agency, the same safeguards should apply. It is a breach of Article 3 of the Convention to torture a person. It is equally a breach to deport a person to face a real risk of torture. Outsourcing the same conduct does not excuse the Council of Europe state from liability. Convention rights are practical and effective, not theoretical and illusory. See *Chahal v UK* (1996) 23 EHRR 413. Where intelligence sharing involves access to information intercepted

[2] *See also, e.g.*, *Rotaru v Romania*, App. No. 28341/95, 4 May 2000, §59.

in bulk, the same standards in Articles 8 and 10 of the Convention apply to it. The regime for intelligence sharing is defective, for essentially the same reasons as the s8(4) Regime is inadequate.

Unjustified discrimination contrary to Article 14

20. The s8(4) Regime is also unjustifiably discriminatory on grounds of national origin. Persons present in the UK, who are more likely to be British citizens, enjoy additional procedural safeguards that could (and should) be provided to persons outside the UK.

Failures of oversight

21. The UK's surveillance oversight system is not sufficient to remedy the above problems. In the past, particularly in *Kennedy*, the Government has relied heavily on the IPT and the Interception of Communications Commissioner ("IOCC") as an effective form of redress for those who have been subject to unlawful surveillance. As applied to modern bulk surveillance practices, the IPT and IOCC are not an effective remedy. The absence of adequate oversight arrangements is relevant to the "in accordance with law" arguments and constitute a separate violation of Article 6, in respect of the IPT.

Structure of this document

22. In this document the Applicants now reply to the Government's observations in accordance with paragraph 12 of the Court's Practice Direction on Written Pleadings. This submission sets out the Applicants' observations on the merits of their application in reply to those submitted by the United Kingdom government (the "Government"). These observations are made at the invitation of the President of the Section pursuant to Rule 54(2)(b) of the Rules of Court. They also address the

Statement of Facts prepared by the Registry and conclude with the Applicants' answers to the six questions posed by the Court.

23. This document is in two parts. Part 1 provides the Applicants' response to the Government's lengthy assertions relating to reports and legislative history by setting out the factual context in which these issues should now be seen. It also updates the legal context in which the applications must be considered, in light of relevant judgments that have been promulgated since the applications were submitted. Part 2 provides direct responses to legal issues raised in the Government's observations, culminating in the Applicants' answers to the specific questions posed by the Court.

Article 41 and Just Satisfaction

24. For the avoidance of doubt, the Applicants confirm that they consider that a reasoned finding of breach of the Convention will constitute sufficient just satisfaction. They do not seek their costs.

II. FACTS

A. Terminology

25. To put the applications and the Government's observations in context, the Applicants consider it helpful to outline and define key terminology that they use throughout this document.

1. "Bulk" versus "targeted"

26. The Government does not explicitly define the terms "bulk" and "targeted" in its Observations. Rather, it states that "*it intercepts communications in 'bulk' – that is, at the level of communications cables – pursuant to the lawful authority of warrants under s.8(4) RIPA*" (§1.21). It therefore

describes its interception of communications (and communications data) as "bulk" because *all* of the data over *entire* fibre optic cables "*making up the core structure of the internet*" are intercepted (§1.23).

27. The Government cites a number of reports, which discuss the Government's bulk surveillance capabilities and, in doing so, sheds some light on the meaning of these terms. It cites, for example, the 17 March 2015 report by the Intelligence and Security Committee of Parliament ("ISC"): "*Privacy and Security: A modern and transparent legal framework*" (hereinafter the "ISC Report").[3] In the section of that report addressing the "*bulk interception*" capability, the ISC refers to "*targeted capabilities*" as those "*deployed against a person or single set of premises…where there is specific knowledge about a threat (e.g. a specific email address that has been linked to terrorism or other intelligence requirements)*".[4] In contrast, where the Government accesses the "'*bearers' which make up the core infrastructure of the internet*", the ISC recognises that "*bulk*" is "*an appropriate term to use*" given "*the volume of communications flowing across these bearers, and the number of people those communications relate to, is…extremely large*."[5]

28. The Government also cites the Independent Reviewer's June 2015 report, in which the Independent Reviewer does not specifically define "bulk", but describes "*bulk collection*" as the Government's "*acquiring material on*

[3] INTELLIGENCE AND SECURITY COMMITTEE (ISC), *PRIVACY AND SECURITY: A MODERN AND TRANSPARENT LEGAL FRAMEWORK*, 2015, HC 1075 (UK) ("ISC Report").
[4] ISC Report, para 49.
[5] ISC Report, para 59. The Applicants observe that the UK Government uses the term "bearer" throughout its Observations and indicates that by "bearer", it means "fibre optic cable": "*GCHQ could theoretically access traffic from a small percentage of the 100,000 'bearers' (i.e. fibre optic cables) making up the core structure of the internet*." (§1.23) The Applicants note however that in its submissions to the ISC, GCHQ described bearers differently, explaining that at the heart of each fibre optic cable "*sit a small number of optical fibres*", which "*carry the data*" and that "*[i]n one transatlantic cable for example, there are eight fibres (arranged as four pairs).*" GCHQ further explained that these fibres "*carry 47 separate bearers*" and analogised the bearers "*to different television channels – there are various ways of feeding multiple bearers down a single optical fibre*". ISC Report, para. 55. For the sake of simplicity, the Applicants refer to fibre optic cables, rather than bearers throughout this document.

persons who are not and will never be subjects of interest to them."[6] The Independent Reviewer returned to the issue of bulk powers in his August 2016 "*Report of the Bulk Powers Review*", which examined the operational case for such powers in the Investigatory Powers Bill, currently being debated by the UK Parliament.[7] There he noted that one definition is a power "*allow[ing] public authorities…to have access for specified purposes to large quantities of data, a significant portion of which is not associated with current targets*".[8]

29. The Applicants note that it is only the term "targeted" that has been defined with any specificity in the reports above. They accordingly adopt a definition of "targeted" similar to that used by the ISC but, more importantly, which draws on the Court's own discussion of the appropriate scope of review for government authorisation of surveillance activities in *Zakharov v Russia* (2015) 39 BHRC 435. In that case, the Court "*reiterate[d] that [the scope of review] must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting 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).

30. Thus, the Applicants define "targeted" conduct as interception aimed at the collection of communications in circumstances where there is reasonable suspicion that a specific target has committed or is likely to commit a criminal offence or is engaging in acts amounting to a threat to national security.[9] Given the lack of consistency in the above attempts to

---

[6] INDEPENDENT REVIEWER OF TERRORISM LEGISLATION, A QUESTION OF TRUST: REPORT OF THE INVESTIGATORY POWERS REVIEW (2015) para 10.22 ("*A Question of Trust*").

[7] INDEPENDENT REVIEWER OF TERRORISM LEGISLATION, REPORT OF THE BULK POWERS REVIEW, 2016, Cm 9326 (UK) ("*Report of the Bulk Powers Review*"). Index of Annexed Documents for the Applicants' Reply No. 32 ("Reply Annex")

[8] Report of the Bulk Powers Review, para 1.5. Reply Annex No. 32

[9] This Court has noted that the definition of "national security" needs to be defined carefully so as to avoid an overly broad interpretation. *See Zakharov*, §248: "*It is significant that [the law*

describe "bulk", the Applicants propose simply to define "bulk" by juxtaposition to "targeted", that is, a capability that is *not* "targeted", involving the interception of information about a wide range of people, most of whom are not of any legitimate interest to the security and intelligence agencies.

2. The bulk interception process

31. The process of collecting, analysing, processing and storing personal communications infringes Article 8 in a number of ways and each of those ways must be justified and accompanied by proper safeguards. The Applicants divide the process that Government describes as 'bulk interception' into six stages:

(1) **Initial Interception** – Obtaining a raw signal from a source (e.g. tapping a fibre optic cable).

(2) **Extraction** – Copying the signal and converting or reconstructing it into an intelligible format.

(3) **Filtering** – Selecting particular information of interest (either content or related communications data or both) through the use of identifiers or selectors and discarding low value internet traffic, such as the content of video streaming from well-known commercial providers.

---

governing interception of communications] does not give any indication of the circumstances under which an individual's communications may be intercepted on account of events or activities endangering Russia's national…security. It leaves the authorities an almost unlimited degree of discretion in determining which events or acts constitute such a threat and whether that threat is serious enough to justify secret surveillance, thereby creating possibilities for abuse."; *United Nations Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, U.N. Doc. E/CN.4/1985/4, Annex (1985): "*National security may be invoked to justify measures limiting certain rights only when they are taken to protect the existence of the nation or its territorial integrity or political independence against force or threat of force.*"

(4) **Storage** – Retaining filtered information in a database for potential future analysis or dissemination.

(5) **Analysis** – Querying, examining, data-mining or otherwise analysing information stored in databases.

(6) **Dissemination** – Distributing the results of analysis to other persons, organisations or agencies.

32. Article 8 is engaged at each stage of the bulk interception process.[10] Each of the six steps listed above constitutes a discrete interference with the right to privacy of the individuals whose communications are affected.

3. "Intelligence sharing"

33. The Applicants use the term "intelligence sharing" to refer to all of the various means by which the UK Intelligence Services may access information intercepted by foreign intelligence agencies, including, but not limited, to in bulk:

(1) access to raw intercept material intercepted by foreign intelligence agencies, permitting the UK Intelligence Services to extract, filter, store, analyse and/or disseminate such information;

(2) access to information initially intercepted, extracted, filtered and stored by foreign intelligence agencies, permitting the UK

[10] *See, e.g., Malone v United Kingdom* (1985) 7 EHRR 14: "*As telephone conversations are covered by the notions of 'private life' and 'correspondence' within the meaning of Article 8…, the admitted measure of interception involved an 'interference by a public authority' with the exercise of a right guaranteed to be the applicant under paragraph 1 of Article 8* (ar. 8-1)."; *Amann v Switzerland* [GC] ECHR 2000-II, §§68-70: "*The Court reiterates that the storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding.*"

Intelligence Services to conduct subsequent stages of the bulk surveillance process, namely analysis and/or dissemination; and

(3) access to information initially intercepted, extracted, filtered, stored and analysed by foreign intelligence agencies, permitting the UK Intelligence Services access to the results of analysis.

34. Article 8 is engaged by each of the above types of intelligence sharing. The UK Intelligence Services' ability to access, extract, filter, store, analyse, and/or disseminate material that has been initially intercepted by a foreign intelligence agency constitutes a discrete interference with the right to privacy of the individuals whose communications are intercepted.

B. UK bulk interception under the s8(4) Regime

1. Overview

35. The scope and nature of s 8(4) interception is unprecedented in the history of the UK and, indeed, of any Contracting Party. Communications cables have crossed the English Channel since 1850 and the Atlantic Ocean since 1858.[11] Instant communications technology over long distances (e.g. telegraphs and telecommunications) has existed since the foundation of the Council of Europe. Yet no Contracting Party has ever put forward the argument that it is necessary or justifiable to intercept – in principle – the totality (or even a substantial portion) of communications transmitted across such networks and to subject those private communications to sophisticated automated processing, storage and analysis.

36. The widespread bulk interception of fibre optic cables is likely to have a particularly serious effect on privacy because of the nature of modern communications technology. Until recently, a telephone call between two

[11] Nigel Linge, *The Trans-Atlantic Telegraph Cable* 150th Anniversary Celebration 1858-2008, University of Salford, available at www.cntr.salford.ac.uk/comms/transatlanticstory.php. Reply Annex No. 35

friends in London would be transmitted via a local exchange and would not be subject to any form of bulk interception. But modern internet communications rely on servers and service providers across the world. The same communication sent by instant messaging service or internet telephone call (such as Skype or WhatsApp) would now be transmitted through several countries en route (e.g. via a server in California) and be subject to bulk interception, even though it is purely internal and local. Until relatively recently, placing an international telephone call was an expensive and unusual thing. Now, almost every communication will be transmitted internationally and be subject to bulk interception. Technological change has meant that far more material falls within the net than ever before. Increases in technical capacity mean that this vast volume of information can be automatically analysed and processed.

37. A single warrant under s8(4) has no upper limit in terms of the number of communications that may be intercepted and, therefore, the number of persons whose privacy may be affected. The Government admits, and the IPT has confirmed, that a single warrant may encompass the communications of all the residents of an entire city in the UK with the residents of another country.[12] That is now a conservative scenario. A single warrant may encompass – in principle – *all* the communications of *all* the residents of the UK with *all* the residents of *any* other country. Indeed, it may encompass *all* the communications of *all* the residents of the UK with *all* the residents of *all* other countries. Further, the s 8(4) Regime permits purely domestic communications travelling over the same communications cables, where they cannot be differentiated from the external communications, to be intercepted, extracted, stored and analysed.

[12] *British-Irish Rights Watch et al v Security Service et al,* IPT/01/77, 9 Dec. 2004, para 9.

2. The nature and scale of bulk surveillance under the s8(4) Regime

38. In its Observations, the Government admits that it "*intercepts communications in 'bulk'*" at "*the level of communications cables*" (§1.21). The ISC report similarly found that "*[b]ulk interception is conducted on external communications*" and that, "*GCHQ's bulk interception is used [(a)] to investigate the communications of individuals already known to pose a threat; or [(b)] to generate new intelligence leads, for example to find terrorist plots, cyber attacks or other threats to national security*".[13] The ISC's choice of terminology was deliberate. It explained that since GCHQ's "*bulk interception*" systems are used to access an "*extremely large*" number of individuals' communications, "*'bulk' remains an appropriate term to use when describing this capability*".[14]

39. The Government claims that "*the resources required to process the data involved means that at any one time GCHQ in fact only accesses a fraction of that small percentage of bearers it has the ability to access*" (Observations, §1.23). But even interception of a small number of fibre optic cables – and the Snowden disclosures suggest the UK is intercepting more than 200 cables landing in the UK – would give the Government access to a very large amount of data.[15] The TAT-14, for example, is a transatlantic cable system, consisting of four pairs of fibres – two active, two backup – with landing stations in the US, UK and a number of other European states.[16] The capacity of the TAT-14 is 3.15 terabit per second, which would be equivalent to roughly 34 petabytes of data transiting the system every day.[17] To put that into perspective, in 2008, Google processed

[13] ISC Report, pp 25, 113 para N.
[14] ISC Report, para 59.
[15] Witness Statement of Eric King, 8 June 2014, para 128 and the sources referred to therein (lodged with the Court in the List of Accompanying Documents in the original Application) ("King Witness Statement").
[16] Nearly all fibre optic cables have at least two fibres, known as a pair – one fibre is used to carry data in one direction and the other fibre is used to carry data in the opposite direction.
[17] TAT-14 Cable System: Sprint Network Administration System, https://www.tat-14.com/tat14/. Reply Annex No. 36.

about 24 petabytes of data per day,[18] and as of January 2013, all of the pictures on Facebook were estimated to amount to approximately 357 petabytes.[19]

40. Moreover, the Applicants submit that it would be dangerous to treat the Government's claims as to GCHQ's current level of resources as a form of safeguard. The necessity and proportionality of bulk interception of private communications is not determined by reference to whether a government agency has the money or technical resources to "*process*" everything that it intercepts. Any conclusion based on such a limitation would, moreover, be invalidated as soon as there was a change in the amount of resources and further technological development. The history of computing since the formation of the Council of Europe has been of continued rapid development of capacity and reductions in cost. Those developments can be expected to continue.

41. The Government appears to deny that GCHQ undertakes "'*untargeted*' *surveillance of communications*" on the basis that "*any selection of communications <u>for examination</u> is undertaken on the basis that they match selection rules used to find those communications of maximum intelligence interest*" (Observations, §1.26). However, the only "*selection*" at the point of initial interception is to select which fibre optic cables to intercept (§1.25). The Government's assertion that it chooses cables "*on the basis of the possible intelligence value of the traffic they carry*" is inconsistent with its own description of how internet communications travel (§1.25). Indeed, the Government later states that "*electronic communications do not traverse the internet by routes that can necessarily be predicted*" (§1.29(2)). In any event, the initial interception of entire

[18] Ian Gordon & Deborah Cracio, Data-Intensive Computing: Architectures, Algorithms and Applications 3 (2013).
[19] Mike Allen, Big Data: This Bytes (Part One), DataCenters.com Blog (22 Sept. 2014), available at https://www.datacenters.com/news/cloud/179-big-data-this-bytes-part-one. Reply Annex No. 16.

cables allows the Government access to an enormous amount of data relating to the lives of private individuals around the world, the vast majority of whom are not and never will be of legitimate interest to UK intelligence services.

42. It is only after having initially intercepted specific cables and extracting the data flowing through each cable in bulk that the Government applies its "*selection rules*" (Observations, §1.26(1)). The development of modern search tools and artificial intelligence techniques mean that the UK Intelligence Services can store and trawl through a large pool of information, querying and disseminating it by reference to unknown selectors that may bear little resemblance to criminal investigations or operations. Until recently, such bulk interception would have been difficult or impossible to analyse.

43. Even at the filtering stage, the s8(4) Regime involves bulk intrusion. The Government claims that its selectors "*relate to individual targets*" but this is just one example of the range of selectors that may be used (Observations, §1.26(1)).[20] For instance, a selector could be used to identify everyone who had read a particular book or newspaper article.

44. People never used to read books, magazines or newspapers using a computer, telephone or electronic tablet. Reading material is now communicated over the internet, and therefore subject to bulk interception under the s8(4) Regime. The effect of bulk interception is for the state to store and analyse the reading habits of the population.

45. The interception of such records by the state poses a serious risk to privacy and freedom of expression. Reading is in the nature of a private

[20] See, generally, Report of the Bulk Powers Review, paras 5.1-5.7, referencing the utility of bulk interception not solely to target specific targets using strict selectors, but also to lead to "*building block*" information which can then be used for new target development and to cultivate better understanding of broader "*intelligence threats and opportunities*". Reply Annex No. 32.

activity, often taking place in the home. It is important in a democratic society that there is free access to ideas, including those that may be controversial. The interception and retention of an official record of what people choose to read will have a chilling effect – when will reading a controversial website excite official suspicion or trigger a red flag on an automated computer system?

46. A law requiring every individual to report to the UK Intelligence Services a list of books, newspapers and magazines read to enable those records to be automatically analysed and checked for suspicious reading material could not be reconciled with Articles 8 and 10 of the Convention. The same outcome, as a result of rapid technological change, can now be achieved under the s8(4) Regime. Everyone's reading activities can be automatically intercepted, stored and made available for analysis, regardless of individual suspicion.

47. The wide scope of bulk interception is illustrated by the facts of these cases. The IPT in its Third Judgment notified one of the Applicants (the South African Legal Resources Centre – South Africa's largest human rights and public interest legal organisation) that its communications had been "intercepted and selected for examination".[21] It also notified another Applicant, (Amnesty International – one of the world's largest human rights organisations) that its communications had been "intercepted and accessed" pursuant to s8(4).[22] The dragnet of bulk intercept includes routine and automated storage and analysis of the communications of human rights advocates. These interferences occurred notwithstanding the fact that both Applicants are well-known and respected non-governmental organisations.

[21] *Liberty et al. v GCHQ et al* [2015] UKIPTrib 13_77-H 2, 22 June 2015, para 14 ("Third IPT Judgment"). This judgment was included as Annex 28 of the Government's Reply.
[22] Third IPT Judgment, para 15. The Judgment does not define "access" and it is unclear whether "access" is analogous to "selection for examination" or accords with another step in the bulk interception process.

3. The accuracy of the Applicants' descriptions of the Government's bulk interception programmes

48. The Government claims that "*[t]he intelligence gathering activities and capacities of the UK, and the nature of the interception programmes in the UK and US, have been widely mischaracterised as a result of the Snowden allegations*" (Observations, §1.1). The Applicants note, however, that the Government has not denied that the Snowden documents are authentic. The Applicants address the accuracy of their descriptions of the US surveillance programmes in the Factual Appendix, and show that the US Government has expressly and publicly avowed a range of programmes revealed by the Snowden documents (see Factual Appendix paras 10-19).

49. The Government maintains that it is constrained by its own policy of neither confirm nor deny ("NCND") in relation to the work of the UK Intelligence Services. The Applicants note, however, that this constraint is self-imposed. The US government has disclosed the existence of surveillance programmes, including PRISM and Upstream. The UK Government, too, has – from time to time – elected to provide details of surveillance programmes to non-governmental bodies, such as the Royal United Services Institute ("RUSI"), where such disclosures have suited its purposes.[23]

50. Moreover, the English courts have declined to treat NCND as a paramount concern that overrides all other considerations. In *Mohamed Ahmed Mohamed and CF v Secretary of State for the Home Department* [2014] EWCA Civ 559 Maurice Kay LJ stated:

> Lurking just below the surface of a case such as this is the governmental policy of "neither confirm nor deny" (NCND), to which reference is made. I do not doubt that there are circumstances in

[23] 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-independent-surveillance-review ("RUSI Report"). Reply Annex No. 19.

> which the courts should respect it. However, it is not a legal principle. Indeed, it is a departure from procedural norms relating to pleading and disclosure. It requires justification similar to the position in relation to public interest immunity (of which it is a form of subset). It is not simply a matter of a governmental party to litigation hoisting the NCND flag and the court automatically saluting it. (para 20).

51. The Government's claim that it is "*only possible to address mischaracterisations in open to a limited extent*" is therefore a matter of choice rather than legal constraint (Observations, §1.2). Indeed, the ISC Report noted that while the Government had placed "*long-standing*" reliance on the NCND policy "*in relation to any allegations about the Agencies' capabilities and operations*", it concluded that, "*greater openness regarding the Agencies' activities is essential*".[24] Accordingly, it recommended that "*the Government will need to adopt a more open approach to the Agencies' activities in order to improve understanding and public trust*".[25] In particular, the ISC called on the Government "*to avow all of the Agencies' intrusive capabilities*".[26]

52. The Council of Europe Commissioner for Human Rights (the "CoE HR Commissioner") likewise recently stated that, "*NCND shields surveillance decisions from effective scrutiny*" and is "*problematic*" because "*it prevents a person from ever knowing if he/she has been the target of surveillance*".[27] Extensive reliance on the NCND principle is unjustified in circumstances where the UK Intelligence Services have used wide interpretations of general powers to justify the operation of sweeping interception programmes whose existence has until recently been concealed from citizens and Parliament.

---

[24] ISC Report, paras 281, 284.
[25] ISC Report, para 285.
[26] ISC Report, p 109, para BBB.
[27] Council of Europe Commissioner for Human Rights, *Memorandum on Surveillance and Oversight Mechanisms in the United Kingdom* (May 2016), para 15, Comm DH(2016)20 ("*Memorandum on Surveillance*"). Reply Annex 28.

4. New facts

53. The Applicants also wish to draw the Court's attention to new evidence, which has come to light since July 2015 (the month of the Applicants' last submissions in this case) and which has not been addressed in the Government's Observations.

54. These facts concern the publication in September 2015 of details of the GCHQ programmes named KARMA POLICE, Black Hole and MUTANT BROTH. They shed important light on the ways in which the UK Government uses bulk interception to create detailed profiles of individuals around the world, whether or not they are of legitimate intelligence interest.

55. The Applicants develop these facts further for the Court in the Factual Appendix. It is important to note that the Applicants have done so not in order to ask this Court or the Government to make express findings or admissions about new allegations. The relevance of these new facts / allegations is to illustrate what is happening – or could be carried out – within the existing legal framework. Whether or not they are avowed or proved, the new facts illustrate that the lack of legal safeguards in UK law permit significant and extensive Government interferences with communications.

5. Intrusiveness of interception of content and communications data

56. 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 (§41). 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,* §77).

57. Citizens of the Council of Europe states live major portions of their lives online. We use the internet to impart ideas, conduct research, explore our sexuality, seek medical advice and treatment, correspond with lawyers, communicate with 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.

58. 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 a communication, which may include the sender and recipient, the date and location from where it was sent, and the type of device used to send it.

59. Communications data is the digital equivalent of having a private investigator trailing a targeted individual at all times, recording where they go and with whom they speak. Communications data will reveal web browsing activities, which might reveal medical conditions, religious viewpoints or 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). Communications data produces an intrusive, deep and comprehensive view into a person's private life,

revealing his or her identity, relationships, interests, location and activities.

60. Moreover, the costs of storing data have decreased drastically, and continue to do so every year. Most importantly, the technical means of analysing data have advanced rapidly so 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.[28]

61. The intrusiveness of communications data is further reflected by the RUSI Report which states that, "*[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*."[29]

C. Intelligence sharing

62. The UK Intelligence Services can access information in several ways. As described above, they can initially intercept the data itself, for example, as it transits over a fibre optic cable. But they may also obtain intercept material under intelligence sharing arrangements with foreign intelligence agencies. For example, a foreign intelligence agency may operate its own bulk interception programme. The information initially intercepted through that programme may be made available, including in bulk, to the UK Intelligence Services.

---

[28] For further reading see THE ECONOMIST, *Data, data everywhere*, 25 Feb. 2010, available at www.economist.com/node/15557443. Reply Annex No. 5.
[29] RUSI Report, para 2.14. Reply Annex No. 19.

1. The nature and scale of the US bulk surveillance programmes

63. As noted in the Government's Observations, the NSA's authority to conduct surveillance of foreign communications stems from two sources: Executive Order 12333 and the Foreign Intelligence Surveillance Act ("FISA") (Observations §1.6(1)).

a. Executive Order 12333

64. Executive Order 12333 sets out the framework for US foreign intelligence activities and permits the agencies to "*collect, retain or disseminate*" a broad range of information, including "*[i]nformation constituting foreign intelligence*", which is defined as "*information relating to the capabilities, intentions and activities of foreign powers, organizations or persons*".[30] Importantly, Executive Order 12333 permits bulk surveillance. Presidential Policy Directive 28 ("PPD-28"), which governs US signals intelligence activities and was issued by President Barack Obama on 17 January 2014, makes this clear by stating that the US "*must…collect signals intelligence in bulk in certain circumstances in order to identify…threats*".[31] Moreover, PPD-28 notably outlines limitations on the *use* – rather than the initial interception – of signals intelligence collected in bulk.

65. The Applicants presented evidence to the IPT, gathered from public reporting of leaked NSA and GCHQ documents, detailing a number of US programmes appearing to fall under the Executive Order 12333 regime and which provide examples of bulk surveillance. These programmes include: [32]

[30] Executive Order 12333, §§2.3, 3.4(d). Reply Annex No. 1.
[31] Presidential Policy Directive 28, §2. Reply Annex No. 13.
[32] King Witness Statement, paras 106-113, 134-141. At the time of the proceedings before the IPT, the Applicants understood these programmes as falling under PRISM and/or Upstream, which are operated pursuant to FISA section 702. This lack of clarity was a result of the fact that information as to the scope and nature of these programmes was and continues to be limited

(1) MYSTIC, which initially intercepts, extracts and stores the communications data of all mobile phone calls made to, from or within targeted countries;

(2) DISHFIRE, which initially intercepts, extracts and stores the content and communications data of 194 million text messages per day;

(3) CO-TRAVELLER, which initially intercepts, extracts and stores nearly 5 billion records a day relating to the location of mobile phones around the world;

(4) MUSCULAR, which initially intercepted and extracted data directly as it transits to and from Google and Yahoo's private data centres;[33] and

(5) XKEYSCORE, a processing and query system used by the NSA and GCHQ for data initially intercepted and extracted through various bulk surveillance programmes.

66. Each of these programmes is described in fuller detail in the Factual Appendix. The US Government has publicly acknowledged a number of these programmes and the details of those acknowledgements are also described further in the Factual Appendix.

67. Apart from evidence the Applicants presented to the IPT, additional information regarding bulk surveillance programmes appearing to operate under the auspices of Executive Order 12333 has also surfaced in the public domain. The Applicants describe four such programmes –

---

primarily to public domain information. Where it is unclear whether a programme is still active, the Applicants have described it in the present tense.

[33] This appears to be a joint programme with GCHQ and/or a programme to which GCHQ has access.

WINDSTOP, INCENSER, RAMPART-A, and MARINA – in further detail in the Factual Appendix.

68. The Government at no point addresses bulk surveillance programmes operated pursuant to Executive Order 12333. Rather, it confines its submissions to a discussion of PRISM and Upstream, two NSA programmes operated pursuant to section 702 of FISA.

b. Section 702 of FISA

69. The earliest Snowden disclosures revealed that the US Government was conducting two surveillance programmes: PRISM and Upstream.[34] PRISM was described as a programme by which the NSA and Federal Bureau of Investigation were "*tapping directly into the central servers of nine leading U.S. internet companies, extracting audio, video, photographs, e-mails, documents and connection logs that enable analysts to track a person's movements and contacts over time.*"[35] Upstream was described as the "*[c]ollection of communications on fiber [sic] cables and infrastructure as data flows past*."[36]

70. As the Government's Observations indicate, the US Government has publicly avowed the existence of both PRISM and Upstream and explained that both programmes operate pursuant to section 702 of FISA (§ 1.5). Generally speaking, FISA governs US foreign surveillance activities

[34] Barton Gellman & Laura Poitras, WASHINGTON POST, *US British intelligence mining data from nine U.S. Internet companies in broad secret program*, 7 June 2013, https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html; Glenn Greenwald & Ewen MacAskill, GUARDIAN, *NSA Prism program taps in to user data of Apple, Google and others*, June 6, 2013, http://www.theguardian.com/world/2013/jun/06/us-techgiants-nsa-data (cited in King Witness Statement, para 91 n 51).

[35] *U.S., British intelligence mining data* (discussed further in King Witness Statement, paras. 94-99).

[36] *U.S., British intelligence mining data*; see also James Ball, GUARDIAN, *NSA's Prism surveillance program: how it works and what it can do*, June 8, 2013, http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google (discussed further in King Witness Statement, paras 100-105).

undertaken within the US.[37] Section 702 of FISA permits the US Attorney General and Director of National Surveillance to authorise surveillance within the US by targeting non-US persons "*reasonably believed to be located outside*" the US.[38]

71. The Government describes PRISM and Upstream as "targeted" rather than "bulk" programmes, and states that they require the NSA to identify a specific person whose communications or communications data are to be obtained (Observations, § 1.6(2)). In the Factual Appendix, the Applicants counter this statement, by detailing why Upstream, in particular, may fairly be characterised as "bulk".

2. The accuracy of the Applicants' descriptions of the US Government's bulk surveillance programmes

72. The Government does not deny that the NSA conducts bulk surveillance, as it clearly does through its programmes under Executive Order 12333. It merely confines its Observations to a discussion of PRISM and Upstream. Even if the Government were correct that PRISM and Upstream are targeted, the factual premise that the US only engages in "targeted" surveillance is false.

3. The nature and scale of US-UK intelligence sharing

73. Intelligence sharing between the US and UK must be viewed within the context of a long-standing arrangement between the intelligence activities of the two countries, along with Australia, Canada and New Zealand,

---

[37] Executive Order 12333 technically applies to all foreign intelligence activities, even where they take place within the US. However, it requires that all activities comply with relevant US statutes, which would include FISA. Thus, to the extent that FISA regulates surveillance undertaken within the US, Executive Order 12333 directs that the US Government comply with that framework. It is also worth noting that FISA does not cover all electronic surveillance that takes place within the US, only such surveillance falling within a particular statutory definition (50 U.S.C. § 1801(f)). The Applicants limit their discussion of FISA to PRISM and Upstream, both of which fall squarely within the FISA framework.

[38] Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to s702 of FISA*, p1, available at https://www.pclob.gov/library/702-Report.pdf.

known as the "Five Eyes" alliance. In 1946, the London Signals Intelligence Board and its American counterpart at that time, the State-Army-Navy Communication Intelligence Board, signed the United Kingdom-United States of America ("UKUSA") Agreement, a post-war "*communications intelligence*" sharing agreement, which was later extended to encompass the other three members of the Five Eyes alliance.[39]

74. Part 3 of the UKUSA Agreement states:

> The parties agree to the exchange of the products of the following operations relating to foreign communications:
> (1) collection of traffic
> (2) acquisition of communication documents and equipment
> (3) traffic analysis
> (4) cryptanalysis
> (5) decryption and translation
> (6)acquisition of information regarding communication organizations, practices, procedures, and equipment.

75. It further stipulates that "*[s]uch exchange shall be unrestricted on all work undertaken except when specifically excluded from the agreement at the request of either party and with the agreement of the other*" but that "*[i]t is the intention of each party to limit such exceptions to the absolute minimum*".

76. The UK Intelligence Services, and in particular GCHQ, are therefore likely to have broad access to the fruits of US communications surveillance, including pursuant to the bulk surveillance programmes described above. This access can take a variety of forms, including direct and unfettered access to raw initially intercepted material, which can then

[39] The National Archives, Newly released GCHQ files: UKUSA Agreement, available at http://www.nationalarchives.gov.uk/ukusa/; *see also* Richard Norton Taylor, *Not so secret; deal at the heart of UK-US intelligence,* The Guardian, 25 June 2010, https://www.theguardian.com/world/2010/jun/25/intelligence-deal-uk-us-released.

be extracted, filtered, stored, analysed and/or disseminated; access to information stored in a database, which can then be analysed and/or disseminated; and access to intelligence reports produced on the basis of analysis by the NSA or other US intelligence agencies.

77. Several Executive Order 12333 programmes specifically permit GCHQ access to material intercepted by the NSA. Under DISHFIRE, for example, it seems that GCHQ has access to the communications data of hundreds of millions of text messages intercepted, extracted and stored by the NSA.[40] XKEYSCORE, the NSA's "*processing and query system*", storing "*full-take data*" intercepted and extracted through various NSA bulk surveillance programmes, is accessible to several foreign governments, including the UK.[41] GCHQ also appears to have access to various NSA databases, including MARINA, the NSA's communications data repository.[42] One of the Snowden disclosures revealed a GCHQ legal training slideshow, which suggests that gaining access to such databases is relatively easy, requiring analysts to undergo "'*multiple choice, open-book' tests done at the agent's own desk on its 'iLearn' system*".[43]

D. Summary of the Applicants and the nature of their work

78. The Applicants are 10 non-governmental human rights organisations based inside and outside the UK: the American Civil Liberties Union, Amnesty International, Bytes for All, the Canadian Civil Liberties Association, the Egyptian Initiative for Personal Rights, the Hungarian

---

[40] James Ball, THE GUARDIAN, *NSA Collects Millions of Text Messages Daily in 'Untargeted' Global Sweep*, (Jan. 16, 2014) available at www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep (cited in King Witness Statement, para 106). Reply Annex No. 11.

[41] Morgan Marquis-Boire, Glenn Greenwald & Micah Lee, INTERCEPT: *XKEYSCORE: NSA's Google for the World's Private Communications,* July 1, 2015, https://theintercept.com/2015/07/01/nsas-google-world-private-communications/ (cited in King Witness Statement, paras 139-141).

[42] See slide titled "Quantum SIGDEV – Marina", available at https://www.spiegel.de/images/image-583972-galleryV9-mmeg.jpg. Reply Annex No. 37.

[43] Ewen MacAskill & James Ball, *Portrait of the NSA: no detail too small in quest for total surveillance*, 2 Nov. 2013, https://www.theguardian.com/world/2013/nov/02/nsa-portrait-total-surveillance (cited in King Witness Statement, para 50).

Civil Liberties Union, the Irish Council for Civil Liberties, the Legal Resources Centre, Liberty and Privacy International.

79. Each of the Applicants is concerned that its communications (and communications data), as well as those of its partners, supporters and victims of human rights violations, could be obtained by the UK either through its bulk interception programme or via intelligence sharing with the US. The Applicants defend and promote respect for fundamental human rights, including the rights to privacy and freedom of expression, through research, litigation, advocacy and public education. This work may include campaigning and holding governments to account. It may also include commenting on the foreign affairs of other countries, such as the national security policy of the US or UK.

80. As part of their work, the Applicants also communicate on a regular basis, in private, with a wide range of individuals and organisations, both nationally and internationally. The persons with whom they communicate include other non-governmental organisations, human rights defenders, journalists, lawyers, prisoners, political activists, victims of human rights abuses, politicians, government officials and whistle-blowers.

81. The Applicants and their staff members communicate using a variety of methods, including email, text messages, phone calls, video calls, social media and instant messaging. The information contained in their communications – as well as the dates, times and identities of the sender/recipient of each communication – frequently include material that is confidential and, in some cases, legally privileged. The integrity of the Applicants' communications and the protection of their sources are of paramount importance in order for them to effectively fulfil their role to seek, receive and impart information related to human rights.

III. SUMMARY OF THE CURRENT LEGAL FRAMEWORK

A. UK bulk interception under the s8(4) Regime

82. Section 5(1) of RIPA empowers the Secretary of State to issue a warrant "*authorising…the interception…of the communications described in the warrant*". Section 8 provides for two types of interception warrants: (1) a "targeted" warrant under s8(1) and (2) an "untargeted" warrant under s8(4). The s8(4) Regime applies where the Government seeks "*the interception of external communications in the course of their transmission by means of a telecommunication system.*" (s8(5)(a)). Section 20 of RIPA defines an "*external communication" as "a communication sent or received outside the British Islands*." Section 5(6) provides that "*conduct authorised by an interception warrant shall…include…conduct for obtaining related communications data*."

83. The s8(4) Regime operates as follows. First, an application must be made by one of the persons listed in s6(2), which includes the Director-General of MI5, the Chief of MI6 and the Director of GCHQ. Second, the Secretary of State shall not issue a warrant "*unless he believes that (a) the warrant is necessary on grounds falling within subsection (3); and (b) that the conduct authorised by the warrant is proportionate to what is sought to be achieved*". Section 5(3) provides that a warrant is considered "*necessary*" if "*it is necessary (a) in the interests of national security; (b) for the purpose of preventing or detecting serious crime; [or] (c) for the purpose of safeguarding the economic well-being of the United Kingdom*." Third, when the Secretary of State issues a warrant, it must be accompanied by "*a certificate…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 sections 5(3)(a), (b) or (c).*" (s8(4)(b)).

84. As stated by the Government in its Observations:

> The s. 8(4) regime does not impose any express limit on the number of external communications which may fall within 'the description of communications to which the warrant relates' in s. 8(4)(a). So in principle, it authorises the interception of all communications passing down a bearer or bearers. (§ 2.65).

85. Section 15 enumerates "*general safeguards*" requiring "*the Secretary of State to ensure, in relation to all interception warrants"* that certain *"arrangements are in force*". Those arrangements relate to storage, dissemination and destruction of intercepted material.

86. Section 16 provides "*extra safeguards*" applying exclusively to s8(4) warrants. Those safeguards require that "*the intercepted material is read, looked at or listened to…[only] to the extent*" that it is not "*(a)…referable to an individual who is known to be for the time being in the British Islands; and (b) has as its purpose…the identification of material contained in communications sent by him, or intended for him*." However, s16(3) provides for an exception where the Secretary of State certifies "*(a)…that the examination of material selected according to factors referable to the individual in question is necessary as mentioned in subsection 5(3)(a), (b) or (c); and (b) the material relates only to communications sent during a period specified in the certificate that is no longer than the permitted maximum*."

87. Section 71 requires the Secretary of State to "*issue one or more codes of practice"* relating to the interception of communications. The Interception of Communications Code of Practice was first issued in July 2002. The current Code of Practice was issued in January 2016 (hereinafter the "Code of Practice"). In March 2016, the Government published a new draft Code of Practice.

88. During the proceedings, the Government provided the Applicants with a witness statement from Charles Farr ("Farr Witness Statement"), the

Director-General of the Office for Security and Counter Terrorism at the Home Office.[44] In that statement, Farr indicates that "*the full details of the [RIPA] sections 15 and 16 arrangements are (and always have been) kept confidential*" and asserts that "*they cannot safely be put into the public domain without undermining the effectiveness of interception methods*."[45] These arrangements remain secret. The Government presented them to the IPT in a closed hearing but they were not disclosed to the Applicants.

B. US-UK intelligence sharing regime

89. When the Applicants initiated proceedings before the IPT, there was no information in the public domain setting out the rules governing intelligence sharing between the UK Government and foreign intelligence agencies, including those of the US.

90. The Applicants note that, prior to their initiation of proceedings, on 10 June 2013, the Secretary of State for Foreign and Commonwealth Affairs addressed Parliament. In that statement, he asserted that the UK Government complies with UK law with respect to information it obtains from foreign governments and referred to RIPA.[46] The Government later admitted, during the IPT proceedings, that RIPA was not applicable to intelligence sharing. In its 5 December 2014 judgment, the IPT held "*[i]t is common ground that RIPA is not applicable to a case where there has not been interception of communications by the Respondents, but receipt of intercepted communications by the Respondents from the NSA*".[47]

---

[44] Witness Statement of Charles Blandford Farr on behalf of the Respondents, Exhibit CF1 (16 May 2014) (lodged with the Court in the List of Accompanying Documents in the original Application).
[45] Farr Witness statement, paras 100-101, and quoted in the *Liberty & Others v GCHQ & Others* [2014] UKIPTrib 13_77-H, at para 77 ("First IPT Judgment").
[46] Privacy International Grounds, para 26, (lodged with the Court in the List of Accompanying Documents in the original Application).
[47] First IPT Judgment, para 17.

91. Before the IPT, the Government cited several statutes, which generally authorise the functions of the UK Intelligence Services.[48] Thus, for example, it cited to s1 of the Security Service Act 1989, which provides, *inter alia*, that "*[t]he function of [MI5] shall be the protection of national security*" and to s2(2)(a), which articulates the Director-General's duty to ensure "*that there are arrangements for securing that no information is obtained by the Service except so far as necessary for the proper discharge of its functions*". The Government referred to analogous provisions authorising the functions of MI6 and GCHQ in the Intelligence Services Act 1994. It also relied on the Counter-Terrorism Act 2008, which sets out, in similarly general terms, that "*[i]nformation obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions.*"

92. Apart from these bare statutory authorisations, the Government alluded to secret internal guidance governing intelligence sharing.

93. These arrangements remain secret. The Government presented them to the IPT in a closed hearing, following which it disclosed a "note".[49] The "note" contains no heading and just a few paragraphs of text, which appear to summarise some of the arrangements. It is unclear whether the note is an actual policy, part of a policy, a summary of a policy or a summary of submissions made by the Government in the closed hearing. It is also unclear whether the note sets out an approach that the Government considers 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. The date on which the arrangements came into force is unknown. It is equally unknown if the arrangements have ever been altered or amended.

[48] First IPT Judgment, para 18(x)-(xi).
[49] Disclosed Note. "Reply Annex" no. 42; *see also* First IPT Judgment, para 47.

94. On 27 January 2016, the Government published an amended Code of Practice,[50] which essentially incorporates the text of the "note" disclosed during the IPT proceedings and provides no additional elaboration on any "arrangements" governing intelligence sharing.

C. Oversight mechanisms

95. In its Observations, the Government relies upon several oversight mechanisms. It submits that the IPT and the ISC provide oversight of both the bulk interception and intelligence sharing regimes (Observations, §6). It further submits that the IOCC "*provides an important means by which the exercise by the Intelligence Services of their interception powers under RIPA may be subject to effective oversight whilst maintaining appropriate levels of confidentiality*" (Observations, §2.106).

1. The Investigatory Powers Tribunal

96. The Applicants note two factual developments with respect to the IPT, which indicate that it is a flawed mechanism, ill-equipped to provide effective oversight.

97. First, the Government claims that *"[a]ny person may bring a claim in the IPT: and they need not be able to adduce any evidence that the Intelligence Services have engaged in relevant 'conduct' in relation to them, in order to have their complaint considered and determined*." (Observations, §3.25; see also §§2.121-122, 4.39). Yet, in separate proceedings before the IPT, the Government made a contradictory assertion, arguing that "*individuals cannot claim to be victims occasioned by the mere existence of secret measures or of legislation pertaining to secret measures*" and, rather, "*must*

[50] Home Office, *Interception of Communications Code of Practice*, Jan. 2016 ("Jan. 2016 Code of Practice").

be able to show that, due to their personal situation, they are potentially at risk of being subjected to such measures."[51] In May 2016, the IPT agreed with the Government and instituted this new test.[52] The IPT has therefore abandoned this Court's description in *Kennedy* of "*the extensive jurisdiction of the IPT to examine any complaint of unlawful interception. Unlike in many other domestic systems, any person who suspects that his communications have been or are being intercepted may apply to the IPT.*" (§167).

98. Second, during the course of another set of proceedings before the IPT, the Government disclosed a document, which is partially redacted, entitled "*Visit of the IPT to Thames House – 28 September 2007*".[53] The document reveals that in 2007, MI5 briefed some of the members of the IPT in secret at its headquarters. It further reveals that, during the course of the briefing, MI5 informed the IPT that their existing (and intended future) practice was neither to search nor disclose any bulk data holdings relating to an applicant to the IPT. As a result, in cases where those datasets include data relating to a particular complainant, MI5 would nevertheless inform the IPT that it held no pertinent information. The members of the IPT who attended the briefing include Mr Robert Seabrook QC, who also sat on the IPT panel during the proceedings in this case.

99. The briefing undermines the purported independence of the IPT. The role of the IPT should be restricted to hearing evidence and argument in cases brought before it. A secret briefing from the UK Intelligence Services, outside the context of court proceedings, relating to the agencies' response

[51] Respondents' Preliminary Submission in Response to Privacy International Campaign, 9 Dec. 2015. This case followed the judgments in the present case. The claim consists of 663 applicants who are requesting the IPT to determine whether their communications, like those of Amnesty International and the Legal Resources Centre in the present case, were unlawfully subject to surveillance. Reply Annex No. 24.

[52] *Human Rights Watch Inc. et al. v. Secretary of State for the Foreign & Commonwealth Office et al.*, [2016] UKIP Trib15-165-CH, 16 May 2016, para 46, available at http://www.ipt-uk.com/docs/Human_Rights_Watch_FINAL_Judgment.pdf.

[53] Letter from Bhatt Murphy Solicitors to IPT, with attachments. Reply Annex, no. 34.

to complaints and the conduct of disputes subject to IPT proceedings is difficult to reconcile with the IPT's role as a neutral arbiter of legal complaints against those very agencies. Moreover, the IPT failed to disclose, in this (or any other) case that a briefing of relevance to the issues in this case had taken place, that a member of the IPT panel had attended such briefing, or that a protocol was in place that might mean relevant material was neither disclosed to the IPT nor reviewed by it.

100. In light of the contents of the briefing, it would appear that the IPT has failed to consider whether any material held in bulk by MI5 was initially intercepted, extracted, filtered, stored or disseminated unlawfully. Each of these steps constitutes a significant interference with Articles 8 and 10 and gives rise to real risks of unlawful conduct by the Government. The IPT has not considered the key evidence available to it.

2. The Intelligence and Security Committee

101. The Applicants note several important structural and practical limitations on the ISC's oversight role with respect to both the Government's bulk interception and intelligence sharing activities.

102. First, the ISC is not a full-time oversight body. It is a parliamentary committee composed of nine Members of Parliament ("MPs").

103. Secondly, the ISC lacks sufficient independence from the Executive. The Prime Minister has sole power to nominate MPs to the ISC. She also has power to veto publication of any material by the ISC.[54] For these reasons, the CoE HR Commissioner has expressed "*concern that the executive control of this Committee may be too strong*".[55] In addition, the Secretary of State may veto disclosure of evidence to the ISC.[56]

[54] Intelligence Services Act 1994, c. 13 (UK).
[55] *Memorandum on Surveillance*, para 9. Reply Annex No.28.
[56] House of Commons *Briefing Paper No. 02178 on the Intelligence and Security Committee* (2 February 2016) explains that: "*The Secretary of State may only veto disclosure of information on*

104. Thirdly, the ISC suffers from significant under-resourcing. On this point, the CoE HR Commissioner has remarked that he "*was struck by the fact that this important Committee only has six permanent staff members*" and "*call[ed] for adequate financial and human resources to be given to the ISC.*"[57]

105. Finally, the ISC has historically devoted little attention to scrutinising the Government's interception programmes and none to its intelligence sharing activities. For example, the 2012/13 Annual Report made no reference to the interception of communications.[58] The 2011/2012 Annual Report contained passing reference to interception in a section explaining why it may be necessary to grant the police and intelligence services greater access to communications data.[59] The 2010/2011 Annual Report again made only passing reference to interception in the context of a two-page section summarising the role of the IPT and the Commissioners. Despite the fact that the IPT had been in existence since RIPA was enacted a decade earlier, the report noted that a meeting between the ISC and IPT "*was the first time that the Committee had an opportunity to hear about the work of the I[PT]*".[60] Finally, the 2009/2010 Annual Report devoted just three short paragraphs to interception in the context of considering whether intercept material should be admissible as evidence in UK legal proceedings (which it is not).[61]

---

two grounds: that it is sensitive and should not be disclosed to the ISC in the interests of national security; or that it is information of such a nature that, if the Secretary of State were requested to produce it before a Departmental Select Committee of the House of Commons, the Secretary of State would consider (on grounds not limited to national security) it proper not to do so." Reply Annex No. 25.

[57] *Memorandum on Surveillance*, para 9. Reply Annex No.28.

[58] INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT, *ANNUAL REPORT, 2012-13*, HC 547 (UK). Reply Annex No.12.

[59] INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT, *ANNUAL REPORT, 2011-12*, Cm 8403, paras. 113-121 (UK). Reply Annex No. 10.

[60] INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT, *ANNUAL REPORT, 2010-11*, Cm 8114, para 282 (UK). Reply Annex No. 9.

[61] INTELLIGENCE AND SECURITY COMMITTEE OF PARLIAMENT, *ANNUAL REPORT, 2009-10*, Cm 7844, paras 58-60 (UK). Reply Annex No. 8.

3. The Interception of Communications Commissioner

106. The IOCC is only in a position to provide limited *post facto* oversight of the Government's interception activities. In particular, the Applicants emphasise that the IOCC's position is part-time. In 2014, the Home Affairs Committee of the House of Commons, in remarking on this point, noted that it had "*some sympathy with the assertion…that the Commissioners are good people doing impossible jobs*."[62] It ultimately concluded that it had "*serious doubts that…the [IOCC] role…should be part-time*" and recommended that the position be made full-time.[63]

107. The Applicants further note that the IOCC has no power to refer a case to the IPT for a remedy. Nor is he permitted to notify the victim of any excessive or unlawful interception. The Applicants discuss these points further in its analysis of its Article 8 claim below.

D. Recognition that the current legal framework is inaccessible, outdated and unfit for purpose

108. Since the IPT delivered its judgments in December 2014 and February 2015, a number of detailed reviews have been undertaken by Parliament, the Independent Reviewer, RUSI and various European Union and Council of Europe bodies. Those reports consistently acknowledge that the existing legal frameworks for the bulk interception and intelligence sharing lack transparency are unfit for purpose and require overhaul.

109. In March, June, and July 2015, the ISC, Independent Reviewer and RUSI respectively published reports on the effectiveness of existing legislation relating to the Government's investigatory powers. The ISC Report observed that the UK's existing legal framework regulating Government surveillance powers "*has developed piecemeal*" and is "*unnecessarily*

[62] House of Commons Home Affairs Committee, *Counter-terrorism*, HC 231, 9 May 2014, para 165. Reply Annex No. 15.
[63] Ibid., para 167.

complicated", "*difficult to understand*" and "*unnecessarily secretive*".[64] The ISC accordingly expressed *"serious concerns about the resulting lack of transparency, which is not in the public interest.*"[65] In particular, the ISC criticised the absence of express powers governing major surveillance activities, noting specifically that "*it is inappropriate that many key capabilities – for example, the exchange of intelligence with international partners – are implicitly authorised rather than formally defined in statute*".[66] The ISC concluded that a "*fundamental review*" of the existing framework is "*overdue*" [67] and that "*the entire legal framework governing the intelligence and security Agencies needs replacing*".[68]

110. The Independent Reviewer Report echoed the serious concerns expressed by the ISC about the fundamental deficiencies in the legal framework governing surveillance and interception powers. With respect to RIPA, in particular, the Independent Reviewer described it as "*complex, fragmented and opaque*" and "*extraordinarily difficult to understand and to apply*."[69] He further observed that "*RIPA has been overtaken by developments in technology, such that in the view of many it is no longer fit for purpose*" and that the "*distinctions laid out in the regime are increasingly defunct, particularly in light of powerful tools for composite analysis."*[70] He concluded that "*[t]his state of affairs is undemocratic, unnecessary and – in the long run – intolerable*."[71]

111. The Independent Reviewer also commented on the failure of existing legal and political oversight to inform the public about the nature of the Government's surveillance techniques. He noted: "*Intelligence is said to have been harvested and shared in ways that neither Parliament nor*

[64] ISC Report, pp 2, 103, para 275.
[65] ISC Report, p 2.
[66] ISC Report, p 7.
[67] ISC Report, pp 8, 118, para WW.
[68] ISC Report, p 8.
[69] A Question of Trust, para 12.20.
[70] A Question of Trust, para 12.24.
[71] A Question of Trust, para 35.

public predicted, and that some have found disturbing and even unlawful. Yet this was brought to light not by the commissions, committees and courts of London, but by the unlawful activities of Edward Snowden."[72] The Independent Reviewer observed that a "*[p]articularly striking*" effect of the Snowden revelations was "*the realisation of the extent to which communications were being intercepted in bulk*", raising "*the potential (if not properly regulated) for spying on a truly industrial scale*".[73]

112. The RUSI Report concluded that "*the present legal framework authorising the interception of communications is unclear, has not kept pace with developments in communications technology, and does not serve either the government or members of the public satisfactorily*".[74] It further recommended that the framework undergo "*a radical overhaul*", which "*must include an enhanced role for the judiciary*".[75]

113. In February 2016, the Joint Committee on the Draft Investigatory Powers Bill published a report. The Committee referred to the reports by the ISC, the Independent Reviewer and RUSI and observed that: "*it is telling that all three reviews found the current legislative framework provided by RIPA and other legislation to be essentially unfit for purpose and in need of replacement by a single piece of statute*".[76]

114. On 17 May 2016, the CoE HR Commissioner published a "*Memorandum on surveillance and oversight mechanisms in the United Kingdom*", which repeated a number of the key criticisms summarised above. It observed that, in addition to RIPA, "*a number of other Acts allow for the interception of communications and provide for the acquisition of communications data. Indeed the legal framework for this area spans some 65 Acts of*

[72] A Question of Trust, para 13.2.
[73] A Question of Trust, para 2.31.
[74] RUSI Report, p xi. Reply Annex No. 19.
[75] RUSI Report, p xii.
[76] Joint Committee on the Draft Investigatory Powers Bill, *Report*, para 30, HL Paper 93 – HC 651. Reply Annex No. 26.

Parliament and is generally agreed to be extremely complicated."[77] The memorandum also acknowledged that the ISC, Independent Reviewer, and RUSI had all "*concluded that the current framework was outdated, unworkable and in need of reform*" and that their "*reports highlighted the need for greater transparency, more stringent safeguards and better oversight.*"[78]

115. In light of the powerful criticisms summarised above, the Government's submission that the existing legal regimes for bulk interception and intelligence sharing are accessible, clear and effective is unsustainable.

IV. SUMMARY OF THE PROCEDURAL HISTORY

116. The Applicants summarise the IPT proceedings below, which are described in greater detail at paras 9-21 of the Additional Submissions.

117. Between June and December 2013, each of the Applicants lodged complaints before the IPT. On 14 February 2014, the IPT directed that the complaints be joined.

118. Between 14 and 18 July 2014, the IPT held an open hearing. The hearing concerned issues of law on the basis of assumed hypothetical factual premises agreed between the parties. The IPT ordered that the hearing be held *inter partes* and in public.

119. On 10 September 2014, the IPT held a closed hearing at which it considered, *inter alia*, the secret arrangements governing the bulk interception and intelligence sharing regimes. The applicants were not represented at the hearing.

[77] *Memorandum on Surveillance*, para 3. Reply Annex No. 28.
[78] *Memorandum on Surveillance*, para 5.

120. On 9 October 2014, the IPT notified the Applicants that it had "*concluded that there was closed material relied upon by the [Government] which could be disclosed to the parties*". The Applicants subsequently received an untitled "note", appearing to summarise some of the Government's secret arrangements governing its intelligence sharing regime. The Government later produced several new versions of the note.

121. On 5 December 2014, the IPT issued its first of three judgments, which held, *inter alia*, that there was "*no contravention of Articles 8 or 10 by reference to*" the bulk interception or intelligence sharing regimes.

122. On 6 February 2015, the IPT issued its second judgment, which held that,

> "prior to the disclosures made and referred to in the Tribunal's Judgment of 5 December 2014, the regime governing the soliciting, receipt, storing and transmitting by UK authorities of private communications of individuals located in the UK, which have been obtained by US authorities…contravened Articles 8 or 10 ECHR, but now complies".[79]

123. On 22 June 2015, the IPT issued its third judgment. The IPT found that the "*email communications*" of the Egyptian Initiative for Personal Rights "*were lawfully and proportionately intercepted and accessed, pursuant to s.8(4) of RIPA*" but that "*the time limit for retention permitted under the internal policies of GCHQ…was overlooked in regard to the product of that interception, such that it was retained for materially longer than permitted under those policies.*" The IPT determined that "*the breach constitutes…a breach of Article 8 ECHR*" and ordered GCHQ "*to destroy any of the…communications that were retained for longer than the relevant retention time limit.*".

124. The IPT further found that "*communications from an email address associated with*" the South African Legal Resources Centre were lawfully

[79] *Liberty et al. v. GCHQ et al.*, [2015] 3 AER 212, 6 Feb. 2015, para 23 ("Second IPT Judgment").

and proportionately "*intercepted and selected for examination pursuant to s.8(4) of RIPA*" but that "*the procedure laid down by GCHQ's internal policies for selection of the communications for examination was in error not followed in this case*." The IPT determined that this breach also constituted "*a breach of the Claimant's Article 8 rights*." The IPT further determined that as "*no record was retained, there is no cause for any order for destruction*."

125. The IPT held that "no determination" was made with respect to the remaining eight Applicants.

126. On 1 July 2015, the IPT notified the Applicants that the finding relating to the Egyptian Initiative for Personal Rights "*in fact related to Amnesty International Ltd*". The IPT provided no explanation for the error in its published judgment.

PART 2: APPLICANTS' REPLY TO THE UK GOVERNMENT'S OBSERVATIONS

I. BULK INTERCEPTION UNDER S8(4) BREACHES THE CONVENTION

127. The interception of communications and communications data is an interference with privacy. As such, that interference must be "in accordance with law" and "necessary in a democratic society".

128. These requirements exist because secret surveillance must be subject to a clear and public legal regime, with adequate safeguards to protect liberty and prevent arbitrary use. The Independent Reviewer explained the importance of both safeguards and firm limits on the use of mass surveillance technology. Not everything that is useful to a secret intelligence service is permissible in a democratic society:

> The capabilities of the state are subject to technical or cost-based limits. But if the acceptable use of vast state powers is to be guaranteed, it cannot simply be by reference to the probity of its servants, the ingenuity of its enemies or current technical limitations on what it can do. Firm limits must also be written into law: not merely safeguards, but red lines that may not be crossed… Some might find comfort in a world in which our every interaction and movement could be recorded, viewed in real-time and indefinitely retained for possible future use by the authorities. Crime-fighting, security, safety or public health justifications are never hard to find… The impact of such powers on the innocent could be mitigated by the usual apparatus of safeguards, regulators and Codes of Practice. But a country constructed on such a basis would surely be intolerable to many of its inhabitants. A state that enjoyed all those powers would be truly totalitarian, even if the authorities had the best interests of its people at heart. There would be practical risks: not least, maintaining the security of such vast quantities of data. But the crucial objection is of principle".[80]

[80] A Question of Trust, paras 13.18-13.21.

A. Intercepting communications data is as intrusive as intercepting content

129. As an initial matter, the s8(4) Regime involves the interception of both communications and communications data. The Government contends that, "*[i]ntercepting communications is in general more intrusive than obtaining communications data*" and that this proposition *"is as true for aggregated sets of information as for individual items of information*" (Observations, §§4.29-4.31).

130. The Government's Observations fail to reflect the intrusiveness of initially intercepting, extracting, filtering, storing, analysing and disseminating communications data. In *Digital Rights Ireland* the Advocate General correctly recognised that the collection and use of communications data makes it possible "*to create a both faithful and exhaustive map of a large portion of a person's conduct strictly forming part of his private life, or even a complete and accurate picture of his private identity*" (§§72-74). In its subsequent judgment, the CJEU observed that: "*data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, 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*" (§27).

131. More recently, in *Tele2 Sverige* and *Watson* the Advocate General "*emphasise[d] that the risks associated with access to communications data (or 'metadata') may be as great or even greater than those arising from access to the content of communications*" (§259). The Advocate General provided examples of hypothetical situations which demonstrate that,

"'metadata' facilitate the almost instantaneous cataloguing of entire populations, something which the content of communications does not" (§§257-259).

132. The EU Working Party on data protection and privacy has likewise warned that "*metadata often yield information more easily than the actual content of our communications do*."[81]

133. Courts in the United States have similarly recognised the highly intrusive nature of the interception and examination of communications data. The United States Court of Appeals for the Second Circuit, in considering the NSA's bulk interception of domestic telephone metadata programme pursuant to §215 of the PATRIOT Act, noted "*[t]hat telephone metadata do not directly reveal the content of telephone calls, however, does not vitiate the privacy concerns arising out of the government's bulk collection of such data*".[82] Indeed, the Court observed that *"[t]he more metadata the government collects and analyses, furthermore, the greater the capacity for such metadata to reveal ever more private and previously unascertainable information about individuals*."[83]

134. In the present proceedings, therefore, the IPT rightly concluded that, when assessing compatibility with Article 8, the same legal principles govern the interception and examination of communications data as apply to the interception and examination of content.[84]

---

[81] Article 29 Data Protection Working Party, *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes* (10 April 2014), pp 4- 5. Reply Annex No. 14.
[82] ACLU v. Clapper, 785 F. 3d 787 (2d Cir., 2015). Reply Annex No. 18.
[83] ACLU v. Clapper.
[84] First Judgment, para 114.

B. Foreseeability and accessibility

135. In *Zakharov* the Court "*note[d] from its well established case-law that the wording 'in accordance with law' requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law*". It elaborated that "*[t]he law must thus meet quality requirements; it must be accessible to the person concerned and foreseeable as to its effects*" (§228).

136. In addition, the Court in *Zakharov* emphasised that "*the reference to 'foreseeability' in the context of interception of communications cannot be the same as in many other fields*." Given that "*where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident*", the Court stated that it is "*therefore essential to have clear, detailed rules*" regulating interception "*especially as the technology available for its use is becoming increasingly more sophisticated*." Thus, "*[t]he domestic law must be sufficiently clear to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures*" (§229).

137. The Applicants submit, at the outset, that the requirements of foreseeability and accessibility are not met where RIPA – the principal legislation governing the bulk interception regime – has been variously described by:

(1) the ISC as "*unnecessarily complicated*", "*difficult to understand*", and "*unnecessarily secretive*";
(2) the Independent Reviewer, as *"complex, fragmented and opaque"*, and *"extraordinarily difficult to understand and apply"; and*
(3) by RUSI as "*unclear*" and *failing to "serve either the government or*

members of the public satisfactorily."[85]

138. Moreover, the key arrangements pertaining to RIPA safeguards under ss 15 and 16 remain secret and unavailable to the public.

1. "Internal" versus "external" communications

139. A key element of the lack of foreseeability of the s8(4) Regime is the lack of clarity concerning definition and scope of "external" communications. Section 20 of RIPA defines an *"external communication*" as "*a communication sent or received outside the British Islands*". The practical application of that definition in the modern communications context – where a message between two individuals based in London might circumnavigate the world – has rendered the application of the s8(4) Regime arbitrary and unforeseeable.

140. The concept of an "*external communication*" was criticised from the inception of RIPA. During the parliamentary debates on what became section 20 RIPA, Lord Phillips of Sudbury said that, "*the meaning of the word 'external' is not clear*". In particular, he expressed concern as to whether or not a communication between two people within the British Islands, but which was routed through outside the British Islands, constituted an external communication. He was assured in Parliament it did not.[86]

141. However, the Farr Witness Statement sets out what the Government considered to be an "external" communication as applied to modern internet communications. In particular, the Government disclosed that it distinguished between emails and other forms of internet-based communications. It explained, for example, that it always considers a

[85] See paras 108-115.
[86] Hansard, 19 June 2000, HL Deb (2000), vol. 614, cc. 97-146, col. 98 (UK). Reply Annex No. 2.

message to "friends" on Facebook to be "external" because Facebook is a "*platform*".[87] This categorisation holds true even if that message was traveling between two "friends" based in the same city in the UK.

142. The Government's revelation contradicts the assurance given in Parliament during debates on RIPA and the explanation in the Code of Practice 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*".[88] At the same time, it remains unclear what other online services falls within the Government's definition of a "*platform*", such that messages exchanged on it would be deemed external. The term "*platform*" appears nowhere in RIPA or in the Code of Practice.

143. Unsurprisingly, the ISC Report found, in March 2015 that, "*[t]he current legal framework of external and internal communications has led to much confusion*" and "*lacks transparency*".[89] It concluded that "*[t]he 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.*"[90] The Government has not done so.

144. The Independent Reviewer similarly noted, in his June 2015 report that "*the distinction" between internal and external communications "is outdated in the context of internet communications and should be abandoned.*"[91]

145. The Government rejects these conclusions. It reiterates 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.*" (Observations, §4.69). But this is a

[87] Farr Witness Statement, paras 133-141.
[88] Code of Practice, para 6.5.
[89] ISC Report, pp 2, 113, para O.
[90] ISC Report, p 113, para O.
[91] A Question of Trust, para 14.76.

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.

146. 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 UK Intelligence Services on which cables to tap (Observations, §§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 entire communications cables. 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).

147. In response, the Government further asserts that clarification would be both "*impractical*" and "*pointless*" (Observations, §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 bulk interception. Convenience is not a good reason for an absence of foreseeability in interception legislation.

C. The framework for analysing the Applicants' claims

148. The Government relies on RIPA's confusing framework to assert that its bulk interception regime is in accordance with law.[92] A decade ago, in *Weber and Saravia v Germany* (2008) 46 EHRR SE5 (decided in 2006) this Court, when considering admissibility, identified the minimum safeguards for communications surveillance that must be satisfied to protect against arbitrary interference and abuse. The s8(4) Regime does not satisfy the requirements of *Weber*, as is explained in more detail below. The Applicants also contend that the *Weber* safeguards are no longer sufficient to address modern forms of communications surveillance in any event. When *Weber* was decided, smartphones did not exist. Facebook was a website for university students, Twitter had not been invented and Gmail was not available in Europe. The public understanding of the intrusive power of the storage and analysis of large quantities of private data was in its infancy.

149. The Government maintains that there is "*no essential difference of kind*" between the s8(4) Regime and the "strategic monitoring" addressed in Weber (Observations, para 4). Rather, it insists that what has changed is "*the sophistication of terrorists and criminals in communicating over the internet in ways that avoid detection"* (para 5).

150. The Government is wrong. The "strategic monitoring" in *Weber* involved interception of international wireless telephone communications, which

[92] The Government also relies on this Court's judgment in *Liberty*, which considered whether the statutory regime for conducting interception in relation to "external communications" was in accordance with law. The Applicants note, however, that, the Government relied in *Liberty* on the statutory framework existing at that time, the Interception of Communications Act 1985 ("IOCA"), which preceded RIPA. The Government raised a number of arguments similar to those raised in the present case. First, it asserted that the relevant statutory provisions could not provide greater clarity without an unacceptable risk to national security. Second, it submitted that there were adequate safeguards contained in s6 of IOCA (which are similar to those contained in ss 15 and 16 of RIPA). Finally, it argued that IOCA was complemented by a range of oversight mechanisms, including the IOCC and the jurisdiction of a specialist Tribunal. The Court rejected these arguments and ultimately found that the IOCA regime for intercepting external communications was not in accordance with law under Article 8.

comprised "*merely some ten percent of all telecommunications*".[93] In addition, "*the persons concerned had to have taken part in an international telephone conversation via satellite connections or radio relay links*" (§97). In practice, the Government could only initially intercept a portion of those communications, namely where satellite signals or radio relay links "*covered the area in which [an intercept] station was located*." (§31). Finally, "*the persons concerned either had to have used catchwords capable of triggering an investigation into the dangers listed…or had to be foreign nationals or companies whose telephone connections could be monitored deliberately in order to avoid such dangers*." (§97). In practice, "*monitoring was restricted to a limited number of foreign countries*" and the legislation prohibited "*the telephone connections of German nationals living abroad could not be monitored directly*." (§110). Thus, "*[t]he identity of persons telecommunicating could only be uncovered in rare cases in which a catchword had been used*." (§110).

151. By contrast, in the present case, as discussed below, the category of persons liable to affected by s8(4) is every person who uses the internet. The s8(4) Regime does not meaningfully differentiate between "internal" and "external" communications, nor does it apply "catchwords" at the point of initial interception. It also lacks a prohibition against monitoring the communications of UK nationals living abroad. Finally, GCHQ not only has considerable resources but has also deployed them to uncover the identities of persons communicating. Consider, for example, its ability to 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, paras 4-9).

[93] See section 3(1) of the G10 Act and *Weber*, §§ 26, 27, 30 and 31. Fixed-line communications could be intercepted for the sole purpose of preventing an armed attack on Germany.

152. In any event, the Applicants submit that the reasoning of the Third Section in *Weber* – while sufficient to address the question of admissibility in that case – is too slender a basis upon which to draw conclusions in the present case. Indeed, this Court has moved on from *Weber* in its jurisprudence.

153. In its recent case law, the Court has made it clear that significant developments in electronic communications and covert surveillance capabilities must be matched by commensurate developments in the minimum legal safeguards applicable to the use of covert surveillance powers. In *Szabó* the Court noted that "*the mere existence*" of legislation authorising the monitoring of electronic communications "*involve[s], for all those to whom the legislation could be applied, a menace of surveillance*" (§53). At the same time, the Court highlighted that *"[g]iven the technological advances since the* Klass *case, the potential interferences with email, mobile phone and Internet services as well as those of mass surveillance attract the Convention protection of private life <u>even more acutely</u>*" (§53, citing *Klass*, §41). In particular, the Court noted the "*remarkable progress*" in the scale and sophistication of surveillance technology and techniques 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).

154. The Court explained that it was necessary, in light of these technological developments, to ensure "*the simultaneous development of legal safeguards securing respect for citizens' Convention rights*" (§68). Otherwise, the Court concluded, "*it would defy the purpose of government efforts to keep terrorism at bay…if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives*." (§68).

155. The Court further noted that one of the reasons why it found no violation of Article 8 in *Kennedy* was because "*the impugned legislation did not allow for 'indiscriminate capturing of vast amounts of communications'*" (§69). While the Government submits that the judgment in *Kennedy* is "*a strong indicator that the same outcome should follow*" for the s 8(4) Regime (Observations, §4.16), *Kennedy* concerned the interception of the communications of a specific individual or premises under s 8(1) of RIPA. As the ISC has explained: "*An 8(4) warrant for bulk interception is quite different from the 8(1) warrants used for targeted interception. Whereas the 8(1) warrant system provides authorisation for deliberate and specific investigation into a named individual, usually in the UK, the 8(4) warrant system is designed for much broader intelligence-gathering purposes*".[94] The s8(4) Regime, is therefore different in terms of the nature and scale of interception.[95]

156. In *Szabó*, the Court stated that it was "*a matter of serious concern*" where "*broad-based*" legislation could potentially enable "*so-called strategic, large-scale interception*" (§69). The Court added, in this respect, 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*" and made specific reference to "*views expressed by the Court of Justice of the European Union and the European Parliament*" (§70). The Court stressed accordingly that "*[t]he guarantees required by the extant Convention case-law on interceptions need to be enhanced so as to address the issue of such surveillance practices*." (§70).

[94] ISC Report, para 95.

[95] Further, in *Kennedy*, the Court relied on the Government's assertion that the IPT is an effective remedy to demonstrate compliance with the "in accordance with law" requirement. But this case and subsequent disclosures have shown that the IPT is not an effective remedy (see paras 96-100, 280-285).

D. Absence of mandatory minimum safeguards

157. For these reasons, the six criteria laid down in *Weber* do not represent a mechanical set of rules for assessing whether the s8(4) bulk interception regime is in accordance with the law. But they do provide an important guide. The Applicants submit that merely meeting the *Weber* criteria is insufficient – especially in the light of the development of surveillance technology – to ensure there are sufficient safeguards for powers to be in accordance with the law. However, if bulk surveillance powers do not even meet the *Weber* criteria, they will certainly be inadequate to and will constitute a violation of Convention rights. For the reasons set out in the Additional Submissions (paras 44 to 60) and expanded upon below, the s8(4) Regime does not even satisfy the six *Weber* criteria.

158. Each of the *Weber* criteria are considered, in turn, below:

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

159. As explained in the Applicants' Additional Submissions at para 44(1), initial interception under a s8(4) warrant does not require any suspicion that a person has committed a criminal offence. Where the Government conducts s8(4) surveillance without contemplating that a particular offence has been, or may be, committed, it is unclear how the public can foresee "*the nature of the 'offences' which may give rise to an interception order*".

160. The Government relies exclusively on what it describes as "*a straightforward application*" of *Kennedy* and *R.E. v United Kingdom* (Observations, §4.40). But both *Kennedy* and *R.E.* were directed at the s8(1) Regime, which was designed for interception of specific targets the Government reasonably suspects of having committed or committing a particular offence.

2. The categories of people liable to have their communications intercepted

161. In *Szabó* the Court stated that this criterion requires "*the authorities to demonstrate the actual or premised relation between the persons or range of persons 'concerned' and the prevention of any…threat*" (§67).

162. The Government fails to draw any connection between the persons liable to have their communications initially intercepted under s8(4) and the "*prevention of any…threat*", because any person is liable to have their communications intercepted under s8(4).

163. Instead, the Government suggests that, at the initial interception stage, the focus of s8(4) on external communications provides a meaningful limitation (Observations, §4.42). However the Government then admits that the s8(4) Regime does not impose any limits on the "*types*" or "*numbers*" of external communications that can be initially intercepted and "*may in principle authorise the interception of internal communications insofar as that is necessary in order to intercept the external communications*." In practice, this means that the Government initially intercepts all communications (external and internal) that transit across the cables it intercepts.[96] Moreover, as discussed above, the Government's own definition of "*external*" captures many communications that seem "*internal*", including messages between two UK residents using a platform such as Facebook. The categories and numbers of people whose communications could be initially intercepted under a s8(4) warrant is therefore inadequately controlled by the law.

164. The Government's admission that a s8(4) warrant "*may in principle authorise the interception of internal communications*" stems from an

[96] For a further discussion on the difficulty in distinguishing between external and internal communications, see the Additional Submissions at para 45.

important feature of the UK interception regime under RIPA, including the s8(4) regime, that pursuant to section 5(6) of RIPA, a warrant permitting interception also permits the interception of content and related communications data "*if it is necessary to undertake in order to do what is expressly authorised by the warrant*".

165. In practice this has two significant implications:

(1) If the UK Intelligence Services conclude that, for technical reasons, even a limited and narrowly authorised interception warrant (much less a broad s8(4) warrant) requires bulk interception or extraction in the context of modern forms of communication, potentially vast amounts of communications may be initially intercepted in bulk, even if the warrant itself or any accompanying certificate had been narrowly drawn. The potential number of persons whose communications may be caught by this form of interception is virtually limitless.

(2) Communications data, in particular, can be obtained through the operation of s5(6), and extracted, stored, analysed and disseminated as if it was all the target of the original authorisation, warrant or certification. The Government may assert that it has voluntary, internal, secret, unpublished rules that result in the UK Intelligence Services limiting in unspecified ways the degree of use of it makes of content and communications data obtained in this way; or how long it retains such communications data. But secret, unpublished rules do not provide a clearly accessible legal framework to protect rights. There is no accessible legal framework to prevent vast amounts of communications data being collected and retained under s5(6) and no concomitant remedial measure to minimise the interference and subsequent examination of material obtained in this way. As a result, the initial rules as to who might

be the target of initial interception under RIPA and the terms of a warrant or its certificate have no practical effect. In reality, every person's communications could be collected in the execution of almost any warrant, if that collection can be justified under s5(6).

166. These implications also have significance insofar as data collected pursuant to s5(6) is extracted, filtered, stored, analysed and disseminated in relation to the other *Weber* criteria considered below.

167. The Government further contends that there are substantive limitations on the categories of people whose information can be selected for examination (Observations, §§4.43-4.48). It relies on the certificates that the Secretary of State issues to authorise selection of information intercepted under s8(4). But the Secretary of State has only ever issued a single certificate, which applies to all 18 of the s8(4) warrants in existence the time of the March 2015 ISC Report. The ISC Report described the single certificate as "*expressed in very general terms*", "*generic*", "*unnecessarily ambiguous*" and liable to "*be misinterpreted*".[97] It noted, for example, that "*the categories of information*" that it authorises GCHQ to examine include "*[m]aterial providing intelligence on terrorism*" and related to "*safeguarding economic well-being and the prevention and detection of serious crime"*.[98] In addition, it highlighted that the certificate also included the category of *"strategic environmental issues*", the true scope of which is very difficult to comprehend.[99]

168. In contrast, the regime in *Weber* was clearer and more focused. As discussed above, the G10 Act only permitted the interception of international wireless telephone communications, which comprised only 10% of the total volume of telecommunications. The legislation further narrowed that category down to persons taking part in such

[97] ISC Report, paras 101, 103.
[98] ISC Report, paras 101-102.
[99] ISC Report, paras 102-103.

communications "*via satellite connections or radio relay links*" (§97). That category was then limited to 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). Finally, the legislation prohibited the monitoring of "*the telephone connections of German nationals living abroad*" (§110).

169. The Government's response is that providing any narrower categories would compromise national security. This is an untenable argument because if accepted it would deprive the concept of foreseeability of all meaning since it would allow everyone's communications to be routinely analysed by every Council of Europe state they pass through to see if they are of interest.

3. Limits on the duration of interception

170. Under s9(6) of RIPA the maximum period of an interception warrant is six months (or three months where the warrant is based on preventing or detecting serious crime). The Secretary of State, however, may renew a warrant – without limitation – so long as she "*believes that the warrant continues to be necessary on grounds falling within section 5(3).*" (s9(2)). This Court criticised long-term rolling renewals of authorisations in *Gillan v UK* (2010) 50 EHRR 45 at [82] ("*the failure of the temporal and geographical restrictions provided by Parliament to act as any real check on the issuing of authorisations by the executive are demonstrated by the fact that an authorisation for the Metropolitan Police District has been continuously renewed in a "rolling programme" since the powers were first granted*"). As discussed above, unlike a s8(1) warrant, a s8(4) warrant requires no reasonable suspicion that the target has committed or is likely to commit a criminal offence or has engaged in acts constituting a specific threat to national security. Thus, the s8(4) Regime places no restriction on the possibility that a person's communications may be routinely initially

intercepted, again and again, for an indefinite period under successive s8(4) warrants. The s9(6) time limits are therefore effectively meaningless.

4. The procedure to be followed for examining, using and storing the data obtained

171. 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.

172. First, the "safeguards" under s16 of RIPA do not apply to communications data. Thus, as the Independent Reviewer has noted, "*communications data…may be selected and reviewed according to a factor which is referable to an individual who is known for the time being to be in the British Islands".*[100] The ISC Report also noted that the s16 "safeguards" do not apply to communications data and that, accordingly, "*UK-to-UK* [communications data] *will be in the pool of Communications Data that GCHQ collect, and may be returned as a result of searches against that pool.*"[101] The revelations regarding the GCHQ programmes KARMA POLICE, Black Hole and MUTANT BROTH provide troubling examples of how the Government makes use of such data to produce automated profiles (Factual Appendix, paras 4-9).

173. Secondly, the Government relies on the certificate issued by the Secretary of State as an additional constraint on the scope of filtering and analysis. But, as discussed above, the certificate is expressed in such broad terms as to provide no meaningful limitation.

174. Thirdly, while s16(2) of RIPA provides that intercepted material cannot be selected for examination "*otherwise than according to a factor*" which is "*referable to an individual who is known to be for the time being in the*

[100] A Question of Trust, para 6.76.
[101] ISC Report, paras 145-146.

British Islands" and also has as its purpose "*the identification of material contained in communications sent by or intended for him*", in practice, many selectors might still include the communications of such individuals. The Independent Reviewer suggested that "*simple selectors such as email addresses or telephone numbers*" might filter out UK-based individuals but noted that "*internal communication may be read…if they are selected by reference to another factor*".[102] In addition, s16(2) only applies where the inspection "*has as its purpose or one of its purposes the identification of material contained in communications sent by…or intended for*" a UK-based individual. This limitation does not restrict the UK Intelligence Services from filtering, storing and analysing material relating to a person known to be in the UK so long as they are for the purpose of identifying material intended for a friend, relative or other associate of that individual.

175. Fourthly, the s16(2) "safeguards" may be removed under s16(3). The Government contends that *"[t]he Secretary of State's power to modify a certificate under s. 16(3)…is in substance as tightly constrained as his power to issue a s. 8(1) warrant*" (Observations, §4.44). However, the ISC Report disagrees. The ISC found that the information provided by GCHQ to the Secretary of State "*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)*".[103] In addition, "*16(3) modifications may contain lists of individuals – i.e. they do not always relate to a specific individual in the same way as 8(1) warrants*".[104] The ISC concluded accordingly that "*the 16(3) modification system…does not provide the same rigour as that provided by an 8(1) warrant.*"[105]

[102] *A Question of Trust*, para 6.57(c).
[103] ISC Report, para 114.
[104] ISC Report, para 114.
[105] ISC Report, para Q.

176. Finally, there is no meaningful regulation or oversight of the use of selectors and search criteria to select particular intercepted material for inspection. With the exception of the limited restriction in s16(2), neither RIPA nor the Code provide any guidance as to what constitutes appropriate selectors and search criteria. Nor is there any requirement for search terms to be specified in the s 8(4) warrant or the certificate. This is in contrast to the position in *Weber* where the search terms had to be specifically identified in the monitoring order and were subject to review and approval by the G10 Commission.[106]

177. In light of the generic nature of the certificate, the ISC "*sought assurance* that "*the application of simple selectors and initial search criteria, and then complex searches which determine what communications are examined*" are "*subject to scrutiny and review by Ministers and/or the Commissioners.*" However, it found that, *"neither Ministers nor the Commissioners have any significant visibility of these issues.*" By way of example, it highlighted that "*neither were aware that the number of 'selection rules'…had doubled between March and November 2014.*"[107]

178. The absence of effective oversight or approval of the filtering, storage and analysis of intercepted material is reflected by the IPT's third judgment in June 2016, which found that communications of one of the Applicants – the South African Legal Resources Centre – had been initially intercepted, extracted, filtered and stored. The IPT specifically found that "*the procedure laid down by GCHQ's internal policies for selection of the communications for examination was in error not followed*".[108] Even if other NGOs and individuals had suffered the same detriment, they would not have any remedy, unless they had the good fortune of blindly bringing a claim before the IPT.

[106] See s3(2) of the G10 Act and *Weber*, §32.
[107] ISC Report, paras 123-125.
[108] Third IPT Judgment, para 15.

5. The precautions to be taken when communicating intercepted material to other parties

179. Under s15(2) RIPA, the Secretary of State is simply required to ensure that disclosure of s8(4) intercepted material "*is limited to the minimum that is necessary for the authorised purposes*." Those authorised purposes, which are enumerated in s15(4), are broadly drawn and do not limit the power to disseminate intercepted material to situations where there is a reasonable suspicion that an individual has committed or is likely to commit a criminal offence or is a threat to national security. Moreover, the s15(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*".[109]

180. 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).

181. The UK Supreme Court has recently observed that, "*it can readily be foreseen that the sharing and exchange of information between public authorities are likely to give rise to disproportionate interference with*

[109] A Question of Trust, para 7.66.

article 8 rights unless the information holder carries out a scrupulous and informed assessment of proportionality" (*The Christian Institute v The Lord Advocate* [2016] UKSC 51, para 88). As the Applicants explain in greater detail below, in the absence of any requirement for individualised reasonable suspicion, it is difficult to see how such a "*scrupulous and informed assessment of proportionality*" can be effectively undertaken.

6. The circumstances in which data obtained may or must be erased or the records destroyed

182. As explained at paragraph 44(6) of the Applicants' Additional Submissions, although intercepted material and data must be destroyed when it is no longer required for the purpose for which it was obtained under the s8(4) warrant, it is unclear what this means in practice.

183. The Government points to provisions in the Code of Practice that specify retention periods "*which should normally be no longer than 2 years*" (Observations, §4.54). Yet the lack of effective safeguards to ensure the prompt destruction of intercepted material is reflected in the judgment of the IPT in June 2015, which found that the email communications of Amnesty International had been intercepted and that, "*the time limit for retention permitted under the internal policies of GCHQ, the intercepting agency, was overlooked in regard to the product of that interception, such that it was retained for materially longer than permitted under those policies*".[110] No explanation has ever been provided as to how this error occurred, or how many other people have been affected (none of whom have been given a remedy). It is not clear whether this was or may have been a systemic problem. Even if other NGOs and individuals had suffered the same detriment, it is not clear how they would know of it or potentially benefit from a remedy unless they decided to blindly bring a claim to the IPT.

[110] The Third IPT Judgment, para 14

E. Further minimum safeguards

184. In addition to failing to satisfy the minimum requirements of the six criteria listed above, the Applicants submit that the s8(4) bulk interception regime lacks a number of other safeguards which are necessary for a communication surveillance regime to satisfy the in accordance with law requirement. In summary, those safeguards are:

(1) A requirement to establish a connection between a particular interception measure and reasonable suspicion that a particular individual has committed or is committing a criminal offence or is engaged in acts amounting to a specific threat to national security.

(2) A requirement for prior judicial independent authorisation of all interception warrants.

(3) A requirement to notify individuals whose communications have been subject to surveillance measures as soon as this can be done without jeopardising the purpose of the measure.

1. No requirement for individual reasonable suspicion

185. Under the s8(4) Regime communications may be initially intercepted, extracted, filtered, stored, analysed and disseminated without any requirement for individuals to be individually identified and targeted. There is also no requirement that there should be a reasonable suspicion that the sender or recipient of the communication has committed any offence.

186. The absence of any requirement for identification or of reasonable suspicion is incompatible with the requirements established in the Court's recent case law. In particular:

(1) 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). The Grand Chamber stated that, "*Russian courts do not verify whether there is a 'reasonable suspicion' against the person concerned*" (§263).

(2) 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).

187. If the hypothetical possibility of discovering a previously unknown threat is a sufficient basis to justify the existence of bulk intrusion, then that rationale effectively obviates any possibility of a meaningful case-by-case assessment of proportionality. The possibility of discovering a threat would automatically assume primacy over any other interests. Accordingly, a necessary safeguard for any interception regime must be the articulation of a reasonable suspicion against an individual in order to allow proportionality to be assessed.

2. No prior independent authorisation

188. Under RIPA there is no requirement for, or process enabling, the prior independent authorisation of s8(4) warrants. Instead, warrants are issued by a Government minister without reference to any judicial or other independent authority. This is incompatible with Article 8. The problem with the current regime was explained by the Independent Reviewer in his June 2015 report. He noted "*the Secretary of State is rarely if ever held politically accountable for the issue of warrants: contributing factors are RIPA s.19* [prohibiting disclosure of the fact a warrant has been issued or its content], *NCND* [the 'Neither Confirm Nor Deny' principle] *and the fact that intercepted material is not admissible in court* [with the effect that a judge will not review the lawfulness of the intercept operation]."[111] The Independent Reviewer noted that the UK Foreign Office argued that judicial authorisation might "*disadvantage the UK*" because judges would refuse applications that a government minister would sign.[112] He observed: "*Were it the case that Ministers might be tempted to issue warrants in circumstances where it is illegal to do so, that would seem to me a strong argument in favour of judicial authorisation rather than against it*"[113]

189. In *Zakharov* the Grand Chamber emphasised that the authorisation of a warrant to intercept telephone calls must be made by an authority that is independent from the Executive (§258).[114]

---

[111] A Question of Trust, para 14.56.
[112] A Question of Trust, para 14.57.
[113] A Question of Trust, para 14.57.
[114] The Court noted at §259 that: "*Russian law contains an important safeguard against arbitrary or indiscriminate secret surveillance. It dictates that any interception of telephone or other communications must be authorised by a court…The law-enforcement agency seeking authorisation for interception must submit a reasoned request to that effect to a judge, who may require the agency to produce supporting materials…The judgment must give reasons for the decision to authorise interceptions*".

190. The Court repeated these principles in *Szabó*. The Court explained that, "*in this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny*" (§77). In particular, "*supervision by a politically responsible member of the executive, such as the Minister of Justice, does not provide the necessary guarantees*" (§77). Independent, "*preferably judicial*," review "*reinforce[s] citizens' trust that guarantees of the rule of law are at work even in this sensitive field and by providing redress for any abuse sustained*" (§79).

191. In his concurring opinion in *Szabó*, Judge Pinto De Albuquerque commented that in view of "*the enlarged consensus in international law…and the gravity of the present-day dangers to citizens' privacy the rule of law and democracy, the time has come not to dispense with the fundamental guarantee of judicial authorisation and review in the field of covert surveillance gathering*" (§OI-23).

192. In addition:

(1) In *Digital Rights Ireland* the Grand Chamber of the CJEU concluded that the 2006 Data Retention Directive ("Directive 2006/24"), which required communications service providers to retain customer communications data in bulk for up to two years for the sake of preventing and detecting serious crime, breached the rights to privacy and data protection under Articles 7 and 8 respectively of the EU Charter of Fundamental Rights.[115] The

[115] The Government argues that *Digital Rights Ireland* is irrelevant to this case because "*the CJEU was…not concerned with a national regime or any provision governing access to, or use of, retained data by national law enforcement authorities"* (Observations, §4.20). The Government is wrong. In *Tele2 Sverige AB* and *Tom Watson & Others* (C-698/15) the Advocate General stressed that, *"the criteria identified by the Court in Digital Rights Ireland are relevant in the assessment of the national regimes at issue in the present cases*" (para 191). Indeed, he observed that "all *the safeguards described by the Court in paragraphs 60 to 68 of Digital Rights Ireland must be regarded as mandatory*" (para 222). Accordingly, it is appropriate to consider those mandatory requirements when assessing bulk interception regimes, such as the s8(4) Regime. Moreover, the Applicants note that this Court expressly referred to the *Digital Rights Ireland* judgment in

CJEU noted that Directive 2006/24 did not contain sufficient substantive and procedural safeguards governing the access and use of retained data. In particular, it highlighted that "*the access by the competent national authorities is not made dependent on a prior review carried out by a court or by an independent administrative body*" (§62).

(2) In *Watson & Others* the Advocate General stated: "*I see no reason to take a flexible attitude to this requirement for prior review by an independent body, which indisputably emerges from the language used by the Court in paragraph 62 of Digital Rights Ireland"* (para 234). Because *"[c]ompetent law enforcement authorities have every interest in requesting the broadest possible access,*" the Advocate General reasoned that "*the intervention of an independent body prior to the consultation of retained data, with a view to protecting persons whose data are retained from abusive access by the competent authorities, is to my mind imperative*" (para 236).

(3) The 2013 report by the United Nations Special Rapporteur on the promotion and protection of the right to freedom of expression stated that: "*Legislation must stipulate that State surveillance of communications must only occur under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority*."[116]

(4) A system of prior judicial authorisation would minimise unnecessary or disproportionate interferences with privacy. As the CoE HR Commissioner has noted, "*there is an obvious advantage of requiring prior judicial authorisation for special investigative techniques, namely that the security agency has to go "outside of*

Szabó (§23) and *Zakharov* (§147), indicating that it is not, as the Government asserts, a radical departure from this Court's case law on Article 8.

[116] Cited and quoted in *Szabó*, para 24.

> *itself" and convince an independent person of the need for a particular measure. It subordinates security concerns to the law, and as such it serves to institutionalize respect for the law. If it works properly, judicial authorisation will have a preventive effect, deterring unmeritorious applications and/or cutting down the duration of a special investigative measure.*"[117]

193. The Applicants submit that the absence of <u>any</u> requirement for prior judicial authorisation means the s8(4) Regime is not in accordance with the law. It is notable that under the Investigatory Powers Bill currently before Parliament, some form of prior judicial review of warrants issued by a Government minister will be introduced for all interception warrants.[118]

3. No requirement for subsequent notification of interception measures

194. In *Szabó* the Court observed that:

> [T]he Court has held that the question of subsequent notification of surveillance measures is 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).

195. The Advocate General in *Watson & Others* explained why recourse is near impossible without notification:

> [F]rom a practical point of view, none of the three parties concerned by a request for access is in a position to carry out an effective review in connection with access to the retained data. Competent law enforcement authorities have every interest in requesting the broadest possible access. Service providers, who will be ignorant of the content of any investigation file, are incapable of checking that

[117] *Memorandum on Surveillance*, para 28 (referring to the Venice Commission's Report on Democratic Oversight (2007))
[118] Investigatory Powers Bill, HL Bill 62, clauses 23, 132.

> requests for access are limited to what is strictly necessary and persons whose data are consulted have no way of knowing that they are under investigation, even if their data is used abusively or unlawfully… (para 236)

196. Accordingly, "*[a]s soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should be provided to the persons concerned*" (*Szabó*, §86). Under Hungarian law no notification of any kind was envisaged. This factor, coupled with the absence of formal remedies in cases of abuse, meant that, "*the legislation falls short of securing adequate safeguards*" (§86).

197. The Court's approach in *Szabó* reflects the recommendations contained in the 2013 Report of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, which stated:

> Individuals should have a legal right to be notified that they have been subjected to communications surveillance or that their communications data has been accessed by the State. Recognizing that advance or concurrent notification might jeopardize the effectiveness of the surveillance, individuals should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath.[119]

198. The CoE HR Commissioner has also expressly supported "*a system of notification when a person has been the subject of surveillance*".[120]

199. Notification becomes especially important in the context of the s8(4) Regime both because it lacks prior independent authorisation and the IPT has limited access to redress through its recent rulings. Nor does the IOCC provide an effective remedy. He has no power to refer a case to the IPT for a remedy. Nor is he permitted to notify the victim of any excessive

[119] Cited and quoted in *Szabó*, §24.
[120] *Memorandum on Surveillance*, para 25.

or unlawful interception. This position was described by the Independent Reviewer in his report as "*hard to understand*" and he recommended the introduction of a system of notification.[121]

200. The IOCC has been strongly critical of these unnecessary limitations on his oversight. He has repeatedly asked for (but does not have) power to refer errors to the IPT so that victims of errors can obtain a remedy, and for power to disclose errors to victims. Without such powers, the oversight provided by the Commissioner is more theoretical than real. The Commissioner has publicly complained about the following: "[122]

> **4 Relaxation on secrecy provisions to aid transparency.** We are constrained by the current statutory provisions in section 19 of RIPA forbidding disclosure, as are the public authorities and the CSPs. The culture of secrecy must continue to be challenged and transparency should be encouraged where it leads to greater accountability without prejudicing national security or the ongoing prevention or detection of crime.
>
> **5 Full provision for reporting errors / breaches and power to refer matters to the IPT.** It is crucial to ensure that the error reporting provisions are clear and comprehensible and that individuals adversely affected are able to seek effective remedy. On the latter point a number of areas would benefit from review here including; the threshold of "wilful or reckless" and whether the Commissioner should be able to refer matters directly to the IPT.

F. The bulk interception regime is unnecessary and disproportionate

1. The test: "strict necessity"

201. In *Szabó* the Court held that in the context of covert interception of electronic communications the requirement of necessity under Article 8(2) imposes a test of strict necessity "*in two aspects*." First, a secret surveillance measure must be "*strictly necessary, as a general*

[121] A Question of Trust, para 14.104.
[122] IOCCO, *Update on Investigatory Powers Bill*, August 2016. Reply Annex No. 33.

consideration, for the safeguarding the democratic institutions". Second, it must be "*strictly necessary, as a particular consideration, for the obtaining of vital intelligence in an individual operation*." The Court explained that "*any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal*." (§73).

202. In considering whether the test of strict necessity is satisfied, the existence of safeguards is a necessary, but not sufficient, condition.

203. As the Advocate General explained in *Watson & Others*:

> "[T]he mandatory safeguards described by the Court in paragraphs 60 to 68 of Digital Rights Ireland are no more than minimum safeguards … a national regime which includes all of those safeguards may nevertheless be considered disproportionate, within a democratic society, as a result of a lack of proportion between the serious risks engendered by such an obligation, in a democratic society, and the advantages it offers in the fight against serious crime." (para 262).

204. The utility of a particular surveillance measure is likewise a relevant, but not conclusive, consideration. As the Independent Reviewer observed in his 2015 report, even if bulk interception makes a "*valuable*" contribution to protecting national security, "*[i]t does not of course follow that it is necessarily proportionate*".[123] Indeed, the Independent Reviewer in his 2016 report on bulk powers explicitly noted that he was not "*asked to opine on…whether the safeguards contained in the [Investigatory Powers] Bill are sufficient to render them proportionate for the purposes of the European Convention on Human Rights*".[124]

[123] *A Question of Trust*, para 7.26
[124] Report of the Bulk Powers Review, para 1.11(b). Reply Annex No. 32.

2. s8(4) is not strictly necessary for the safeguarding of democratic institutions

205. On 12 March 2014 the European Parliament issued a "Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs". The resolution observed that the Snowden revelations have "caused numerous concerns within the EU", including, inter alia:

> - the possibility of these mass surveillance operations being used for reasons other than national security and the fight against terrorism in the strict sense, for example economic and industrial espionage or profiling on political grounds;
>
> - the undermining of press freedom and of communications of members of professions with a confidentiality privilege, including lawyers and doctors; [and]
>
> …
>
> - the increasingly blurred boundaries between law enforcement and intelligence activities, leading to every citizen being treated as a suspect and being subject to surveillance.[125]

206. The European Parliament's "*Main Findings*" included the "*[c]onsider[ation] that data collection of such magnitude leaves considerable doubts as to whether these actions are guided only by the fight against terrorism, since it involves the collection of all possible data of all citizens*" and "*points, therefore, to the possible existence of other purposes including political and economic espionage, which need to be comprehensively dispelled*".[126]

---

[125] European Parliament, Resolution on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs, 12 Mar. 2014, para F ("EU Parliament Resolution").

[126] EU Parliament Resolution, para 7.

207. The Court has recognised on numerous occasions that bulk data holdings may not be justified. In *S and Marper v UK* (2009) 48 EHRR 50 the Grand Chamber held that the collection and retention of DNA and fingerprints of innocent people was contrary to Article 8. In particular, the Grand Chamber was "*struck by the blanket and indiscriminate nature of the power of retention in England and Wales*", noting that "*[t]he material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; fingerprints and samples may be taken—and retained—from a person of any age, arrested in connection with a recordable offence, which includes minor or non-imprisonable offences*" (§119). It further noted that retention was "not *time limited; the material is retained indefinitely whatever the nature or seriousness of the offence of which the person was suspected*" and a lack of safeguards to ensure that material was deleted "*according to defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances*" (§119).

208. The Grand Chamber concluded that "*the blanket and indiscriminate nature of the powers of retention…fails to strike a fair balance between the competing public and private interests*" (§125). It held that the UK had "*overstepped any acceptable margin of appreciation in this regard*" even though the DNA database was undoubtedly a valuable tool for detecting and prosecuting serious criminals (§125).

209. Similarly, in *MK v France*, App No. 19522/09, 18 April 2013, the Court held that the French national digital fingerprint database was unlawful. In doing so, it rejected the arguments of the French 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). The Court also noted that the need for safeguards *"is all the greater where the protection of personal data undergoing automatic*

processing is concerned, not least when such data are used for police purposes" (§32). 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*".

210. As in *Marper* and *MK*, the Government claims the power to intercept in bulk information relating to the lives of millions of individuals without any individual reasonable suspicion that they have committed or are committing a criminal offence or are engaged in an act amounting to a specific threat to national security. This interception is "*blanket and indiscriminate*" and is no less intrusive because it "*undergo[es] automatic processing*" (in fact, the opposite is true – the availability of sophisticated search and processing tools makes holding a large quantity of data more intrusive because it can be rapidly analysed).

211. Further, as to the individual necessity of bulk interception, one unique feature of the UK interception regime is worth noting. Under s17 of RIPA, evidence obtained by interception is not admissible in criminal proceedings. It is difficult to understand how evidence that will never be put before a judge can be construed as strictly necessary for solving serious crime.

3. Conclusion on necessity and proportionality of the bulk interception regime

212. One of the Government's primary rationales for justifying bulk interception is that it is "*critical both for the discovery of threats and for the discovery of targets who may be responsible for threats*" (Observations, §1.29(1)). The Government thus admits that bulk interception is not aimed at obtaining vital intelligence in any individual operation. Rather, it is effectively a speculative fishing expedition, designed to check the behaviour of an entire population. Such programmes are inherently

susceptible to abuse and would inevitably lead to the acceptance of a total surveillance approach.

213. The Government's other rationale for justifying bulk interception is that even where the UK Intelligence Services "*know the identity of targets, their ability to understand what communications bearers those targets will use is limited, and their ability to access those bearers is not guaranteed*", making it "*necessary…to intercept a selection of bearers, and…scan the contents of all those bearers for the wanted communications*" (Observations, §1.29(2)). In other words, the Government relies on the unpredictability of internet communications, namely the fact that such communications are broken into packets, which may be transmitted via different routes, to justify bulk interception.[127] The Applicants acknowledge that to initially intercept the communications of a particular legitimate target (approved by an independent authority on the basis of reasonable suspicion), it may be necessary in some circumstances to initially intercept (as the Applicant's define that term) a communications bearer. But the Government should then immediately discard the unwanted communications, rather than storing and analysing collateral data. This technical limitation should not be used to justify the fishing expedition the Government seeks to engage in under its primary rationale.

214. The Applicants submit that the Government's bulk interception regime is not necessary and proportionate:

(1) The scale of the bulk interception regime is unprecedented in terms of (a) the number of individuals whose communications are potentially affected; (b) the quantity of communications content and

[127] The Government also claims that "*[t]he s8(4) Regime was designed with the internet in mind, and on the basis that some form of s. 8(4) Regime was required*." (Observations §4.2(1)). This assertion is another iteration of the technical rationale for bulk interception. The Applicants note that, whether or not that assertion is true, s8(4) makes no reference to the internet and it is clear that developments in communications and surveillance technology have exceeded what could possibly have been envisaged when RIPA was enacted sixteen years ago.

related communications data that is actually initially intercepted, extracted, filtered, stored, analysed and/or disseminated by the UK intelligence agencies.

(2) The s8(4) Regime falls far short of complying with the minimum procedural safeguards listed above. The operation of sophisticated covert surveillance powers without adequate safeguards is *ipso facto* disproportionate.

(3) In particular, there is no requirement of individual reasonable suspicion. The twin justifications advanced for the existence of the regime – technical necessity and the ability to discover previously unknown threats – would, if accepted, render a case-by-case assessment of the treatment of particular intercepted material impossible and meaningless. On the Government's case, the ends sought would automatically justify the means in every case. This is the antithesis of what a proper application of Article 8 entails.

4. Response to the IPT's handling of questions of proportionality in its Third Judgment

215. The IPT did not adequately address issues of proportionality:

a. No proper consideration of the general proportionality of the s8(4) regime

216. The IPT's Third Judgment asserted that the submissions it had received "*enabled it to take into account questions relating to both generic (or 'systemic') questions and those relating to the individual claimant and its communications*".[128] However, save for that bald assertion, the remainder of the judgment did not contain any discussion or examination of the proportionality of the bulk interception regime.

[128] IPT Third Judgment, para 3.

217. As a result, the Applicants have been left entirely in the dark about the basis for the IPT's conclusion that the bulk interception regime is necessary and proportionate. This is an unsatisfactory outcome and illustrative of the systemic deficiencies in the IPT's oversight.

b. Deliberate targeting of human rights organisations

218. The Government submits that no inference that human rights NGOs are deliberately targeted "*can possibly be drawn from the IPT's conclusions*" in relation to the unlawful handling/retention of Amnesty International and the Legal Resources Centre's email communications (Observations, §4.103). In view of the terse nature of the IPT's third judgment, the Applicants are unable to know in what circumstances their communications were intercepted. Nevertheless, the communications of legitimate and well-respected human rights organisations have been initially intercepted, extracted, stored and analysed.

219. There is no evidence that these interceptions were necessary or proportionate. The Government has not sought to explain – even in barest terms – why providing any further information would have jeopardised national security or harmed the public interest. It is unclear, for example, how either the public interest or national security could be imperilled by revealing the statutory purpose(s) for which the initial interception, access and/or selection of these communications were based.

220. The IPT has also failed to explain what practical steps it had taken to satisfy itself that the relevant initial interception, access and/or selection of communications was lawful and proportionate. It simply limited itself to the bald statement that Amnesty International's communications had been "*lawfully and proportionately intercepted and accessed*" and that the interception of the Legal Resources Centre's communications "*was lawful*

and proportionate and that the selection for examination was proportionate".[129]

II. INTELLIGENCE SHARING BREACHES THE CONVENTION

221. The UK Intelligence Services can access information in several ways. They can initially intercept the data itself, for example, while it transits over a wire, a fibre optic cable or a wireless link. Under UK law, interception also includes "collect[ing] or otherwise…hav[ing] access to" data stored by "the system by means of which the [information] is being, or has been, transmitted" (see section 2(7) of RIPA 2000).

222. Intercepted material can also be obtained under intelligence sharing arrangements with foreign intelligence agencies. For example, a foreign agency may operate its own bulk interception programme. The safeguards and oversight of such programmes may be inadequate. Nevertheless, the data initially intercepted may be shared with or made available, including in bulk, to the UK Intelligence Services. Such access is as intrusive to privacy as if a UK agency had initially intercepted the information itself and the means by which the interference with privacy is carried out is irrelevant. Conduct that is as intrusive as interception ought to be accompanied by safeguards and oversight that are at least as strong. Otherwise, states may be tempted to adopt means of surveillance that provide fewer safeguards, but remain highly intrusive. The rights granted in Articles 8 and 10 must be practical and effective, not theoretical and illusory.

223. The UK regime governing the circumstances in which the UK Intelligence Services can access, extract, filter, store, analyse and/or disseminate material which has been initially intercepted by a foreign intelligence

[129] IPT Third Judgment, paras 14-15.

agency does not meet the "*in accordance with the law*" requirement of Article 8. That suffices to dispose of the claim.

224. In addition, the regime continues to fail to meet the "*in accordance with law*" requirements despite the amendments to the Interception of Communications Code of Practice made on 27 January 2016.

225. The Applicants' argument is developed under the following headings:

(1) Factual premises

(2) Minimum safeguards are required where the Government accesses information intercepted by a foreign intelligence agency

(3) The UK legal regime on intelligence sharing lacks the required minimum safeguards.

A. Factual premises

226. The nature of modern communication means that many private communications (and their communications data) between individuals, even where both reside in the same country, can now be intercepted by foreign intelligence services in a way that could never have happened in the past. The technical architecture of the internet directs data to travel over the least congested, cheapest or most reliable route, not the shortest. Communications between two people in the UK may be transmitted via other countries, making them available to multiple intelligence services along the route. Communications are also transmitted via servers which may be far away from the people communicating. An email between two people in London may be transmitted via a server in the US. Communications, which in the past would have remained entirely within the UK, can, therefore, be intercepted across the globe.

227. The US, as described by the NSA itself, is "*the principal hub in the world's telecommunication system*".[130] Much of the world's communications and communications data transit fibre optic cables landing in or traversing the US or via servers located within the US. Thus if A (located in London) sends an email or text to B (also located in London), it may very well pass through cables, or be stored on servers, which the NSA can, at least in principle, access.

228. There are a range of different ways in which the NSA could obtain that communication between A and B or the data associated with it, and then provide the UK Intelligence Services with access to it. For instance, the US could engage in "*bulk*" initial interception of vast quantities of communications or communications data as they transit the internet without limiting what is obtained to specific individuals or specific communications. It could then provide GCHQ with access to the raw initially intercepted material. GCHQ could then extract communications or communications data from that material, filter those that are of interest and store, analyse and disseminate them.

229. The Government suggests (see, in particular, Observations, §§ 1.1-1.20) that the Court should assume that the USA only engages in targeted interception and does not give access to raw material, initially intercepted in bulk by the NSA, to the UK Intelligence Services. If that is the Respondent's submission, it should be rejected. That is, in the first place, because of clear and credible evidence (see paras 69-71 above and Factual Appendix, paras 10-19) that the US intelligence agencies engage in bulk interception and that the UK has access to this material. The US Government has itself publicly acknowledged the veracity of certain of this evidence. Moreover, the Government has never denied the contents or authenticity of this evidence.

[130] Farr Witness Statement,

230. That evidence suggests the following:

(1) An email or text sent by A to B, when both are located in London, could be intercepted by the NSA either because it is one of a mass of emails or texts intercepted as part of a bulk programme or as part of some more targeted exercise.

(2) The UK Intelligence Services could then obtain that email or text (or its associated communications data) because:

i. The NSA gives the UK Intelligence Services access, in bulk, to raw initially intercepted material and the UK Intelligence Services themselves extract, filter, store, analyse and/or disseminate emails/texts that are of interest to them;
ii. The NSA provides the email/text, unsolicited, to the UK Intelligence Services;
iii. The UK Intelligence Services ask the NSA to initially intercept or otherwise obtain the email/text and provide it to the UK Intelligence Services.

231. The Court should determine whether, if material is accessed or obtained in any of the ways described above, the safeguards in place are sufficient to meet the Article 8 in accordance with law requirement.

B. Minimum safeguards are required where the Government accesses information intercepted by a foreign intelligence agency

232. In paragraphs 157-183 above, the Applicants lay out the minimum safeguards this Court has indicated should apply to communications interception. The Government's position is that these safeguards developed in relation to intercept material have no application where the initial act of initial interception was conducted by a foreign state but

which allows the UK Intelligence Services to extract, filter, store, analyse and/or disseminate the intercepted material (Observations, §3.29).

233. In support of its position, the Government relies upon *Uzun v Germany* (2011) 53 EHRR 24 (Observations, §3.32). In *Uzun*, a suspect complained about the covert installation of a GPS device on his car and argued that the *"minimum safeguards*" from the Court's interception jurisprudence should be applied. The Court rejected the argument. It held that the "*rather strict standards, set up and applied in the specific context of surveillance of telecommunications…are not applicable as such to cases such as the present one, concerning surveillance via GPS of movements in public places and thus a measure which must be considered to interfere less with the private life of the person concerned than the interception of his or her telephone conversations*." (§65).

234. The Government's position, based on *Uzun*, is that where communications are intercepted by a foreign intelligence agency, and the UK is granted access to those communications, the "*rather strict standards*" the Court has developed for interception of communications should not apply. In doing so, the Government suggests that intelligence sharing that leads to access to intercepted communications is more akin to cases where movements in public places are obtained from a GPS location of a car than to this Court's jurisprudence on the interception of communications (Observations, §3.34).

235. That argument should be rejected. Just because an additional party is involved in the interception of the communication does not lessen the interference with privacy. Fundamentally, whether communications and communications data are initially intercepted by the US and shared with the UK or initially intercepted by the UK directly, the result is the same – the UK obtains access to highly intrusive private information. Such an intrusion is not at all analogous to obtaining public movements via GPS

tracking of a vehicle on the public roads. The UK's case places form over substance and is inconsistent with the principle underpinning the Convention, that it "*guarantees rights that are practical and effective and not theoretical and illusory*".[131]

236. A similar argument made by the UK was rejected by the Court in *R.E v UK*. There, the Court 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, the *Weber* standards set out minimum requirements, to be enhanced as necessary in light of *Szabo* and the development of modern mass surveillance practices.

237. The starting point is that intercepting communications is regarded as a particularly serious interference with privacy. The Court held as far back as *Malone v UK* (1985) 7 EHRR 14 that interception of communication is a "*secret and potentially dangerous interference with the right to respect for private life and correspondence*" (§67) and that therefore particular safeguards are required for such activity. Interception of communications is thus treated differently to other forms of state surveillance in terms of the interference with privacy which it entails.

238. If the State is to be permitted to intercept communications the Court has required particularly strict attendant safeguards. When one considers how much more of individuals' private lives can now be revealed through examining their intercepted communications and communications data (whether in the form of emails, text-messages, internet searches or location of mobile phones) than was the case at the time of *Malone*, or indeed when RIPA was enacted, the dangers for privacy of such

[131] See among many other authorities, *Airey v Ireland (*1979–80) 2 EHRR 305, §24; *Imbrioscia* (1994) 17 EHRR 441, §38; *Goddi v Italy* (1984) 6 EHRR 457, §30; and *Salduz* (2009) 49 EHRR 19, §55.

interception, and the requirement for robust safeguards, are all the more pressing.

239. How, then, should the Court approach access to intercepted communications when the interception itself was undertaken by another state? One element of the Government's argument can be dealt with easily. The Government argues that it is not possible to have a legal regime that governs intercept material obtained from a foreign state, as distinct from other intelligence that is then shared with the UK Intelligence Services (see Observations, § 3.34). It relies on the evidence of Mr Farr who asserts that no *"workable distinction"* can be drawn between material intercepted by another state, and, for example, material "*derived from covert property searches*" carried out by a foreign intelligence service and shared with the UK (Farr witness statement para 29).[132]

240. That submission is impossible to reconcile with the Government's own policies. In its recently revised Code of Practice, specific provision is made for "*Rules for requesting and handling unanalysed intercepted communications from a foreign government*".[133] It is clear that the Government itself considers it possible to formulate "*Rules*" that apply specifically to obtaining "*intercepted communications*" from a foreign government and has no difficulty distinguishing such material from other material the UK Intelligence Services receive. Whether or not that Code is sufficient to meet the in accordance with law requirement of Articles 8 and 10 is disputed by the parties, but it is clear that the Respondent can and does formulate rules which apply specifically to intercepted material.

241. Turning to the jurisprudence on interception, the Court has yet to consider how communications and communications data initially intercepted by a State and then shared with a signatory State to the Convention, should be

[132] Farr Witness Statement, para 29.
[133] Jan. 2016 Code of Practice, Ch. 12.

treated by the Convention. It is, therefore, necessary to consider the issue as a matter of principle. Is the Respondent correct that the *"rather strict standards*" of the Court's interception jurisprudence have no application if material is initially intercepted by foreign intelligence services and then access to it shared in some form? Or are the Applicants correct that the standards applicable to interception are similarly required when access is given to intercepted material even if the actual initial interception was carried out by a foreign intelligence service?

242. The difference between the parties' positions can be illustrated by considering how they apply to a number of scenarios:

(1) Scenario 1 The UK Intelligence Services initially intercept a text between A and B, who are both located in London, as the communication is leaving the UK on transatlantic fibre optic cables;

(2) Scenario 2 The NSA taps a transatlantic fibre optic cable arriving in the USA. The UK Intelligence Services are given access to the raw intercept material, allowing them to extract, filter, store, analyse and/or disseminate communications (or communications data) – including the same text between A and B – traveling along this fibre optic cable.

(3) Scenario 3 The NSA initially intercepts the same text between A and B, who are both located in London, through one of its multiple bulk interception programmes. The NSA, of its own volition or at the request of the UK Intelligence Services, then provides the latter access to the text.

243. The Applicants' position is that the UK Intelligence Services' access to the text between A and B (or of emails, calls or other communications in similar circumstances) should, for the purposes of the in accordance with

law requirement, be treated in the same, or approximately the same way under scenarios (1)-(3). In each scenario, the same communication is being initially intercepted using similar techniques in the course of transmission. Whether the UK Intelligence Services have full or partial control over the means of initial interception is irrelevant to the question of the legal regime that should apply. The "*quality of the law*", in terms of its foreseeability and the level of protection it provides against arbitrary interference, must be of a similar nature.

244. That is because all of the scenarios concern the legal provision necessary to protect the same right to privacy, *i.e.* A and B's right when they communicate with one another in the UK not to have the UK Intelligence Services access, extract, filter store, analyse or disseminate those communications. The fact that the route by which the communications reached the UK was via US initial interception (where the US authorities may have done nothing more than tap a communication stream and where the UK authorities extracted, filtered, analysed and/or stored the relevant material) does not change the extent of the interference with A and B's privacy or the necessity of putting in place protections against such interference occurring arbitrarily, disproportionately or unlawfully.

245. The Respondent's position is that scenario (1) should be approached quite differently from scenarios (2)-(3) in terms of required minimum safeguards. That cannot be correct. Where A and B communicate in London, it is impossible to see why the safeguards that protect their privacy from interference by the UK Government should be substantially different between the scenarios. In each scenario, the UK Government is able to access, store, analyse, collate with other information, disseminate and use private communications (and communications data). The interference with privacy, and the dangers that entails if not subject to sufficient safeguards, is essentially the same whoever conducted the initial interception.

C. The UK legal regime on intelligence sharing lacks the required minimum safeguards

246. The IPT has already held that the intelligence sharing regime was not sufficiently foreseeable, prior to December 2015, because aspects of the regime had not been made public. The arrangements were not therefore in accordance with the law.

247. In addition, the regime was also not in accordance with law in substance. First, it has all the defects of the s8(4) Regime identified above. There is no provision for prior independent authorisation or any requirement for individual reasonable suspicion. The oversight arrangements are inadequate. Second, the regime is governed by a bare statutory power, drafted in general terms and exercised in secret. The present arrangements are *a fortiori Liberty* and therefore inadequate. As in *Liberty* there was no Code of Practice. But in *Liberty* the powers for bulk interception in IOCA 1985 were set out in publicly accessible legislation in some detail. In contrast, until recently nothing was in the public domain about intelligence sharing

248. The "note" setting out current practice is insufficient.[134] It was only disclosed as a result of this litigation. It is not law. It is unclear whether it 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 the closed hearing. 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. Further:

[134] Reply Annex no. 42; *see also* First Judgment, para 47.

(1) The note operates on the basis of applying RIPA by analogy. The receipt of intercepted material ought to be governed by legislation that is binding, not by a voluntary and discretionary practice of applying other legislation by analogy and in secret.

(2) The note 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 UK Intelligence Services 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.

(3) In addition, the concepts of "analysed" and "unanalysed" are not defined or explained, and do not derive from statute.

(4) The arrangements appear to provide no protection at all for communications data.

249. 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.

250. Yet the revised Code is equally inadequate because it applies the RIPA regime to intercepted data received from abroad. Those safeguards are inadequate for the reasons set out above (see 157-183).

III VICTIM STATUS

251. The first question posed by the Court is as follows:

Can the Applicants claim to be "victims", within the meaning of Article 34 of the Convention, of violations of their rights under Articles 8 and 10?

252. The Government contends the Applicants are not "victims" according to the two-stage test in *Zakharov*. Under that test, first "*the Court will take into account the scope of the legislation…by examining whether the applicant can possibly be affected by it*." Secondly, "*the Court will take into account the availability of remedies at the national level and will adjust the degree of scrutiny depending on the effectiveness of such remedies*" (§170).

A. Scope of the legislation

253. In considering the scope of legislation permitting secret surveillance measures, the Court has explained it will consider whether "*the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted*." (§171).

254. By the Government's own admission, the s8(4) Regime "*intercepts communications in 'bulk' – that is, at the level of communications cables – pursuant to the lawful authority of warrants under s.8(4) RIPA*" (Observations, §1.21). Thus, s8(4) of RIPA "*directly affects all users of communications services by instituting a system where any person can have his or her communications intercepted*". The Government does not attempt to claim that the Applicants might not have had their communications

initially *intercepted* by the UK Government. This admission alone is sufficient to satisfy the "scope of the legislation" requirement with respect to the s8(4) claim.

255. The Government then suggests that there is no relevant interference unless the data is selected or examined (Observations, §4.1). There is no support in this Court's case law for this distinction. Even if this distinction was tenable, the IPT concluded the UK Intelligence Services *selected for examination* the communications of one of the Applicants, the South African Legal Resources Centre.[135] That one of the Applicants' communications were selected for examination leads to a reasonable inference that the other Applicants, who engage in similar work and communicate with similar individuals and groups around the world, may be "at realistic risk of selection/examination" (Observations, §4.1).

256. In relation to the intelligence sharing claim, as discussed above, the US Government captures communications in bulk, then shares at least some of those communications with the UK Government. Under Executive Order 12333 – a regime the UK Government does not all address in its Observations – the US Government operates a range of programmes around the world, which collect communications and communications data in bulk. These programmes include those which intercept 194 million text messages per day (DISHFIRE), nearly 5 billion records relating to mobile phone locations (CO-TRAVELLER) and data directly as it transits to and from Google and Yahoo's private data centres (MUSCULAR). Under section 702 of FISA, the US Government operates PRISM and Upstream, the latter of which, like the s8(4) Regime, initially intercepts data in bulk as it transits over fibre optic cables. Evidence suggests that the UK Intelligence Agencies have access to material initially intercepted in bulk

[135] The IPT also found that the UK Intelligence Services "accessed" the communications of Amnesty International. It does not clarify what distinction, if any, exists between "accessed" and "selected for examination" but the Applicants note that the Government itself considers both Applicants to have had their communications selected and examined (Observations, §4.1).

by the US Government (DISHFIRE, XKEYSCORE and MARINA). The breadth of these programmes indicate that "*all users of communications services*", including the Applicants, could have their communications intercepted by the US Government and shared with the UK Intelligence Services.

257. The Government relies on the "note" relating to the intelligence sharing arrangements, as evidence supposedly cabining the UK Intelligence Services' access to information intercepted by the US Government (Observations §3.5(2)). But the note itself is of questionable authority, as is described in paragraph 93 above.

258. In any event, the text of the note is so broad as to reasonably permit the sharing of the Applicants' communications. 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." While the "request" is purportedly limited to that which could be authorised by RIPA (except in special circumstances), since RIPA permits bulk interception under s8(4) this is not a substantive limitation. "Receipt" is not defined at all. It is possible, therefore, that "request" or "receipt" could cover all the scenarios posited above in paragraphs 33-34 where the UK Intelligence Services may access material intercepted by foreign intelligence agencies, from raw, unanalysed intercept material to fully analysed reports.

B. Availability and effectiveness of remedies

259. The Court has held that "*if the national system provides for effective remedies…the individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret*

measures only if he is able to show that, due to his personal situation, he is potentially at risk of being subjected to such measures." (*Zakharov*, §171).

260. The IPT does not "*provide…effective remedies*". As discussed above, significant factual developments alter this Court's description of the IPT in *Kennedy*. In particular, the IPT does not offer "*extensive jurisdiction…to examine any complaint of unlawful interception*" (*Kennedy*, §167). Moreover, the effectiveness of the IPT as an oversight body is undermined by its briefing with MI5 in 2007 and its acquiescence not to receive categories of stored information when a complaint was made. The Applicants discuss the failures of the IPT in this case in its section addressing Article 6(1).

261. Finally, the Applicants note that the Government never disputed before the IPT that the Applicants were "victims" in relation to the s8(4) and intelligence sharing claims. The Government should not now be permitted to change the stance which it took before the domestic courts and must be regarded as having conceded and accepted that the Applicants are, indeed, victims.

IV VIOLATION OF ARTICLE 14, TAKEN TOGETHER WITH ARTICLES 8 AND/OR 10

262. The s8(4) Regime is indirectly discriminatory on grounds of national origin because of the additional safeguards granted to those known to be in the British Islands but denied to those abroad under s16 RIPA. It is not disputed that the facts in issue fall within the ambit of Articles 8 and 10.

263. The Government contends that there is no violation of Article 14 for two reasons. First, the Government asserts that there is no relevant difference in treatment. Second, it submits that any difference in treatment is justified. These will be considered in turn.

A. Relevant difference in treatment

264. The Court's case-law has established that "*discrimination means treating differently, without an objective and reasonable justification, persons in relevantly similar situations*." (*D.H. and Others v Czech Republic*, §175). The Court has further "*accepted that 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*." (§175)

265. The Government accepts that, under the s8(4) Regime, "*at the selection stage, limitations are imposed on the extent to which intercepted material can be selected to be read, looked at or listened to according to a factor which is referable to an individual who is known to be for the time being in the British Islands*." (Observations, §8.4). Specifically, "*[b]efore such a course may be taken, the Secretary of State must certify that it is necessary under s.16 RIPA*". (§8.4). Thus, the Government admits that persons resident outside the British Islands have less protection against the analysis of their communications than persons known to be present on those islands.

266. It is clear that persons in the British Islands are more likely to be of British nationality than those outside. Accordingly, the s16 safeguards have "*disproportionately prejudicial effects*" on non-British nationals and, as a result, there is indirect discrimination on the grounds of national origin. The IPT came to this conclusion in its First Judgment.[136]

267. The Government has advanced no legitimate basis for challenging this finding of the IPT. It relies solely on *Magee v United Kingdom*, a case where the applicant challenged "*a difference in treatment of detained*

[136] First Judgment, §144.

suspects" within the UK (§50). The Court found, in that case, that "*in the constituent parts of the United Kingdom there is not always a uniform approach to legislation*" and that "*[w]hether or not an individual can assert a right derived from legislation may accordingly depend on the geographical reach of the legislation at issue and the individual's location at the time*" rather than "*in terms of personal characteristics, such as national origin*" (§50). The Applicants contend that *Magee* is irrelevant to the issues raised by the s8(4) Regime, which concerns a single piece of legislation that accords disparate treatment to persons inside and outside the UK.

268. Furthermore, in *Carson v United Kingdom*, no. 42184/05, 16 March 2010, the Court held the words "other status" in Article 14 "*have been given a wide meaning so as to include, in certain circumstances, a distinction drawn on the basis of a place of residence*." (§70). Notably, in *Carson*, the Court also distinguished *Magee* on the basis that it concerned "*regional differences of treatment, resulting from the application of different legislation depending on the geographical location of an applicant*" rather than "*the different application of the same…legislation to persons depending on their residence and presence abroad*." (§70).

269. As a result, the lack of additional safeguards applying to those not resident in the British Islands is a relevant difference in treatment for the purposes of article 14. The Government was therefore correct to make the concession it did below, and there is no proper basis for taking a different approach now.

B. Justification

270. The Government contends that the difference in treatment between those for the time being in the British Islands and those who are not is justified because the Government has greater, alternative, powers of investigation

in relation to those in the British Islands. Thus, as it is put, the need for a s8(4) warrant is much rarer in relation to a person in Britain, and it is easier for the Secretary of State to satisfy herself that a s16(3) certificate is necessary (Observations, §§8.8-8.16).

271. In response:

(1) The Court's case law establishes that a difference of treatment is discriminatory 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*, §54).

(2) Contracting States enjoy a margin of appreciation in assessing whether and to what extent differences in otherwise similar situations justify a difference in treatment (§54; see *Hämäläinen v. Finland,* GC, App. no. 37359/09, 16 July 2014, §108). But the scope of the margin of appreciation will vary according to the circumstances, the subject matter and its background. The final decision as to the observance of the Convention's requirements rests with the Court (*Biao v Denmark,* GC, App. no. 38590/10, 24 May 2016, §93).

(3) The Government urges on the Court the case of *Stec v UK*, App. No. 65731/01, 12 April 2006, and its "*manifestly without reasonable foundation*" test. But *Stec* was a welfare benefits case, concerned with an upper limit of eligibility that had been tied into other benefits (and so severing them would have a number of complex implications). It was therefore a classic economic or social strategy case where a wider margin of appreciation is often afforded. *Stec* is very different to the present case.

(4) In the present case, there is no proper evidential basis for the practical problems claimed by the Government. No relevant open evidence was presented to the IPT. Furthermore, it is plain from the First Judgment that no evidence was advanced in closed: rather the IPT simply accepted a submission that it was "*obvious*" that it would be difficult "*if not impossible*" to provide a case for a certificate under section 16(3) in every case.[137]

(5) But it is submitted it is far from obvious. First, if no good justification could be put forward, it is difficult to see why there is a sound case for interception of such individuals.

(6) Secondly, it is impossible to reconcile the Government's claimed difficulties with its own case about how the s.8(4) regime works at the selection for examination stage. Paragraph 1.26(1) of the Government's Observations claims that the Government uses "*specific selectors, that is, specific identifiers relating to an individual target such as (for example) an e-mail address*." This directly contradicts the claim made here that it cannot issue a s16(3) certificate because it "*may not know who the individual is*". But if the target is known, there is no good reason not to afford the same level of safeguards. If GCHQ wish to target an NGO's London office they would need a warrant or 16(3) certificate. But if they wish to target the same NGO's German office, they would not need to do so. That distinction has no rational basis.

(7) Thirdly, the position is irrational. Section 16(3) is concerned with someone "*who is known to be for the time being in the British Islands*". That is concerned with present location (not, it may be noted, long term residence), and present location changes. It follows

[137] IPT First Judgment, §147(ii).

that the Government will require a certificate whilst someone is in Britain, but will not – and may access any s8(4) material unimpeded – once they are on holiday abroad. This shows that the regime is arbitrary, but it also makes it unjustifiable in Article 14 terms. Present geographical location has no necessary connection with what the Government does and does not know about someone.

V. VIOLATION OF ARTICLE 6

A. Determination of civil rights and obligations

272. Article 6 §1 "*secures to everyone the right to have a claim relating to his civil rights and obligations brought before a court*" (*Roche v United Kingdom*, App. no. 32555/96, 19 October 2005, §120). The Court has set out that, in determining whether civil rights and obligations are engaged, "*the starting point must be the provisions of the relevant domestic law and their interpretation by the domestic courts*" (*Fazia Ali v United Kingdom*, App. no. 40378/10, 20 October 2015, §54). Further, the Court has explained that it "*would need strong reasons to differ from the conclusions reached by the superior national courts by finding, contrary to their view, that there was arguably a right recognised by domestic law*." (§54).

273. In *Kennedy*, this Court noted 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*." (§179). While this Court formally left open in *Kennedy* the question of "*whether Article 6 applies to proceedings of this nature*", it nevertheless proceeded to an examination on the merits in that case.

274. The Government fails to engage this starting point. Rather, it relies entirely on pre-*Kennedy* jurisprudence. Thus, it cites the European Commission of Human Rights Report in *Klass*, which found that "*Art. 6 does not apply to this kind of State interference on security*" (Observations §7.1). The Government also makes reference to *Association for European Integration and Human Rights v Bulgaria,* no.62540/00, 28 June 2007 (Observations §7.2).

275. Neither of these cases is relevant. In *Klass,* the Applicants submitted that Article 6(1) had been violated because "*the legislation…does not require notification to the person concerned in all cases after the termination of surveillance measures and excludes recourse to the courts to test the lawfulness of such measures*." (§74), Similarly, in *Association for European Integration*, the Applicants' Article 6(1) complaint was that "*because by law they were not to be apprised at any point in time of the use of special means of surveillance against them, they could not seek redress against that in the courts*." (§104). Both cases therefore challenged the absence of a legal remedy against unlawful surveillance.

276. In the present case, by contrast, a tribunal that offers Applicants "*recourse…to test the lawfulness*" of surveillance and to "*seek redress against that*" already exists.

277. In *Klass*, this Court made clear that legal remedies of this nature "*satisfy the requirements of Article 6*" (§75). Its reasoning, in full, was:

> As long as it remains validly secret, the decision placing someone under surveillance is thereby incapable of judicial control on the initiative of the person concerned, within the meaning of Article 6; as a consequence, it of necessity escapes the requirements of that Article. The decision can come within the ambit of the said provision only after discontinuance of the surveillance…[T]he individual concerned, once he has been notified of such discontinuance, has at his disposal several legal remedies against

the possible infringements of his rights; these remedies would satisfy the requirements of Article 6 (§75).

278. The Government erroneously cites this reasoning for the proposition that "*the requirements of Art. 6 cannot apply to a dispute concerning the interception powers insofar as the use of such powers in the case at issue remain validly secret*" (Observations, §7.4). The UK, however, has established a system of "*judicial control*" enabling a person to challenge the lawfulness of surveillance and seek a legal remedy, *without* disclosing the existence of such surveillance. It has thereby granted persons a legal remedy "*against the possible infringements of [their] rights*" irrespective of secrecy. The Court has made clear that "*these remedies would satisfy the requirements of Article 6*".

279. The concept of "civil rights and obligations" is, of course, autonomous under the Convention (*Kennedy*, §179). In this respect, the Applicants observe, as set out in *Ferrazzini v Italy*, App. no. 44759/98, 12 July 2001, "*[t]he Convention is…a living instrument to be interpreted in the light of present-day conditions*" and the Court's consideration of the scope of Article 6(1) should assess "*changed attitudes in society as to the legal protection that falls to be accorded to individuals in their relations with the State*" (§26).[138] As discussed above and as this Court has recognised in Szabó, "*[g]iven the technological advances since…Klass…, the potential interferences with email, mobile phone and Internet services as well as*

[138] Further, the Court has taken an increasingly broad approach over the years to the interpretation of the concept of "civil rights and obligations". Thus, by way of example, it has considered that the right to welfare (*Fazia Ali v UK*), prisoners' detention arrangements (*Enea v Italy*, App. no. 74912/01, 17 Sept. 2009), the right to a good reputation (*Helmers v Sweden*, App. no. 11826/85, 29 Oct. 1991), and the right of access to administrative documents (*Loiseau v France*, App. no. 46809/99, 18 Nov. 2003), all constitute "civil rights and obligations" for the purposes of Article 6. In addition, although the Government seeks (Observations, §7.8) to rely on *Maaouia v France*, App. no. 39652/98, 5 Oct. 2000, to the effect that "the fact that a dispute may have major repercussions on an individual's private life does not suffice to bring proceedings within the scope of "civil" rights protected by Article 6(1)", the Court's jurisprudence has moved on since the time of that decision. Thus in *Alexandre v Portugal*, App. no. 33197/09, 20 Feb. 2013, the Court considered that Article 6 extends to proceedings which may unquestionably have a direct and significant impact on the individual's private life (§51). In that case, it was held that proceedings relating to the applicant's criminal record engaged Article 6 in view of the incontestable consequences those proceedings would have on his private life.

those of mass surveillance attract the Convention protection of private life even more acutely" (§53). The Applicants would submit – apart from the clear legal remedy afforded by the IPT and its own recognition that it determines questions of "civil rights" – that the development of covert surveillance capabilities and the resulting breadth and depth of intrusion warrant a recognition that Article 6(1) applies "*to proceedings concerning a decision to place a person under surveillance*" (*Kennedy*, §177).

B. Fairness

280. The question, therefore, is whether the restrictions in this case, taken as a whole, were disproportionate or impaired the very essence of the Applicants' fair trial rights.

281. The Applicants say that they did:

(1) In July 2016 it was discovered that on 15 November 2007, judicial members of the IPT met with MI5 at its headquarters.[139] MI5 explained its existing protocol, the effect of which was that the IPT would not be told about database holdings concerning any application to the IPT, save where those holdings had actually been accessed. The IPT did not dissent from this protocol, which appears to have been applied ever since.

(2) It is striking that a meeting of this kind took place at all. It was a secret meeting, and its existence was not known until the protocol was disclosed in other proceedings.[140] Prior to that, and despite the present proceedings, no-one apparently thought it necessary to inform the Applicants about the meeting, still less about the fact that one of the judges in this case had been present at it (Mr Robert

[139] Reply Annex, no. 34.
[140] *Privacy International v Secretary of State for Foreign and Commonwealth Affairs et al.,* IPT/15/110/CH.

Seabrook QC). Had it not been for the other IPT proceedings, this would never have been known.

(3) This is contrary to the Article 6 requirement for independence.

282. In addition, however, there is the issue of the protocol itself. If this protocol was applied in the present case then the IPT would be entirely unable to determine the question whether information had been obtained and stored (but not accessed) and whether that was proportionate. Under the protocol, the IPT would never be told. It could not even determine whether such data had been held too long, and in breach of the security services' own internal arrangements.

283. For this reason the Government has been asked whether the protocol was applied in this case. The Government's response is that it would not have been reasonable or proportionate to search "*unselected section 8(4) data*", and this is to the "*evident satisfaction*" of the IPT. The Applicants disagree, and the Applicants have not even been heard on the issue. This is plainly unfair.

284. Another issue casting doubt on the IPT's effectiveness concerns how it came to make a determination in favour of the wrong applicant. By way of recap:

(1) Prior to the third judgment formally being handed down, the Applicants and the Respondents received an embargoed copy of the draft judgment. Both sides submitted a list of suggested corrections at the request of the IPT. The Respondents did not identify any error in relation to the identity of the parties in whose favour the IPT had made a determination.

(2) Thirteen days after the third judgment was circulated to the Applicants, and nine days after it was published, the IPT emailed the Applicants to inform them that the finding relating to the breach of the time limits for retention "*in fact related to Amnesty International Ltd…and not the Egyptian Initiative for Personal Rights*".

(3) The IPT did not explain how such a fundamental error had occurred or why it was not detected until sometime after the judgment was handed down. Instead, the Tribunal merely stated (some three weeks later) that the "*mistaken attribution occurred after all judicial consideration had taken place and related only to the production of the determination for hand down*".[141]

285. It is submitted that this error matters. The IPT was, at this stage, carrying out an assessment concerning the proportionality of the interference with the applicants' rights. Plainly the identity of Amnesty International was relevant to that assessment. There are very serious concerns surrounding the obtaining, and storage, of the communications of a respected human rights organisation. Put simply: how did the IPT carry out the necessary balancing exercise when it thought it was dealing with a different NGO carrying out a different function?

VI. VIOLATION OF ARTICLE 10

286. 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, App. no. 37374/05, 14 April 2009, §27; *Riolo v. Italy*, App. no. 42211/07, 17 July 2008, §63; *Vides Aizsardzības Klubs v. Latvia*, App. no. 57829/00, 27 May 2004, §42).

[141] Letter from the Tribunal dated 1 July 2015. Reply Annex No. 18A.

287. The Government accepts "*NGOs engaged in the legitimate gathering of information of public interest in order to contribute to public debate may properly claim the same Art. 10 protections as the press*." (Observations, §6.1). Accordingly, it recognises that *"[i]n principle, therefore, the obtaining, retention, use or disclosure of the applicants' communications and communications data may potentially amount to an interference with their Art. 10 rights*" (§6.1).

288. The IPT determined that "*[t]he issues in relation to Article 10…were…simply mirror images of the same issues under Article 8 and raised…no further or separate issue*."[142]

289. In general terms, both the s8(4) and intelligence sharing regimes contravene Article 10 for the same reasons that they contravene Article 8.

290. In addition, the IPT erred in failing to address whether particular safeguards – to protect NGOs' confidential and privileged communications – existed in the s8(4) and intelligence sharing regimes. The Government has provided no indication of the existence of any procedural safeguards – secret or otherwise – commensurate with the importance of the social watchdog role of human rights NGOs' Article 10 rights. (*Sanoma Uitgevers B.V. v. the Netherlands*, App. no. 38224/03, 14 Sept. 2010, §88).

291. The regimes for dealing with including accessing privileged NGO communications under s8(4) and intelligence sharing are insufficient because they fail to provide a guarantee of review by a judge or other independent and impartial decision-making body. (*Sanoma Uitgevers B.V.*, §89). As noted by the Court in *Sanoma Uitgevers B.V.*, "*the 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*

[142] First IPT Judgment, §135.

journalistic sources exists prior to the handing over of such material capable of disclosing the sources' identity" (§90).

292. Compounding this deficiency, the regimes lack any effective, independent and impartial post-factum review of decisions to access privileged NGO communications. The IPT neither offers nor performs an effective review function, as explained above.

293. The Government insists in its Observations that its Code contains sufficient safeguards concerning journalistic material. But these alleged safeguards are nothing more than restatements of "considerations" which may be taken into account.[143] The Code does not address NGOs' privileged communications.

294. The Applicants also submit that the subjection of human rights NGOs' privileged communications to s8(4) surveillance or intelligence sharing is neither a necessary nor a proportionate restriction on their Article 10 rights. Both regimes put human rights NGOs' public watchdog role and functions at risk by exerting a chilling effect on them and those with whom they communicate. (mutatis mutandis, *Nordisk Film & TV A/S v. Denmark*, App. no. 40485/02, 8 Dec. 2005[144]). It also raises risks to the safety, well-being and life of victims of serious human rights violations that work with human rights NGOs.

[143] Code of Practice, §4.2.
[144] The Court accepted the possibility that the compulsory handover of research material might have a chilling effect on the exercise of journalistic freedom of expression and was therefore in breach of Article 10.

APPLICANTS' REPLY TO THE COURT'S QUESTIONS

Question 1.

Can the applicants claim to be "victims", within the meaning of Article 34 of the Convention, of violations of their rights under Articles 8 and 10?

Yes, for the reasons set out at paras 251-261 above.

Question 2.
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 in respect of "external communications", in particular with regard to their impact on non-governmental organisations and their confidential information and communications;
(b) the soliciting, receipt, search, analysis, dissemination, storage and destruction of interception data by the United Kingdom in respect of "communications data", in particular with regard to their impact on non-governmental organisations and their confidential information and communications;

"in accordance with the law" and "necessary in a democratic society" within the meaning of Article 8 of the Convention, with reference to the principles set out in, among other authorities, Weber and Saravia v. Germany (dec.), no. 54934/00, ECHR 2006-XI; Liberty and Others v. the United Kingdom, no. 58243/00, 1 July 2008; and Iordachi and Others v. Moldova, no. 25198/02, 10 February 2009?

No, for the reasons set out at paras 127-250 above.

Question 3.
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 in respect of "external communications", in particular with regard to their impact on non-governmental organisations and their confidential information and communications;
(b) the soliciting, receipt, search, analysis, dissemination, storage and destruction of interception data by the United Kingdom in respect

of "communications data", in particular with regard to their impact on non-governmental organisations and their confidential information and communications;

"prescribed by law", and "necessary in a democratic society" in the pursuit of a legitimate aim, within the meaning of Article 10 of the Convention reference to the principles set out in, among other authorities, Nordisk Film & TV A/S v Denmark, no. 40485/02, 8 December 2005; Financial Times Ltd and Others v the United Kingdom, no 821/03, 15 December 2009; Telegraaf Media Nederland Landelijke Media B.V. and Others v the Netherlands, no. 39315/06, 22 November 2012; and Nagla v. Latvia, no. 73469/10, 16 July 2013?

No, for the reasons set out at paras 127-250 and 286-294 above.

Question 4

Did the proceedings before the Investigatory Powers Tribunal involve the determination of "civil rights and obligations" within the meaning of Article 6 § 1 (*Klass and Others v. Germany*, 6 September 1978, § 75, Series A no.28)?

Yes, for the reasons set out at paras 272-279 above.

Question 5

If so, were the restrictions 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 Kennedy v. the United Kingdom, no. 26839/05, § 186, 18 May 2010)?

Yes, for the reasons set out at paras 280-285 above.

Question 6.

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

Yes, for the reasons set out at paras 262-271 above.