IN THE EUROPEAN COURT OF HUMAN RIGHTS Application No.

B E T W E E N

10 HUMAN RIGHTS ORGANISATIONS

Applicants

- and -

UNITED KINGDOM

Respondent Government

ADDITIONAL SUBMISSIONS ON THE FACTS AND COMPLAINTS

I. OUTLINE

1. The Applicants – the American Civil Liberties Union, Amnesty International, Bytes for All, the Canadian Civil Liberties Association, the Egyptian Initiative for Personal Rights, the Hungarian Civil Liberties Union, the Irish Council for Civil Liberties, the Legal Resources Centre, Liberty, Privacy International - are ten non-governmental human rights organisations based both within and outside the United Kingdom. Their complaints to this Court are concerned with mass bulk interception, collection, inspection, distribution and retention of communications on a vast, unprecedented scale. The process involves hundreds of millions of communications and takes place without any judicial authorisation.

2. The UK Government carries out such activity itself. It also receives the product of such activity carried out by the US Government. The Applicants complain of violations of their rights both in relation to the content of their communications and the associated metadata ('communications data').

3. In June 2013, a former US National Security Agency ('NSA') systems administrator, Edward Snowden, disclosed the existence of secret programmes relating to bulk collection, retention and sharing of millions of communications. The Applicants complained about violations of their rights to the Investigatory Powers Tribunal ('IPT'). A public hearing took place in July 2014, followed by a 'closed' hearing from which the Applicants were excluded. The IPT rejected most of the Applicants' claims in judgments in December 2014 and February 2015. The Applicants complain to this Court of the following violations of their Convention rights:
   (1) **Articles 8 and 10**: The UK Government's interception, inspection, retention and storage and disclosure of the Applicants' communications (content and 'communications data') and its receipt, inspection, retention and storage of such communications from the US Government was not in accordance with the law <u>and</u> was disproportionate.
   (2) **Article 14**: In association with interferences with Articles 8 and 10, the different treatment and applicable safeguards for persons within the UK when compared to persons outside the UK were discriminatory and not justified.
   (3) **Article 6**: The procedure by which the Applicants' claims were heard was unfair, particularly in relation to the IPT holding closed proceedings on issues of law; and the lack of adequate disclosure.

II. STATEMENT OF THE FACTS

4. As part of their human rights activities, each of the Applicants communicates on a regular basis with a wide range of groups and individuals, both nationally and internationally. The persons with whom they communicate include other NGOs and human rights defenders, journalists, lawyers, prisoners, victims of human rights abuses, politicians, governmental officials and whistle-blowers.

The Applicants and their staff members communicate using a variety of means, 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 is of paramount importance in order for them to effectively fulfil their role to seek, receive and impart information of public interest.

5. In May 2013, Edward Snowden leaked copies of classified files to a group of journalists. The disclosures revealed, for the first time, the existence and scale of the following bulk interception programmes:
   (1) *TEMPORA* – a UK Government programme that involves intercepting communications passing through submarine fibre optic cables entering and exiting the United Kingdom. This enables GCHQ to access both content and communications data being transmitted through those cables. The UK Government has not admitted the existence of TEMPORA. However, leaked documents indicate that it has been authorised by a series of generic warrants issued under s8(4) of RIPA (which permit the interception of *"external communications"* – see below). The Intelligence and Security Committee of Parliament has now subsequently confirmed that: "GCHQ … has access to communications as they move over the internet via major internet cables."[1]
   (2) *UPSTREAM* – a series of US Government programmes, similar to TEMPORA, that enable the NSA to access vast amounts of communications and communications data carried by the submarine fibre optic cables passing through, into and out of the US.
   (3) *PRISM* - a US Government programme which allows the NSA to access communications from many of the leading internet service providers including Apple, Facebook, Google, Microsoft, Skype, Yahoo, and YouTube. Reports indicated that GCHQ has had access to PRISM material since 2010 and has generated a number of intelligence reports as a result. The existence of PRISM and UPSTREAM has since been acknowledged publicly by the US Government.
   The communications and communications data obtained by the US Government under both PRISM and UPSTREAM may be provided by the US Government to the UK Government, and then inspected and stored by the UK Government.

6. Following the issuing of the IPT proceedings in this case, over the past two years a number of additional programmes by which the NSA and GCHQ intercept, store and analyse communications and communications data within and outside the US and UK have been revealed. These were drawn to the attention of the IPT.

7. The scale of these programmes is underlined by the fact that the majority of the world's internet traffic – particularly that between Europe and North America –travels on undersea fibre optic cables that are being tapped by GCHQ, the NSA or both. PRISM, TEMPORA, UPSTREAM and the other programmes therefore enable GCHQ and the NSA to intercept the communications – and collect the communications data – of hundreds of millions of people worldwide on a daily basis.

8. In light of these programmes, the Applicants believe that the content of their private communications and/or their communications data have been obtained by the UK government:
   (1) As a result of their interception and/or collection by the NSA, pursuant to PRISM and UPSTREAM, and subsequent provision by the US Government to the UK Government's security and intelligence agencies; and/or

[1] Report on the intelligence relating to the murder of Fusilier Lee Rigby (HC 795, 25 November 2014), p135.

(2) As a result of interception and collection by GCHQ directly, by way of programmes such as TEMPORA.

9. Between June and December 2013, each of the Applicants lodged complaints before the IPT. The complaints alleged that the intelligence services, the Secretary of State for the Home Department and Secretary of State for Foreign and Commonwealth Affairs had acted unlawfully under Articles 8, 10 and 14 by (a) intercepting, inspecting and retaining the Applicants' communications and their communications data; and (b) accessing or otherwise receiving their intercepted communications and communications data from the US government and inspecting, retaining and storing that material.

10. As part of their complaints, each of the Applicants sought disclosure of all relevant material relied on by the intelligence services, in particular disclosure of all policies and guidance adopted by the services (redacted as necessary).

11. On 14 February 2014, the IPT ordered that the Applicants' claims should be joined. The Government adopted a "neither confirm nor deny" stance in response to the Applicants' claims. As a result, it was agreed that the hearing would determine issues of law on the basis of assumed hypothetical factual premises agreed between the parties. The IPT ordered that the hearing would be *inter partes* and held in public.

12. On 16 May 2014, the respondents provided the Applicants with a witness statement from Charles Farr, the Director-General of the Office for Security and Counter Terrorism ("OSCT") at the Home Office. In that statement, Mr Farr claimed that the internal arrangements of the intelligence services under ss15 and 16 RIPA *"cannot safely be put into the public domain without undermining the effectiveness of interception methods"* (§100). Similarly, the UK's international intelligence sharing arrangements and the intelligence services' internal guidance for the handling and use of such information *"cannot safely be published without undermining the interests of national security and the prevention and detection of serious crime"* (§55). Mr Farr also set out, for the very first time, how the government understood the term "external communications" under s20 RIPA operates in the context of some common uses of the internet, such as a Google search, a Facebook post or a 'tweet' on Twitter (§126 – 141).

13. Between 14 and 18 July 2014, an open hearing was held in which the parties made submissions on the agreed issues.[2] In the course of the open hearing the Respondents invited the IPT to hold a closed session in order to consider the intelligence services' secret internal guidance. The Applicants objected on the basis that there could be no proper basis for the IPT to consider closed material in order to determine whether the relevant legal framework was 'in accordance with law' pursuant to Articles 8 and 10 ECHR.[3] In the alternative, the Applicants invited the IPT to disclose sufficient information concerning the closed material in order to allow them to make effective submissions. In addition, some of the Applicants asked the IPT to appoint one or more special advocates to represent their interests at any closed hearing. The IPT refused each of these requests.

14. On 10 September 2014, the IPT held a closed hearing at which it considered *inter alia* the internal arrangements of the intelligence services as outlined above[4]. The Applicants were not represented

[2] The hearing was also attended by Counsel to the IPT, who made submissions on the relevant law.
[3] Counsel to the IPT supported this submission.
[4] See paragraph 7 of the IPT's judgment.

at the hearing. Nor were they provided with a summary of the closed material.

15. On 9 October 2014, the Applicants were notified by the IPT that it had "*concluded that there was closed material relied upon by the [Respondents] which could be disclosed to the parties, and invited the [Respondents] to consent to such disclosure*". The Applicants subsequently received an untitled note from the IPT that appeared to summarise some of the Respondents' internal guidance for the receipt of intercepted material from foreign governments.

16. On 14 October 2014, the Applicants asked the IPT to provide some indication as to the "*nature, provenance and history*" of the note as well as "*the reliance placed upon it*" by the intelligence services in the closed proceedings. By an email dated 15 October 2014, the IPT refused this request. The status of the note was unclear. It is not clear whether it is an actual policy, or part of a policy, used by the intelligence services, a summary of a policy, or a summary of submissions made by the services at a closed hearing. It is also not clear whether the note sets out an approach that the intelligence services regard as binding or is simply a description of desirable practices. It is not clear who promulgated the note or has the power to amend it.

17. On 23 October and 5 November 2014, the Respondents produced fresh versions of the note, each time containing further corrections.

18. On 6 November 2014, the NGO Reprieve published details of the disclosure that it had received from the intelligence services on 29 October 2014 in the matter of *Belhaj and others v Security Service and others* (IPT/13/132-9/H) ('the *Belhaj* material'). This material included internal guidance from the Respondents on how they dealt with intercepted material subject to legal professional privilege ('LPP').

19. At an open hearing held on 7 November 2014, the Applicants renewed their application for further disclosure of all relevant material relating to the Respondent's internal arrangements under ss.15 and 16 RIPA. Among other things, the Applicants noted that Exhibit 14 of the *Belhaj* material appeared to be the original document upon which the intelligence service's note had been based. The IPT refused the Applicants' application but directed the intelligence services to clarify the relationship between Exhibit 14 of the *Belhaj* material and the note provided to the Applicants.

20. On 12 November 2014, the intelligence services provided the Applicants with a note on Exhibit 14, together with a further version of the note containing additional text *"intended to address certain of the [Applicants'] concerns in relation to the [note]".*
21. On 17 November 2014, the Applicants renewed their application for disclosure of all relevant material relating to the internal guidance of the intelligence services, particularly in relation to the handling of confidential material that had been obtained by the interception of private communications either under s8(4) of RIPA or from a foreign intelligence service. This was refused.

The First IPT Judgment

22. On 5 December 2014, the IPT gave judgment on several of the legal issues. In relation to the regime for interception, examination and retention of communications and data under s8(4) associated with TEMPORA, the IPT reached the following conclusions:
    (1) Bulk surveillance would be impermissible within the statutory regime: "*the Respondents are not seeking, <u>nor asserting that the system entitles them</u> to seek, to carry out what has been described as "mass" or "bulk" surveillance*" (§72).

(2) It was "*impossible*" to know or differentiate at the time of interception, i.e. in the course of transmission, what is an 'external' and what is an 'internal' communication, "*and such has always been the case*" (§94(i)-(ii));
(3) It was "*inevitable*" that, "*when a telephone call is made from a mobile phone or iPhone, or an email is sent to an email address, it will not necessarily be known whether it will be received in the United Kingdom or in the course of travel or at a foreign destination*" (§95(iii));
(4) Interception under a s8(4) warrant occurs before any question of selection for examination arises under s16 (which contains safeguards relating to examination). Accordingly, "*the relevance of the internal/external distinction has no relation to the s16 examination, when a communication may be accessed and read*" (§95);
(5) Although the changes in technology since RIPA's enactment in 2000 have been "*substantial*", they do not "*constitute any material addition to the quantity (or proportion) of communications which either could or could not be <u>differentiated</u> as being* internal *or* external *at the time of interception*" (§98(iii));
(6) Notwithstanding that RIPA purported to distinguish between targeted and non-targeted interceptions, the absence of targeting at the point of interception was "*acceptable and inevitable*" (§116(ii));
(7) The absence of any requirement for search terms to be included in an application for an interception warrant, or for judicial authorisation of such warrants, was not incompatible with the requirements identified with the Court in *Weber and Saravia v Germany* (§§116(v)-(vi));
(8) The IPT was entitled to look at "*the rules, requirements and arrangements, both those expressly set out in statute or in the Code and those set out in more detail in arrangements below the waterline, but which are sufficiently signalled in publicly available documents to ensure both that any abuse is avoided and a sufficient degree of accessibility and foreseeability is secured*" (§120);
(9) It was not, therefore, necessary for the Applicants to receive further disclosure of any arrangements from "*below the waterline*" along the lines of that provided in *Belhaj* since the IPT's task on this issue was only to assess their accessibility "*by reference to the extent to which the scope of the discretion of the Respondents is revealed or the nature of the arrangements is adequately signposted*" (§133(ii)). There were already "*very substantial published procedures in s15 and the Code*" (§137);
(10) The IPT was satisfied that there were "*adequate arrangements, in respect of duration of retention and destruction, to control and regulate the retention of [intercepted] material*" and the s8(4) regime was therefore "*sufficiently compliant with the Weber requirements and in any event is in accordance with law*" (§140).

23. In relation to Article 10, the IPT accepted that the Applicants "*may be entitled to the benefit of any protection under Article 10 otherwise available to journalists*" but held that "*the present system is adequate in accordance with Convention jurisprudence without prior judicial authorisation*", particularly given that the Applicants' case was "*not … a case of <u>targeted</u> surveillance of journalists, or indeed of NGOs*" (§151).

24. On the issue of discrimination under Article 14, the IPT concluded that any indirect discrimination entailed by the differential treatment under s16(2) of the communications of persons in the UK, as against those outside the UK, was sufficiently justified because "*it is harder to investigate terrorism and crime abroad and difficult if not impossible to provide a case for a certificate under s16(3) in every case*" and "*the imposition for a s16(3) certificate in every case would radically undermine the efficiency of the s8(4) regime*" (§§147-148).

25. Following the first judgment, the IPT invited the parties to make submissions on whether the US/UK intelligence sharing regime was in accordance with the law prior to the disclosures made

by the intelligence services following the closed hearing, as well as submissions "*on the proportionality and lawfulness of any alleged interception of [the Applicants] communications*". In the course of those submissions, the intelligence services further clarified the safeguards that existed in relation to the receipt of communications intercepted by foreign intelligence services.

26. In relation to the legal framework governing the receipt of information obtained under PRISM and UPSTREAM - the IPT ruled that following the disclosure described above at (15)-(17):
    (1) It was "*entitled to look below the waterline in order to be satisfied (a) that there are adequate safeguards (b) that what is described above the waterline is accurate and gives a sufficiently clear signpost to what is below the waterline without disclosing detail of it*" (§50(i));
    (2) It was satisfied that "*there are adequate arrangements in place for the purpose of ensuring compliance with the statutory framework and with Articles 8 and 10 of the Convention, so far as the receipt of intercept from Prism and/or Upstream is concerned*" (§55(i));
    (3) Those arrangements were "*sufficiently accessible to the public*" because they were "*sufficiently signposted by virtue of the statutory framework … and the Statements of the ISC and the Commissioner quoted above, and … after the two closed hearings … publicly disclosed by the [intelligence services] and recorded in this judgment*" (§55(ii)); and
    (4) Those arrangements were also "*subject to oversight*" (§55(iii)) including by the IPT itself (§§45-46) and therefore the scope of the intelligence service's discretion to receive and handle intercepted material and communications data and the manner of its exercise were "*accessible with sufficient clarity to give the individual adequate protection against arbitrary interference*" (§55 (iv)).

The Second IPT Judgment

27. On 6 February 2015, the IPT delivered its second judgment, in which it declared that prior to the disclosures made and referred to in its first and second judgments: *"the regime governing the soliciting, receiving, storing and transmitting by UK authorities of private communications of individuals located in the UK, which have been obtained by US authorities pursuant to Prism and/or Upstream, contravened Articles 8 or 10 ECHR."* The IPT went on to conclude that, as a result of those disclosures, the regime now complies with Articles 8 and 10.

28. As of the date of this application, the IPT has yet to determine whether in fact any interception of the Applicants' communications has taken place and, if so, whether such interception was necessary and proportionate.

The ISC Report

29. On 12 March 2015, the Intelligence and Security Committee of Parliament, which has responsibility for oversight of the UK intelligence services, published a report entitled *'Privacy and Security: A modern and transparent legal framework'* ('the ISC Report'). It was the most detailed review since the Edward Snowden disclosures. The ISC expressed significant concerns about several aspects of the statutory regimes considered in this claim, including the definition of 'external' and 'internal' communications; the lack of clarity within the existing statutory provisions; and the lack of a clear legal framework in relation to the compiling, retention and oversight of databases of communications and related data. It recommended fundamental changes to the existing legislative and oversight regimes in order to address those concerns.

B. Relevant Domestic law

The Regulation of Investigatory Powers Act 2000

30. Section 5(1) of RIPA empowers the Secretary of State to issue a warrant authorising the interception of the communications described in the warrant. Under s5(2), no warrant for interception of communications shall be issued unless the Secretary of State believes that the

warrant is necessary on grounds falling within subsection (3) and that the conduct being authorised is proportionate. Subsection (3) provides:

Subject to the following provisions of this section, a warrant is necessary on grounds falling within this subsection 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

31. Section 5(6) further provides that:

The conduct authorised by an interception warrant shall be taken to include—

(a) all such conduct (including the interception of communications not identified by the warrant) as it is necessary to undertake in order to do what is expressly authorised or required by the warrant; [and]
(b) conduct for obtaining related communications data; …

32. Section 8 provides for two types of interception warrants: a 'targeted' warrant under s8(1) and an 'untargeted' warrant for the interception of external communications under s8(4):

(1) An interception warrant must name or describe either—
(a) one person as the interception subject; or
(b) a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place.
(2) The provisions of an interception warrant describing communications the interception of which is authorised or required by the warrant must comprise one or more schedules setting out the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications that may be or are to be intercepted.
(3) Any factor or combination of factors set out in accordance with subsection (2) must be one that identifies communications which are likely to be or to include—
(a) communications from, or intended for, the person named or described in the warrant in accordance with subsection (1); or
(b) communications originating on, or intended for transmission to, the premises so named or described.
(4) Subsections (1) and (2) shall not apply to an interception warrant if—
(a) the description of communications to which the warrant relates confines the conduct authorised or required by the warrant to conduct falling within subsection (5); and
(b) at the time of the issue of the warrant, a certificate applicable to the warrant has been issued by the Secretary of State certifying—
(i) the descriptions of intercepted material the examination of which he considers necessary; and
(ii) that he considers the examination of material of those descriptions necessary as mentioned in section 5(3)(a), (b) or (c)
(5) Conduct falls within this subsection if it consists in—
(a) the interception of external communications in the course of their transmission by means of a telecommunication system; and
(b) any conduct authorised in relation to any such interception by section 5(6).
(6) A certificate for the purposes of subsection (4) shall not be issued except under the hand of the Secretary of State.

33. An "external communication" is defined by s20 as "*a communication sent or received outside the British Islands*".

34. Section 15 RIPA imposes a general duty on the Secretary of State to make relevant

"arrangements" as follows:

(1) Subject to subsection (6), it shall be the duty of the Secretary of State to ensure, in relation to all interception warrants, that such arrangements are in force as he considers necessary for securing—

(a) that the requirements of subsections (2) and (3) are satisfied in relation to the intercepted material and any related communications data; and

(b) in the case of warrants in relation to which there are section 8(4) certificates, that the requirements of section 16 are also satisfied.

(2) The requirements of this subsection are satisfied in relation to the intercepted material and any related communications data if each of the following—

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

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

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

(d) the number of copies that are made,

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

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

(4) For the purposes of this section something is necessary for the authorised purposes if, and only if—

(a) it continues to be, or is likely to become, necessary as mentioned in section 5(3);…

(5) The arrangements for the time being in force under this section for securing that the requirements of subsection (2) are satisfied in relation to the intercepted material or any related communications data must include such arrangements as the Secretary of State considers necessary for securing that every copy of the material or data that is made is stored, for so long as it is retained, in a secure manner.

(6) Arrangements in relation to interception warrants which are made for the purposes of subsection (1)—

(a) shall not be required to secure that the requirements of subsections (2) and (3) are satisfied in so far as they relate to any of the intercepted material or related communications data, or any copy of any such material or data, possession of which has been surrendered to any authorities of a country or territory outside the United Kingdom; but

(b) shall be required to secure, in the case of every such warrant, that possession of the intercepted material and data and of copies of the material or data is surrendered to authorities of a country or territory outside the United Kingdom only if the requirements of subsection (7) are satisfied.

(7) The requirements of this subsection are satisfied in the case of a warrant if it appears to the Secretary of State—

(a) that requirements corresponding to those of subsections (2) and (3) will apply, to such extent (if any) as the Secretary of State thinks fit, in relation to any of the intercepted material or related communications data possession of which, or of any copy of which, is surrendered to the authorities in question; and

(b) that restrictions are in force which would prevent, to such extent (if any) as the Secretary of State thinks fit, the doing of anything in, for the purposes of or in connection with any proceedings outside the United Kingdom which would result in such a disclosure as, by virtue of section 17, could not be made in the United Kingdom.

35. Section 16 imposes further duties in respect of warrants issued under s8(4):
    (1) For the purposes of section 15 the requirements of this section, in the case of a warrant in relation to which there is a section 8(4) certificate, are that the intercepted material is read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant to the extent only that it—
        (a) has been certified as material the examination of which is necessary as mentioned in section 5(3)(a), (b) or (c); and
        (b) falls within subsection (2).
    (2) Subject to subsections (3) and (4), intercepted material falls within this subsection so far only as it is selected to be read, looked at or listened to otherwise than according to a factor which—
        (a) is referable to an individual who is known to be for the time being in the British Islands; and
        (b) has as its purpose, or one of its purposes, the identification of material contained in communications sent by him, or intended for him.
    (3) Intercepted material falls within subsection (2), notwithstanding that it is selected by reference to any such factor as is mentioned in paragraph (a) and (b) of that subsection, if—
        (a) it is certified by the Secretary of State for the purposes of section 8(4) that the examination of material selected according to factors referable to the individual in question 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.

36. Section 71 of RIPA requires the Secretary of State to issue a Code of Practice relating to the interception of communications. The Interception of Communications Code of Practice ('The Code') was originally published in 2002.

The Security Service Act 1989 and the Intelligence Services Act 1994

37. The functions of the Security Services ('MI5') are set out in s1 of the Security Service Act 1989. Those of the Secret Intelligence Service and GCHQ are set out at ss1 and 3 respectively of the Intelligence Services Act 1994.

The Counter-Terrorism Act 2008

38. Section 19(2) of the 2008 Act provides that information which any of the intelligence services obtain in connection with any of their functions "*may be used by that service in connection with the exercise of any of its other functions"*.

39. Sections 19(3)-(5) provide that information obtained by MI5, MI6 and GCHQ respectively for the purpose of any of their functions may also be disclosed for "*the purpose of the proper discharge of [those] functions*", "*the prevention or detection of serious crime*" or for "*any criminal proceedings*". Additionally, MI6 alone may also disclose information it obtains "*in the interests of national security*" (s19(4)(b)).

The Human Rights Act 1998

40. Section 6(1) of the Human Rights Act 1998 ('HRA') provides that it is unlawful for a public authority (which includes the Respondents) to act in a way that is incompatible with a right under the Convention.

III. STATEMENT OF ALLEGED VIOLATIONS OF THE CONVENTION AND OF RELEVANT ARGUMENTS

41. The UK Government does not dispute that its interception and/or receipt, examination and storage of individuals' personal communications and data interferes with their rights under Articles 8 and 10. The issue is whether such interference is 'in accordance with the law/ prescribed by law', necessary and proportionate. There is also no dispute that the Applicants have sufficient standing to pursue their complaints, even in circumstances where the Government has not formally confirmed the existence of the programme in question.

A. Violations of Articles 8 and 10 – Bulk interception, examination and storage of communications* and *communications data, pursuant to s8(4) / TEMPORA is not in accordance with the law / prescribed by law.

42. The interception of communications constitutes an interference with the right to privacy of those communications under Article 8(1), whether made via email, phone, text message, or social media: see e.g. *Klass v Germany* 6 September 1978, Series A No 28 at §41; *Weber and Saravia v Germany* ECHR 2006 XI at §77; *Kennedy v United Kingdom* 26839/05 18 May 2010 at §118. The same is true in respect of accessing communications data or 'metadata': see e.g. *Malone v United Kingdom* 2 Aug 1984, Series A No 82 at §84. Further interferences arise from the collection and retention of such material (see e.g. *Amann v Switzerland* [GC] ECHR 2000-II – especially on a searchable database – and its transmission to other authorities (*Weber and Saravia v Germany* at §79)).

43. The s8(4) regime under which the UK Government carries out bulk interception, examination and storage, is not "in accordance with the law" as required Article 8(2) for the following reasons:

<u>*Lack of adequate safeguards*</u>

44. This Court has made clear that in order for the bulk interception of communications to be in accordance with the law, the legal framework must provide the minimum statutory safeguards to protect against arbitrary interference and abuse. Specifically, the legal framework must address:
    (1) *The nature of the offences which may give rise to an interception order:* interception under a s8(4) warrant does not require any suspicion whatsoever on the part of the authorities that a person has committed a criminal offence;
    (2) *A definition of the categories of people liable to have their communications monitored:* there are no categories of persons who are liable to have their communications intercepted under a s8(4) warrant;
    (3) *A limit on the duration of such monitoring*: warrants under s8(4) are limited in duration, but may be renewed. Unlike a s8(1) warrant there is no requirement of targeting against a particular individual or premises and therefore no restriction on the possibility that a person's communications may be routinely intercepted, again and again, for an indefinite period under successive s8(4) warrants. The scale of interception, taken together with their generic nature and the power to renew such warrants indefinitely, renders the statutory time limits effectively meaningless;
    (4) *The procedure to be followed for examining, using and storing the data obtained:* The details in relation to the examining, using and storing of the material are entirely unclear, particularly in the context of communications data;
    (5) *The precautions to be taken when communicating the data to other parties:* under s15(6), the usual restrictions on communicating and dealing with data obtained under a s8(4) warrant do not apply if the material is provided to foreign authorities, subject to the further restrictions of s15(7). Other than requiring the Secretary of State to ensure that the existence of the interception is not disclosed, however, any restrictions placed on the use of the disclosed material by the foreign authorities is entirely at the discretion of the Secretary of State; and
    (6) *The circumstances in which data obtained may or must be erased or the records destroyed*: Although the 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 – particularly in the context of communications data – what this means in practice.

The statutory distinction under s20 of RIPA between targeted interception of 'internal' and untargeted interception of 'external' communications under provides no meaningful safeguard in the context of bulk interceptions

45. In practice, any practical distinction between the interception of 'internal' communications and that of 'external' communications, has been fundamentally eroded:
    (1) Tapping fibre optic cables means that vast amounts of both 'internal' and 'external' communications will be gathered as a by-product of bulk interception under s8(4). Once collected, there is no statutory requirement on the UK Government to discard, filter or ignore those communications only as a by-product of bulk collection. The UK Government may examine, retain and store <u>all</u> communications intercepted, subject only to the safeguards contained in ss15 and 16. Those safeguards are themselves ineffective (see below).
    (2) In any event, the definition of 'internal' and 'external' communications under s20 is unclear. In its first judgment, the IPT accepted that "*the changes in technology*" were "*substantial*" (§98(iii)) and acknowledged that there was a real dispute between the parties as to whether certain internet-based communications were properly to be treated as 'internal' or 'external' for the purposes of s20 (see §97(iv)). The IPT's suggestion that such uncertainty was foreseen by Parliament, is flawed: if there is real uncertainty as to which types of internet-based communications are internal and external, then it follows that the scope of s8(4) warrants in relation to 'external' communications lacks clarity. The Code provides only limited assistance and is silent on the status of many forms of modern internet based communication, (see below).
    (3) Members of the public remain entitled to "*an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures*" (*Malone,* §67). The definition of '*external communications*' under s20 and the warranty and certification provisions in ss5 and 8(4) do not meet this standard.

<u>*The additional s16 safeguards are inadequate*</u>

46. Section 16 of RIPA purports to provide additional safeguards for material obtained by way of bulk collection, through a s8(4) warrant. However, it is inadequate in a number of critical ways:
    (1) Section 16 does not apply to 'communications data' (metadata). It only applies to "intercepted material", which s20 defines as "*the <u>contents</u> of any communications intercepted by an interception to which the warrant relates*". The inspection, storage, use and communication of a person's metadata therefore is a significant interference with their Article 8 rights[5], but the s16 safeguard is simply absent in relation to such material;
    (2) Material intercepted under a s8(4) warrant may only be "*read, looked at or listened to*" under s16(1)(a) if it has been certified "*as material the examination of which is necessary*" for one of the grounds in s5(3), e.g. in the interests of national security or the purpose of preventing or detecting serious crime. However, each of these categories is exceedingly broad and – taken together with the absence of any requirement for targeting – provides no meaningful restriction on the scope of the intelligence services' discretion to inspect intercepted material;
    (3) Section 16(2) provides that intercepted material cannot be selected to be "*read, looked at or listened to otherwise than according to a factor*" which is "*referable to an individual who is known to be for the time being in the British Islands*" and also has as its purpose "*the identification of material contained in communications sent by him or intended for him*":
        (a) A factor "*referable to an individual*" might prevent an individual in the UK being searched

[5] See the First Statement of Eric King, §§18-24; and more generally *Malone v United Kingdom* at §84)

for by their name or last known address, but it would not prevent inspection of their communications by reference to a wide range of other selectors, e.g. residence of a particular neighbourhood or attendance at a particular mosque;

(b) Section 16(2) prevents inspection where the individual is "*known to be for the time being in the British Islands*". It does not prevent inspection even where there is a strong suspicion that a person is currently in the UK, or where a person has temporarily left the UK;

(c) The restriction in s16(2) also only applies where the inspection has "*as its purpose or one of its purposes the identification of material contained in communications sent by him or intended for him*". It places no restriction on the inspection of material relating to a person, if the inspection was for the purpose of identifying material intended for a friend, family member or associate.

(4) In any event, the 'safeguards' in s16(2) can be swept aside by the wide discretion given to the Secretary of State under s16(3), to permit searches not subject to the section 16(2) safeguards of any material obtained through a s8(4) warrant;

(5) Section 16(2) provides no protection for persons who are known to be outside the British Islands, even if they are living in the UK but are only abroad for a short period. The majority of the Applicants and their staff fall into this category, being based outside the UK.

There are no meaningful safeguards against the compiling and retention of databases or 'datasets' of intercepted communications and communications data

47. Section 15(3) of RIPA requires that any copies of intercepted material and any related communications data should be destroyed "*as soon as there are no longer grounds for retaining it as necessary for the authorised purposes*". However, that safeguard is undermined by s15(4) which directs that retention will be "*necessary for any of the authorised purposes"* if it is necessary "*or is likely to become*" necessary for one of the broad generic categories in s5(3)(a)-(c). In effect, if mass interception under TEMPORA is carried out on the basis that obtaining and/or retaining vast quantities of communications data about the population will assist in building intelligence databases, and doing so is in the interests of national security or in preventing and detecting serious crime, then that data and those databases may be retained indefinitely while those generic purposes persist. There is nothing within RIPA or any published document which prevents or provides adequate oversight for such data collection and retention.

48. The ISC considered problems relating to databases and the need for changes to be made to address those problems, at Chapter 7 of its Report.

IPT misinterpretation of the decision of this Court in Liberty v UK (2008)

49. The approach of the IPT is also inconsistent with existing authority on UK bulk surveillance as reflected in this Court's decision in *Liberty and others v UK* (58243/00, 1 July 2008):

(1) The regime for the bulk interception of external communications under s8(4) RIPA is largely identical to the bulk interception regime under s3(2) of the Interception of Communications Act 1985 which the Court in *Liberty and others v United Kingdom* (58243/00, 1 July 2008) held to be insufficiently foreseeable and accessible, contrary to Article 8;

(2) To the extent that the regime under s8(4) differs from that under the 1985 Act - most notably by virtue of the Code - its provisions remain insufficiently foreseeable and accessible. In particular, the definition of "*external communications*" under s20 has not kept pace with fundamental changes in communication technology, to the extent that it is neither sufficiently precise nor adequately foreseeable in its application;

(3) The regime does not comply with the six requirements ("*minimal statutory safeguards to protect against arbitrary interference and abuse"*) identified by the Court in *Weber and Saravia v Germany*. The safeguards provided by ss15 and 16 RIPA are inadequate;

(4) The internal arrangements of the intelligence services under ss15 and 16 are neither publicly accessible nor foreseeable;
(5) Neither the Code nor the external scrutiny provided by the Interception of Communications Commissioner and the IPT are sufficient substitutes for the non-disclosure of the intelligence services' internal arrangements under ss15 and 16; and
(6) In any event, the internal arrangements do not themselves have the quality of 'law', as they are not publicly accessible and have never been either enacted by, or laid before, Parliament. Moreover, they can be changed by the Executive without public knowledge or Parliamentary oversight or consent.

50. In *Liberty and others v United Kingdom* this Court held that the regime for the bulk interception of external communications under s3(2) of the Interception of Communications Act 1985 did not indicate the scope and manner of the exercise of a very wide discretion, so as to provide adequate protection against abuse of power. In particular, it did not set out in a form accessible to the public the procedure to be followed for examination, sharing, storing and destroying intercepted material (§69).

51. The key elements of the s3(2) regime for the interception of external communications under the 1985 Act and those of the s8(4) regime under RIPA are materially identical. In particular, the requirements for the making of arrangements under ss15 and 16 RIPA are substantially the same as those under s6 of the 1985 Act.

52. In its first judgment, the IPT sought to distinguish *Liberty v UK* on the basis that the Court was "*addressing a regime which did not have the Code under s71 of RIPA … which had not been brought into force under the old Act*"[6]. The IPT also placed considerable weight on the Court's observation that, subsequent to the 1985 Act, "*extensive extracts [from the Code] are now in the public domain, which suggests that it is possible for the state to make public certain details about the operation of a scheme of external surveillance without compromising national security*"[7]. The IPT characterised this as being "*at the very least, a strong inference that with the Code the situation would have been different*"[8].

53. The IPT's approach misinterprets the decision in the *Liberty* v *UK* case, this Court was doing no more than noting the possibility that more information *could* have been made available. It therefore found a violation and did not need to determine other questions about the compatibility of the s8(4) regime. This Court was not suggesting that the subsequent publication of a Code made every other aspect of the disputed regime in accordance with the law.

54. Despite the IPT's reliance on it, the Code does not remedy flaws in the statutory regime for several reasons:
(1) It was published in 2002, well before the development of Facebook (2004), Gmail (2004), YouTube (2005) and Twitter (2006). It is therefore silent on how modern forms of internet use – such as Facebook messages – would fall to be defined under ss8, 15, 16 and 20 RIPA. Indeed, prior to the witness statement of Charles Farr in May 2014, there was no indication as to how Part 1 of RIPA – and s20 in particular – would apply to such services;
(2) It provides little further explanation about the s8(4) regime beyond what is already set out in statute. Chapters 5 and 6 in particular do little more than restate the statutory provisions using

[6] First IPT judgment, §88
[7] §68 of *Liberty v UK,* cited at §89 of the First IPT judgment.
[8] First IPT Judgment, §90.

slightly different language.[9] To the extent that the Code provides information not contained in RIPA, the material is generic and lacks specificity; and

(3) In particular, it contains no indication as to how the intelligence services may exercise their power of bulk interception under s8(4), including the potential scale of such interceptions. It gives no details as to the contents of a certificate issued under s8(4), nor how material intercepted under a s8(4) warrant (including communications data) may be subsequently selected for examination.

No public disclosure of broad terms of s8(4) certificates, or of internal rules

55. The s8(4) regime requires warrants to be certified by the Secretary of State. But that certification power is being interpreted very broadly to provide vague, generic purposes to be certified, with no meaningful safeguard against discriminatory and arbitrary exercise of the power. There are no published guidelines or requirements – even in general terms - as to the specificity required for a certificate; and the general terms of the certificates themselves are unnecessarily secret. Further, there are no clear requirements as to when and how frequently the terms of broad, vague certificates must be reviewed. This exercise of a broad, vague certification power, in secret and not subject to proper scrutiny or oversight, is not 'in accordance with the law / prescribed by law'. The ISC expressed concern on this issue, and recommended public disclosure in relation to s8(4) certificates at Chapter 5 of the ISC Report.

56. The s8(4) regime also allows for internal arrangements to be made by the Respondents under ss15 and 16. The IPT placed significant weight on those secret arrangements in finding that the s8(4) regime was 'in accordance with the law'. Those arrangements do not have the necessary quality of 'law' in that:
    (1) They are not contained in either primary legislation (e.g. Part 1 of RIPA) or secondary legislation (e.g. the Code made under s71 RIPA);
    (2) They are not otherwise seen or made available to Members of both Houses of Parliament (see *Silver and others v United Kingdom* 25 March 1983, Series A No 61), §26 and 89; and *Khan v United Kingdom* (35394/97, ECHR 2000-V) at §§16 and 27);
    (3) The arrangements can be changed as a result of secret administrative decision without any legislative oversight whatsoever; and
    (4) They have never been made publicly accessible.

57. The ISC Report explained further problems with the s8(4) regime that were not revealed by the UK Government at the IPT hearing: that there appears to be a single certificate in place for the whole s8(4) bulk collection regime; it is so generic in nature that there appears to be little justification for it being secret; and it is 'unnecessarily ambiguous and could be misinterpreted' (see ISC Report at §§95 – 104). The report also revealed that there are only 18 s8(4) warrants in existence, which together cover an unspecified number of communications service providers (the number of service providers affected was redacted in the report) (§99).

58. The IPT accepted that the arrangements "*were not … made known in their detail to the public and to that extent are not accessible and … not even a summary of what they contain was disclosed*" (§44). It nonetheless concluded that it was entitled to have regard to those "*below the waterline*" arrangements, particularly given that the Code itself refers to "*a number of arrangements not contained in the Code*" and there is a "*system of oversight, which the ECtHR has approved, which ensures that such arrangements are kept under constant review*" (§129).

[9] See for example §§5.3, 5.5, 5.7-8, 5.10-13, 6.1-3, 6.5 and 6.8.

59. This IPT erred in its approach in three ways. First, although the Court approved the system of oversight in *Kennedy,* that was only in relation to targeted warrants under s8(1) and the Court itself had been at pains to stress that it was not addressing the adequacy of oversight in relation to untargeted interceptions under s8(4) (see especially §160). Second, there is nothing in the Court's judgment to indicate that the Code's own references to arrangements meant that such arrangements could be relevant to the Court's assessment of accessibility, particularly where they themselves were not publicly accessible. Third, the "*the system of oversight*" referred to by the IPT does not provide proper legal protection against arbitrary interference by public authorities (see *Gillan v United Kingdom* 4158/05, 12 Jan 2010, §§82 and 86). In any event, oversight does not itself contribute to the accessibility of the arrangements under ss15 and 16. (for the need for relevant procedures to be in a form which is open to public scrutiny and knowledge, see *Liberty v UK*, at §67).

60. The IPT's conclusion that the s8(4) arrangements are "*sufficiently signposted in the statute, in the Code, in the Commissioner's Reports and as now recorded in this judgment*" (§140) therefore proceeds upon a false premise. The mere fact that the Code and the Commissioner refer to the ss15 and 16 arrangements does not provide members of the public with any indication of what those arrangements are. Further and more fundamentally, "signposting" is not sufficient to render the arrangements 'in accordance with law'. A "signpost" is something that points elsewhere. What Articles 8 and 10 require is that the relevant arrangements are understood by those subject to them, not that those persons are given indications that the understanding is located somewhere else that is inaccessible to the public. For these reasons, the internal arrangements under ss15 and 16 RIPA not having being made publicly accessible and in a form satisfying the quality of 'law' requirement, the scope and manner of the intelligence services' discretion to undertake bulk interception under s8(4) warrants is not set out with sufficient clarity in the law itself.

B. Violations of Articles 8 and 10 – Bulk interception under s8(4) RIPA, pursuant to TEMPORA is unnecessary and disproportionate.

61. Interception under a s8(4) warrant:
    (1) does not involve any requirement to specify or target the communications of some particular person or premises, at the point of interception as well as at the point at which the intercepted material is selected to be looked at, listened to or read;
    (2) makes no distinction between communications which are 'internal' and those which are 'external';
    (3) "*may and can result … in the interception of all communications between the United Kingdom and an identified city or country*". In fact, there is no upper limit on the number of communications that may be intercepted under a s8(4) warrant, "*provided that the requirements of s8(4) and (5) are satisfied*" [10];
    (4) does not require any prior judicial authorisation and involves only very limited ex post facto oversight by the Interception of Communications Commissioner, the IPT, and the Intelligence and Security Committee;
    (5) permits s8(4) warrants to be certified in broad, generic terms (see above and Chapter 5 of ISC Report)

62. The interception regime under s8(4) cannot be characterised as either "necessary in a democratic society" or proportionate under Articles 8(2) and 10(2) ECHR, for the following two reasons.

63. First, the lack of any requirement under RIPA for a s8(4) warrant to be directed at either a

[10] *British Irish Rights Watch* case (IPT/01/77, 9 December 2004, §9)

particular person or premises is disproportionate. In *Gillan and Quinton v United Kingdom* (4158/05, 12 January 2010), this Court expressed particular concern over an intrusive power that did not require any "reasonable suspicion" (in that case the power of random stop and search individuals under s44 of the Terrorism Act 2000). Such broad discretion gave rise to a "*clear risk of arbitrariness*" (ibid, §85) and was difficult to challenge by way of judicial review or an action in damages.

64. The same reasoning applies in relation to communications and communications data both at the point of interception, and separately in relation to inspection, retention and storage on a database. For the reasons outlined above, in the context of s16 of RIPA, there are no adequate safeguards in place to justify those interferences with fundamental rights.

65. In *S and Marper v United Kingdom* ([GC] 30562/04, 4 December 2008) the UK government submitted that the retention of DNA samples from people who had not been charged or convicted of a criminal offence was of "inestimable value" and produced "enormous" benefits in the fight against crime and terrorism (§92). The Grand Chamber nonetheless held that the retention was a "*disproportionate interference*" with those individuals' private lives (§135). Central to the reasoning was the absence of any assessment of suspicion by the authorities against the individuals that was sufficient to justify the retention of their DNA data. The same reasoning applies in this case.

66. There is a significant interference with individual's rights caused by a regime that permits the retention of immense quantities of their communications data, not based on reasonable suspicion. In *Digital Rights Ireland v Minister for Communications and others*, 8 April 2014, C-293/12 the Grand Chamber of the CJEU concluded that the 2006 Data Retention Directive (Directive 2006/24/EC of the Parliament and the Council of 15 March 2006) which required communications service providers to retain customer data for up to two years for the purpose 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. The Chamber first of all drew an analogy with *Marper* (§47), stressing the limited nature of the EU Legislature's discretion given "*the important role played by the protection of personal data in the light of the fundamental right to respect for private life*" (§48 and also §§54-55). It further observed that the scope of the data retention *"entails an interference with the fundamental rights of practically the entire European population* (§56). The Court went on to note the Directive was flawed for not requiring any relationship between the data whose retention was provided for and a threat to public security (see §59). The Grand Chamber concluded that the Directive amounted to a "*wide-ranging and particularly serious interference*" with the rights to privacy and data protection "*without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary*".

67. In light of these judgments, GCHQ's interception each day of millions of emails, Google searches, Facebook messages and other data concerning internet use is not a proportionate interference with the right to privacy and to freedom of expression of the vast number of individuals affected.

68. Second, the lack of prior judicial authorisation of warrants under the s8(4) regime breaches the requirement of 'necessity' under Articles 8(2) and 10(2). The Applicants note the repeated observations of the Court that, "*it is in principle desirable to entrust supervisory control to a judge*" (*Klass and Others v. Germany*, at §56). In *Digital Rights Ireland* the CJEU noted that, "*Above all, access …to the data is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued*" (§62). Moreover, prior

judicial authorisation is required before the state may seize and retain journalistic source material (*Sanoma Uitgevers BV v The Netherlands* [GC] 38224/03, 14 Sep 2010, §92). Prior authorization by the Secretary of State falls far short of any necessary requirement of independence.

69. The Interception of Communications Commissioner is only in a position to provide very limited *ex post facto* oversight of specific warrants and does not provide a sufficient safeguard against abuse:
    (1) The Commissioner's position is part-time[11], and he examines only a sample of interception warrants made annually.
    (2) In his 2013 report, the Commissioner referred to having inspected at least some s8(4) warrants, although he does not state how many. It is also unclear whether he had the opportunity to examine any of the material that had been selected by the Respondents to be "read, looked at or listened to" under any warrant or certificate; and, if so, how much of that material he was able to examine in order to assess proportionality;
    (3) The UK Parliament Home Affairs Select Committee has expressed "*serious doubts*" on both of the above issues relating to the Interception of Communications Commissioner.[12]

C. Violations of Articles 8 and 10 - Receipt of intercepted communications under PRISM and UPSTREAM not in accordance with the law

70. The IPT found that the regime for the UK Government to receive intercepted communications and communications data from the US Government was (by the time it delivered its judgment) 'in accordance with the law / prescribed by law', save in one respect. That one point, set out in its second judgment, related to the fact that important aspects of that regime, setting out the internal arrangements of that regime, had been unnecessarily secret prior to disclosure by the Respondents, in a note, following the closed hearing before the IPT. It therefore declared that "*the Prism and/or Upstream arrangements contravened Articles 8 or 10 ECHR, but now comply*" (§32 of second judgment).

71. The IPT's approach to the intelligence sharing regime was based on a fundamental error. It found that the *Weber* criteria applied in a significantly attenuated form when raw intercepted communications and data was solicited/received by the UK Government. That approach mischaracterised or misunderstood the nature of modern communication and the close collaboration between the UK and US intelligence services. For example, a communication between two individuals in London can be intercepted by the US and then, because the NSA and GCHQ collaborate so closely, solicited by GCHQ or provided in bulk to it. That is indistinguishable in terms of interference with privacy and freedom of expression to GCHQ intercepting the material directly and requires equal levels of protection to satisfy the in accordance with law requirements.

72. The intelligence sharing of communications and communications data intercepted by PRISM and UPSTREAM are not 'in accordance with the law' for the following reasons:
    (1) The relevant provisions of the Security Service Act 1989 and the Intelligence Services Act 1994 governing the receipt of information are exceedingly broad and give no indication whatsoever as to the relevant arrangements that the respective heads of each service must put in place regarding the receipt of intercepted material and communications data from foreign intelligence services;
    (2) There is no Code of Practice or other secondary legislation that provides any further

[11] See House of Commons Home Affairs Committee, Counter-terrorism, HC 231, 9 May 2014, §165.
[12] The Committee stated that: "The fact that less than 10% of warrants which allow intrusion in to the private lives of individuals are examined is concerning—we believe this figure ought to be at least 50%, if not higher."

indication as to how those powers may be exercised; In particular, the statutory framework gives no indication of any kind as to:

(a) the situations in which the intelligence services can lawfully request foreign intelligence services to target and intercept the private communications of (1) persons who are or may be within the British Islands; or (2) persons outside the British Islands.

(b) the situations in which the intelligence services can request and receive access to communications data and the content of communications that have been obtained by foreign intelligence agencies; and

(c) the procedures to be followed by the intelligence services in relation to the storage, inspection, use and dissemination of intercepted communications data and communications that have been received from foreign intelligence agencies (whether solicited or unsolicited).

(3) Contrary to the finding of the IPT, the note disclosed following the closed hearing did not cure these deficiencies.

(a) The note is not law. There is no indication as to its status, binding nature or how and by whom it may be amended.

(b) The note introduced new and undefined concepts of "analysed" and "unanalysed" communications. These concepts are not derived from any statutory definition, are not explained and are inherently unclear. Moreover, there is no published regime governing "analysed" material.

(c) The note does not cover "communications data" which is not "associated" with intercepted communications. There is no published regime of any kind governing the soliciting, obtaining or receipt of such data.

73. The ISC expressed concern over the lack of a clearer statutory framework for intelligence sharing at Chapter 10 of the ISC Report.

D – Specific issues relating to the Applicants' Article 10 rights

74. For the reasons set out above in relation to the issue of "in accordance with the law" under Article 8, the legal framework governing the interception of communications and communications data under s8(4) warrants, and the receipt of intercepted material and communications data from foreign intelligence agencies, fails to meet the "prescribed by law" requirement of Article 10 ECHR.

<u>*Confidential material belonging to NGOs*</u>

75. The protection afforded by Article 10 is of critical importance to the Applicants. Where an NGO is involved in matters of public interest it is exercising a role as public watchdog of similar importance to that of the press and warrant similar protections to those afforded to the press (see *Gusova v Bulgaria* 6987/07, 17 Feb 2015, §38 and the cases there cited).

76. At the outset of proceedings, the Applicants each alleged that the interception of their communications by the intelligence services violated not only their right to privacy under Article 8 but also their right to freedom of expression under Article 10. The intelligence services maintained, however, that "*the [Applicants] cannot … claim to be victims of any Art. 10 interferences. Neither are journalists or news organisations*".[13] Until July 2014 the intelligence services' pleaded position was that NGOs were not entitled to the protection of Article 10 ECHR. Despite repeated requests for disclosure of any relevant closed material relied upon by the intelligence services, the IPT refused to direct the intelligence services to disclose their internal guidance (First Judgment, §§135-137).

[13] §35 of the intelligence services' response to Liberty's claim, 15 November 2013

77. The published procedures under s15 and the Code therefore give no indication as to whether the intelligence services' internal guidance has properly addressed the position of NGOs as being entitled to the same protection as journalists and media organisations in respect of their sources. Indeed, the pleaded position of the intelligence services over a period of more than six months was that NGOs were simply not entitled to the protection of Article 10 in this fundamental respect. The IPT judgments give no indication that there is any relevant internal guidance that is in conformity with Article 10 on this particular issue.

78. In circumstances in which the Applicants are in daily communication with sources, some of whom risk their lives by so communicating, the failure of the relevant legal framework to provide sufficient indication as to how their confidential material is liable to be treated by the intelligence services constitutes an additional respect in which the s8(4) regime is not in accordance with the law.

Judicial authorisation

79. This Court's case law establishes that obtaining confidential communications to or from sources without any form of prior judicial authorisation is incompatible with Article 10, even if the intercepted material is never actually inspected (*Sanoma Uitgevers BV v The Netherlands* 38224/03, 14 Sep 2010 [GC]). This is particularly important where the measure is capable of interfering with "the right to protection of sources" which "must be attended with legal safeguards commensurate with the importance of the principle at stake" (Ibid, §88). Under Part I of RIPA there is no requirement of prior judicial authorisation before the security and intelligence agencies may intercept any communications under s8(1) or 8(4) warrants. The position is markedly at odds with the procedure for obtaining journalistic material under the Police and Criminal Evidence Act 1984, which requires judicial authorisation in every case.

80. Indeed, the Interception of Communications Commissioner has recently recognised the deficiencies of the legal framework in this area, and the importance of judicial authorisation, when reviewing the obtaining of communications data under Chapter 2 of Part 1 of RIPA. (See Interception of Communications Commissioner report of 4 February 2015, at para 8.7 and 8.9.1).

81. The absence of any requirement for judicial pre-authorisation (as well as automatic *post facto* judicial scrutiny) involves a clear violation of the Applicants' Article 10 rights.

E – Violation of Article 14

82. The s8(4) framework governing bulk interception is indirectly discriminatory on grounds of nationality and national origin because s16 RIPA grants additional safeguards to people known to be in the British islands but denies them to people abroad. A British person is more likely to be present in the British Islands and vice versa. The nature of the discrimination is serious. If a large quantity of data is collected under s8(4), it cannot be searched using a term referable to a person known to be in the UK without a certificate issued by the Secretary of State. However, where a person is not known to be in the British Islands, this requirement does not apply.

83. A person outside the United Kingdom is entitled to the same protection for the privacy of his or her communications as a person inside the United Kingdom. The majority of Applicants, being based outside the United Kingdom, or having a large number of staff working outside the United Kingdom, are disproportionately likely to have their private communications intercepted and communications data intercepted and accessed as a result of the lack of safeguards in respect of warrants issued under s8(4) when compared to those afforded to UK persons present in the UK in respect of communications wholly internal to the United Kingdom. No proper justification for this

differential treatment has been advanced by the intelligence services, save that "*it is harder to investigate terrorism and crime abroad*" – an explanation that the IPT accepted.[14]

84. Any distinction between the domestic and external interception regimes operated by the intelligence services has been substantially eroded by the rise of internet-based communications. Indeed, the available evidence concerning TEMPORA shows that GCHQ is able to exercise an identical degree of control over *all* communications passing through the fibre-optic cables that they intercept, whether the email in question is between Birmingham and London, on the one hand, or between Toronto and Cairo on the other hand.

85. For the above reasons, the s8(4) regime is also discriminatory, contrary to the requirements of Article 14 taken together with Articles 8 and 10.

F - Violation of Article 6

86. The proceedings before the IPT breached the Applicants' right to a fair hearing in a number of respects:
    (1) The IPT declined to direct the intelligence services to disclose any of their internal guidance concerning the treatment of confidential material of non-governmental organisations under Article 10, notwithstanding that:
        (a) the intelligence services had maintained for almost a year that Article 10 did not apply to non-governmental organisations;
        (b) the IPT had directed disclosure of similar material in *Belhaj* and partial disclosure in relation to PRISM and UPSTREAM, without apparent prejudice to national security; and
        (c) the Applicants had requested disclosure of such material from the outset..
    (2) The IPT took the position that it had no power in any event to require the intelligence services to disclose such evidence.
    (3) The IPT wrongly held a closed hearing on whether the relevant framework governing the intelligence services' bulk interception and receipt of material of foreign intelligence agencies was in accordance with law. The IPT proceeded in secret in deference to the government's policy of "neither confirming nor denying" the existence of particular interception programmes (the "NCND policy").
    (4) The IPT refused to hear and decide one of the preliminary issues that had been agreed between the parties (and with the express approval of the IPT), namely whether the application of the NCND policy was justified on the facts of the present cases.
    (5) In finding that the existing interception regime was in accordance with the law, the IPT placed significant reliance on secret "arrangements below the waterline" which were not disclosed to the Applicants and on which the Respondents were permitted to make submissions during closed proceedings.
    (6) The IPT took no steps to ensure that the Applicants were effectively represented in the closed proceedings.

For Liberty, the American Civil Liberties Union, the Canadian Civil Liberties Association, the Egyptian Initiative for Personal Rights, the Hungarian Civil Liberties Union, the Irish Council for Civil Liberties and the Legal Resources Centre: **James Welch, Matthew Ryder QC, Eric Metcalfe, Edward Craven**

For Privacy International and Bytes for All: **Mark Scott, Ben Jaffey, Dan Squires**

For Amnesty International: **Nick Williams, Hugh Tomlinson QC, Nick Armstrong, Tamara Jaber**

[14] First IPT judgment, §§147(ii) and 148.