IN THE INVESTIGATORY POWERS TRIBUNAL **Case No. IPT/13/92/CH**

B E T W E E N:

PRIVACY INTERNATIONAL

Claimant

and

(1) SECRETARY OF STATE FOR THE FOREIGN AND COMMONWEALTH OFFICE

(2) THE SECRETARY OF STATE FOR THE HOME OFFICE

(3) THE SECRET INTELLIGENCE SERVICE

(4) THE SECURITY SERVICE

(5) GOVERNMENT COMMUNICATION HEADQUARTERS

(6) THE ATTORNEY GENERAL

Respondents

REPLY

Introduction

1. This is Privacy International's Reply to the Open Defence. It sets out proposals for the future case management of the Claim. This Reply will be supplemented by a skeleton argument in due course. It does not repeat points already made in the Grounds of Claim, and where a point is not expressly admitted, it should be treated as being in dispute.

2. The Respondents propose that a number of *"pure issues of law"* be determined at a "*Legal Issues Hearing*". The Claimant agrees that it is sensible to identify the issues that are in dispute between the parties and which the Tribunal will need to resolve in order to dispose of the claim. The Claimant does not, however, agree that the issues can or should be determined as *"pure"* questions of law. The claim raises questions of fact and law and they should be determined on the basis of the evidence submitted by the parties, and as far as possible, in open hearings. The

Claimant recognises that it may be necessary for some of the evidence to be heard in "*closed*". There is, however, no reason why that cannot occur alongside open hearings dealing with law and evidence as occurs, for example, in SIAC or in Control Order/TPIM cases, or civil claims pursuant to the Justice and Security Act 2013. Privacy International has agreed suggested issues with Liberty, and these are provided by Liberty under separate cover.

Ground 1

1. In Ground 1 of their claim, the Claimant seeks to challenge the absence of a legal regime containing sufficient safeguards to satisfy ECHR Art 8 and/or 10 which governs:

    (i) the circumstances in which UK authorities can access, obtain, store and process phone calls, emails, web-browsing and other communications of individuals located in the UK or data about those communications which have been intercepted by US authorities (including, but not limited to, where the interception has occurred at the behest of UK authorities), and

    (ii) the circumstances in which the UK authorities can access, obtain, store and process the contents of communications or data about those communications of individuals located in the UK which have been obtained by US authorities from telecommunication or internet companies (including, but not limited to, where the information has been obtained at the behest of UK authorities).

    The Claimant also challenges the lack of proportionality in the obtaining, storing, accessing and processing of such material.

2. As set out in the Claimant's grounds, evidence revealed in the press about the external intelligence-gathering programme operated by the US National Security Agency ("*NSA*") indicates that:

    (i) The NSA routinely intercepts the communications of non-US citizens located outside the USA including while the communications pass

through fibre-optic cables in the USA.

(ii) Given the operation of the global communication system, the above-described interception can include phone-calls and emails between two individuals both of whom are located outside the US (and who may both be in a third country such as the UK) but which happen to be routed through the US. Potentially vast amount of information can be intercepted in this way.

(iii) The NSA also obtains communications stored on the servers of electronic communication providers such as Yahoo, Google and Facebook. This is known as the Prism Program.

(iv) GCHQ and the NSA operate closely together. Reports indicate that GCHQ captures content flowing through undersea cables that land in the UK and shares the information with the US (see Ground 2 of the Claimant's case). The material intercepted by GCHQ is examined by a team consisting of 250 NSA analysts and 300 GCHQ analysts . It is essentially a joint project. The Claimant stated in their Grounds that it was assumed that, similarly, where the NSA intercepts communications and data about communications, both GCHQ and NSA staff have access to them and analyse them jointly. It is clear that there is "task-sharing" between the US and the UK. According to reports, the level of co-operation under the countries signals intelligence agreement (UKUSA agreement) is so complete that "the national product is often indistinguishable." [1] This has resulted in former intelligence officials explaining that the close-knit cooperation that exists under the UKUSA agreement means "that SIGINT customers in both capitals seldom know which country generated either the access or the product itself."[2] Another former British spy has said that "[c]ooperation between the two countries, particularly, in SIGINT, is so close that it becomes very

[1] Robert Aldrich (2006) paper 'Transatlantic Intelligence and security co-operation', available at: http://www2.warwick.ac.uk/fac/soc/pais/people/aldrich/publications/inta80_4_08_aldrich.pdfIntelligence'

[2] S. Lander, 'International intelligence cooperation: an inside perspective', in Cambridge Review of International Affairs, 2007, vol. 17, n°3, p.487.

difficult to know who is doing what [...] it's just organizational mess."[3] Indeed, leaked NSA documents reveal the existence of shared and integrated databases, such as "GCHQ-accessible 5-eyes [redacted] databases."[4]

(v) It is therefore clear that GCHQ has obtained information from the US Government that the US Government has obtained through the Prism Program.

(vi) It is also clear that GCHQ staff have been given, or have direct access to, material intercepted directly by the NSA from fibre optic cables and other sources.

3. The Respondents admit (iii) and (v) of the above, and neither confirms nor denies the remainder of the allegations (Defence [28] and [31]). The Respondents also accept that the Claimant may challenge the compatibility of the regime governing interception and sharing of information "*on the basis their communications / communication data might in principle have been obtained by the US Government and might in principle have been obtained by the Intelligence Services from the US Government*" (Defence [34]).

4. Given that the Respondents have provided no further disclosure or admission, it is assumed that the Respondents position is that the Claimant is able to challenge the legal regime on the further basis: (i) that their private communications might have been intercepted by US authorities or obtained from telecommunication or internet companies, and (ii) that given the relationship between the NSA and GCHQ, staff at GCHQ, in practice, have access to communications content and data intercepted in bulk by the NSA, including communications of the Claimant.

5. The Respondents also admit at Defence [57] that they are not required to seek

---

[3] Britain's GCHQ 'the brains,' America's NSA 'the money' behind spy alliance, Japan Times, 18th November, 2013, accessible at: http://www.japantimes.co.jp/news/2013/11/18/world/britains-gchq-the-brains-americas-nsa-the-money-behind-spy-alliance/#.UozmbMvTnqB

[4] US and UK struck secret deal to allow NSA to 'unmask' Britons' personal data, 20 August 2013, available at: http://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data#

authorisation under RIPA in order to obtain communications content or data from foreign intelligence agencies. Other than generally applicable legal provisions such as the Data Protection Act 1998 and Human Rights Act 1998 (Defence [48]-[54]), the only apparent legal limitation on the Respondents ability to access, store and process such material is that UK authorities must not, pursuant to *Padfield v MAFF* [1968] AC 997, 1030, act so as to "*deliberately circumvent*" RIPA (Defence [58]) (emphasis added).

6. For the reasons set out in the Claimant's Grounds that does not come close to satisfying the requirement that accessing, processing or storing their private communications is "*in accordance with the law*" for the purposes of ECHR Arts 8 and 10. It does not provide sufficient protection against abuse. Indeed, it does not impose any practical restriction on the processing or use of data. Nor does it indicate, with any degree of certainty, the circumstances in which the private communications of UK residents may be intercepted by US authorities, or obtained by them from electronic communication providers, and then shared with, or otherwise accessed by, UK authorities. Nor does it prescribe the manner in which such material will be stored, processed or shared or when it will be destroyed.

7. The Respondents suggest that the claim can be determined by resolving pure issues of law. As indicated above, the Claimant does not oppose an attempt to formulate agreed issues in dispute, but there is no reason why the issues should be determined as "*issues of pure law*" as the Respondents propose (Defence [77]). The Claimant wishes to have the opportunity to submit factual material in support of its claim and to examine witnesses that the Respondents seek to rely upon.

8. The Claimant also does not agree with the proposed issues formulated by the Respondents which assume, in the Respondents' favour, key legal disputes between the parties.

9. The Respondents propose the following issues at Defence [77]:

> *Issue (i) does the Intelligence Sharing regime satisfy the requirement in Art 8(2) that any interference be 'in accordance with the law'.*

Issue (ii) does the Intelligence Sharing regime ensure that the obtaining, retention and disclosure of information by the Intelligence Services pursue one or more legitimate aims for the purposes of Art 8(2).

10. That assumes two disputed questions in the Respondent's favour.

11. Firstly, it assumes that it is only Art 8 in dispute and not Art 10 (Defence [35]).

12. Secondly, it assumes that the same legal principles apply to all forms of "*intelligence sharing*". It assumes that the legal principles applicable to the interception and sharing of private communication material must be the same as that applicable, for example, to the obtaining and sharing of information from informants or the product of surveillance. The Respondents' principal submission in response to Ground 1 is that because, on their assertion, the same legal principles apply to all forms of "*intelligence sharing*", and because it cannot be correct that the principles in the "*Strasbourg intercept cases*" apply to <u>every</u> form of intelligence sharing, the principles relied on by the Claimant cannot be applicable to the instant case (Defence [88]-[90]).

13. The Claimant submits that that is not a good argument and that it proceeds on a false premise. The Strasbourg jurisprudence makes clear that intercepting and storing of communications or metadata is an intrusive invasion of privacy and requires a commensurate and exacting legal framework if it is to be "*in accordance with the law*". The ECtHR does not assume that the same principles apply to all intelligence gathering irrespective of the nature of the material in question and irrespective of the manner in which it was obtained. Similarly, where private communications are intercepted, or obtained from electronic communication providers, by one intelligence service, and it provides access to them for another intelligence service which then obtains, processes and stores them, that too is a serious interference with privacy. There is no reason why the regime required to ensure that such interference occurs in a manner that is "*in accordance with the law*" will be the same as for other forms of intelligence sharing.

14. The Respondents are, of course, entitled to argue the contrary, but it does not

assist in resolving the issues in dispute to assume in their favour that all "*intelligence sharing*" is subject to the same legal principles.

Ground 2

15. The Claimant complains about the intelligence operation known as TEMPORA reported in the *Guardian* newspaper on 21 June 2013. Under this operation, GCHQ has intercepted more than 200 fibre optic cables landing in the United Kingdom. Extracted data is stored for at least three days for content, and 30 days for metadata, and is automatically analysed and searched. Intercepted traffic includes internet usage and telephone calls. It is reported that GCHQ has set over 40,000 search terms and the US National Security Agency has set over 31,000 search terms which are used to determine which data should be extracted. GCHQ is also reported to collect more metadata than the NSA. Under this programme, there is therefore bulk interception, storage and search of internet traffic of all users of intercepted fibre optic cables.

NCND

16. The Respondents' reliance on the 'neither confirm nor deny' ("NCND") principle is misplaced. In the circumstances, NCND does not apply, and the open Defence of the Respondents is inadequate. Without a proper open statement of the Respondents' case, which places as much into open as possible, a fair trial will not be possible:

    a. NCND is a justifiable principle. It has an important role in some litigation raising national security issues. For example, when an individual (such as the applicant in *Kennedy v UK*) asks if he is being spied upon, a NCND response will ordinarily be justified, to prevent an inference that the true answer is 'yes' in any case where the answer is not 'no'.

    b. However, the NCND principle is no more than a policy. It is not a rule of law. It has a number of relevant exceptions, and is only to be applied by the Tribunal in an appropriate case. The judicial function of the Tribunal requires it to hold a fair hearing, which includes the rejection of an unjustified attempt to rely on the NCND principle.

c. The proper approach to NCND was considered by the National Security Panel of the Information Tribunal in *Baker v SSHD* (2001) (Sir Anthony Evans, Michael Beloff QC and James Goudie QC):

> "33. There are some well-established circumstances in which the [Security] Service does acknowledge that information has been collected and is still held. Sometimes, the information may be released. These circumstances, as Mr Burnett QC [for the SSHD] put it in his oral submissions to us, can be grouped together as cases where the person concerned already knows "conclusively" that there is information held upon him. Another situation which can arise is where the Service itself decides that the acknowledgement should be made, and even that the information should be published, because that is seen as assisting the proper performance of its statutory functions, or as otherwise being in the public interest. This too becomes a case of "official confirmation" that the information is held. <u>These and similar cases, Mr Burnett QC submits, are "well recognised exceptions" to the policy of answering requests with some variant of the formula NCND. They are "dictated by common sense".</u>
>
> 34. <u>This group of cases (which is not closed)</u> includes –
>
> (a) Members or former members of agencies who know that data are held.
> (b) Individuals who are subject to removal from the United Kingdom on grounds of national security who have become conclusively aware of Security Service interest in them.
> (c) Those involved in criminal proceedings who have conclusively become aware of Security Service interest in them.
> (d) Others in whom Security Service interest has been publicly confirmed in [Court or other] proceedings."

d. The other exceptions include where material is in the public domain and its authenticity cannot seriously be disputed. In *R (Bancoult) v SSFCA* [2013] Env LR 2 at [28] the Divisional Court (Richards LJ and Mitting J) considered the admissibility of a 'Wikileaks' cable from the US embassy in London. The Court was asked to rule on whether the cable could be relied upon in cross-examination and put to the Secretary of State's witnesses as being a genuine document. The Defendant sought to rely on NCND for the same reasons as the Respondents do so here. As the Divisional Court put it at [26]:

> "Mr Kovats was properly handicapped in dealing with the issue because of the longstanding NCND policy of the British Government. The reason for the policy is explained in the witness statement of Mr Martin Sterling, a senior policy adviser in the

Cabinet Office: it would be prejudicial to the effective administration of public affairs to do so. Confirming the accuracy of information within a leaked document would compound any prejudice already caused and would reward persons involved in the leaking. Even a denial of accuracy would, by inference, lead to an unwarranted assumption that an undenied leak was accurate. Hence, subject to exceptional circumstances, the policy must apply universally to be effective."

e. The Court rejected the NCND argument (although it held that the document was inadmissible on other grounds) at [28]:

> "We make clear that if the only objection to the admission in evidence of the document were the NCND policy, we would have permitted it to be admitted, for the following reasons, which lay behind our initial ruling on the point. First, it is far from clear that the documents of other governments are covered by the policy. All that Mr Sterling states is that he "cannot see any reason for the NCND principle not applying in these circumstances". Secondly, as Mr Sterling accepts, the policy admits of exceptions. Thirdly, it does not, as such, bind the court. Fourthly, in the circumstances with which we have to deal, the interests of justice would override the policy: the document has been in the public domain for many months, even if it got there as a result of an unlawful act. If it were necessary for us to take it into account evidentially to determine the true purpose of declaring the MPA , we would not regard the NCND policy as a sufficient reason for refusing to do so. To refuse to do so could, in principle, permit Her Majesty's Government (HM Government) to conceal an improper and unlawful motive for an executive act which is claimed to have had an adverse impact upon the rights of a significant number of individuals of Chagossian origin or descent."

f. There are therefore many circumstances in which NCND policy is not lawful or appropriate. The Divisional Court has rejected the claim that the NCND policy can properly be applied to a 'Wikileaks' cable. The same applies, *a fortiori*, to materials obtained by Edward Snowden and now published worldwide by various media outlets:

   i. The Respondents have, as a result of Mr Snowden's disclosures, officially confirmed the existence of PRISM and the UK use of PRISM.

   ii. Given that:

      1. Edward Snowden had very extensive access to secret material;

2. He took that material and gave it to a small number of journalists, who published it in the Guardian, the New York Times the Washington Post and other outlets;
3. Articles by the same journalists using the same materials have disclosed TEMPORA;
4. Both PRISM and TEMPORA are referred to in the same documents and Powerpoint presentations;

to officially admit one programme but to NCND another is untenable.

iii. The documents obtained by those journalists are genuine and derive from the records of GCHQ and the US NSA. Indeed, this has been confirmed by the evidence given on behalf of the Home Secretary in the claim brought by David Miranda (*R (Miranda) v SSHD)* which confirmed that the Guardian held sensitive information derived from GCHQ's records, and that Mr Miranda was stopped under Schedule 7 of the Terrorism Act 2000 because he was carrying such information (witness statement of Oliver Robbins, 27 August 2013).

iv. Similarly, the Secretary to the D-Notice Committee (Air Vice Marshal Vallance) reported to the 7 November 2013 meeting "*the dominant aspect of this reporting period was the publication by The Guardian, and latterly by The Independent, of information from the classified documents stolen by the NSA fugitive Edward Snowden*". The Secretary referred to the "*highly sensitive information about GCHQ*" that had been published, and the Guardian's agreement "*not to publish certain highly sensitive details*". During this period, the Intelligence Services had "*continued to ask for more advisories to be sent out*" but the Secretary was skeptical about this. The Secretary then referred again to "*the publication ... of selected parts of the highly sensitive intelligence information stolen by Edward Snowden*". There is no suggestion in these public minutes that it was sensible or necessary to maintain a 'NCND' response. Indeed, the minutes are entirely inconsistent with 'NCND' because

they do not even attempt to maintain the stance that the documents are anything other than accurate and genuine. To the contrary, the concern was understandably to prevent the publication of certain highly sensitive operational details.

v. Finally, the Chairman of the Intelligence and Security Committee wrote in The Guardian on 20 September 2013:

> "On Tempora, it has been well known that the fibre optic cables that carry a significant proportion of the world's communications pass close to the British coastline and could provide intelligence opportunities. The reality is that the British public are well aware that its intelligence agencies have neither the time nor the remotest interest in the emails or telephone conversations of well over 99% of the population who are neither potential terrorists nor serious criminals. Modern computer technologies do permit the separation of those that are of interest from the vast majority that are not."

vi. Reliance on NCND in these circumstances is a misuse of the NCND policy and is not lawful.

g. The suggestion that *Kennedy* [IPT 01/62] prevents the Tribunal rejecting NCND, holding a factual hearing or giving reasons for its rulings is incorrect. Where appropriate, the Tribunal has held factual hearings in public and given reasoned, public, judgments. It should do so in this case. See, for example *BA, RA and CT v CC of Cleveland Police* (IPT/11/129/CH and others) and *Paton v Poole Borough Council*. It is for the Tribunal to determine whether information (which includes a claim to rely on the NCND principle) would harm national security if disclosed, not the Respondents. As with other courts and Tribunals, any claim to rely on the NCND policy should be subjected to proper examination and, where appropriate, rejected.

Open Defence – admissions and omissions

17. The Open Defence makes significant admissions about the Respondents' interpretation of RIPA:

a. RIPA permits, through the use of certificated warrants under section 8(4), dragnet interception of communications in bulk.
b. Where it is necessary to intercept internal communications in order to also collect the external communications, that is permissible (s. 5(6)). For example, if a fibre optic cable transmits internal and external communications, all the data can be collected.
c. It would, in principle, be possible under RIPA to issue a warrant covering all external communications, made by whatever means, anywhere in the world. Such a certificated warrant or warrants could be renewed indefinitely.

18. The Respondents accept that the interception of a communication (even without it being electronically scanned and analysed) is an Article 8 interference that requires justification (footnote 28). However, the other key issues before the Tribunal are not dealt with at all:

a. No explanation is given as to how selectors used for processing bulk intercepted data are set or used. In particular, there is no explanation as to:

i. How selectors are identified and approved, removed and checked to ensure that they are effective, appropriate, necessary and proportionate.
ii. What oversight there is over the number and scope of selectors.
iii. Whether other countries (including other members of the '5 Eyes' group) are permitted to choose selectors.
iv. The extent to which the selectors used are effective in selecting only external communications, and communications of genuine national security interest.

Prescribed by law

19. The argument advanced (§194) by the Respondents is that every person is, in principle, liable to have all of their communications intercepted, at all times, providing they are transmitted using a technique that includes some external communications. Almost all use of the internet would fall within this category. No meaningful limiting factors are identified. All types of communication, transmitted by any means, and whether or not the communication is with an external party, may be intercepted, and then subjected to automated analysis. For the reasons given in the Grounds, such bulk interception is not prescribed by law.

20. Some limitations are imposed under section 15 and 16 of RIPA on reading or listening to internal communications. However, no controls are imposed over the use of communications data collected under section 8(4) certificated warrants. The bulk information can be collected and processed to obtain communications data (about who contacts who, where they are, when they communicate, how they communicate and what sites they look at on the internet).

21. Under RIPA, communications data includes the following categories of information

Data associated with emails:

- Sender's name, email, and IP address
- Recipient's name and email address
- Date, time, and time zone in which email is sent and received

Data associated with mobile phones:

- Phone number of every caller
- Serial numbers of phones involved
- Time of call
- Duration of call
- Cell site location

Data associated with web browsers:

- Activity including pages the user visits and when visited
- User IP address, internet service provider, device hardware details, operating system, and browser version

22. That information can be used without restriction. Put together, communications data can reveal as much as content, including an individual's identity, relationships, location and activity, as well as a vast array of diverse information about her web browsing activities, medical conditions, political and religious viewpoints and/or affiliations, interactions and interests. For instance, knowing a person called just a single phone number, if that number has a specific purpose such as hotlines addressing suicide prevention, rape crisis, or alcohol abuse, can reveal extremely sensitive information. Patterns of communications can also be revelatory. Phone and email records may indicate the hours a person keeps, or his religious affiliation, such as if he never communicates on the Sabbath or visits a Mosque multiple times a day. Access to and analysis of such data allows deep, intrusive

and comprehensive view into a person's private life. Such information will also disclose the identity of confidential sources, including journalistic sources which are deserving of special protection.

23. Further, such information can be surrendered in bulk to foreign intelligence services. The restrictions on surrender of information in section 15(7) are extremely weak, give the Secretary of State the widest possible discretion and do not prescribe the circumstances in which information can be transferred with any clarity.

24. There is no published information as to the circumstances in which bulk data may be shared, the circumstances in which it may be analysed or processed, and the circumstances in which it must be destroyed. It is, in particular, unknown whether data surrendered abroad may be analysed by the foreign state by reference to a factor that is internal to the United Kingdom, and would be prohibited if information were collected here. Such a position is not sufficiently circumscribed to be prescribed by law.

Proportionality

25. No attempt is made in the Open Defence to deal with the proportionality of bulk interception, either as a matter of principle or on the basis that the facts in the Grounds can be assumed to be correct. If the Respondents are able to justify the bulk collection and analysis of most internet and telephone usage entering or leaving the UK on fibre optic cables, they ought to do so publicly, explaining how they are able to provide effective protection for privacy when every person's communications, regardless of who they are, are being automatically checked and analysed.

26. The Claimant contends that such blanket collection cannot be justified. Economic and technical constraints on bulk surveillance have now gone. It is possible to intercept and automatically analyse and process data in bulk. As Sotomayor J put in her concurring judgment in the US Supreme Court in *US v Jones* (2012), a case about GPS monitoring, but applicable *a fortiori* here:

> "... GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously [and] evades the ordinary checks that constrain abuse law enforcement practices: "limited police resources and community hostility".
>
> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring – by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track – may "alter the relationship between citizen and government in a way that is inimical to democratic society"...

27. Bulk interception, data retention and automated analysis is not merely a technical interference with privacy. It is a serious matter requiring weighty justification. As the Advocate General said in *C-293/12 Digital Rights Ireland* at [72]:

> "However, the fact remains that the collection and, above all, the retention in huge databases, of the large quantities of data generated or processed in connection with most of the everyday electronic communications of citizens of the Union constitute a serious interference with the privacy of those individuals, even if they only establish the conditions allowing retrospective scrutiny of their personal and professional activities. The collection of such data establishes the conditions for surveillance which, although carried out only retrospectively when the data are used, none the less constitutes a permanent threat throughout the data retention period to the right of citizens of the Union to confidentiality in their private lives. The vague feeling of surveillance created raises very acutely the question of the data retention period."

28. Similarly, in *Kayman v Obama* (2013), the US District Court for the District of Columbia (Judge Leon) granted an injunction restraining the continued operation of the NSA's blanket metadata collection programme. The judge noted that the extent of collection was fundamentally different from what was technologically possible in earlier decades, and that this presented novel and serious risks to privacy:

> "... people have a reasonable expectation of privacy that is violated when the Government, without any basis whatsoever to suspect them of any wrongdoing, collects and stores for five years their telephony metadata for purposes of subjecting it to high-tech query and analysis without judicial approval."

29. The Respondents seek to rely on two decisions of the European Court of Human Rights:

a. In *Weber v Saravia v Germany* (2006) the Third Section (by a majority) declared a claim about 'strategic interception' inadmissible. Strategic interception was the German practice of intercepting communications transmitted by satellite and searching them using 'catchwords'. The strategic interception policy covered "*merely some ten per cent of all communications*" and in practice was restricted to "*a limited number of foreign countries*" [110]. Personal information collected could only be used if "*specific facts – as opposed to mere factual indications – had aroused the suspicion that one of the offences*" listed in the legislation had been committed [127]. The Germans scheme was therefore significantly narrower and circumscribed than TEMPORA, and had substantially better safeguards. (Further, the extensive information given about safeguards by the German authorities is evidence that the NCND response is inappropriate, and the current scheme under section 8(4) of RIPA is not prescribed by law).

b. Subsequently, in *Liberty v UK* (2008) the Fourth Section unanimously upheld Liberty's complaint that bulk interception of communications between the UK and the Republic of Ireland was in breach of Article 8. The interception was, at the relevant time, directed at the terrorist threat posed by Republicans. The ECtHR held that a claim alleging blanket interception was admissible and sufficient safeguards were not present. The scheme was therefore not prescribed by law. Compensation was awarded to Liberty and its co-claimant. As the 'prescribed by law' complaint was upheld, the Court did not need to consider the proportionality of blanket interception operations and it did not do so. Indeed, the ECtHR has not yet considered the proportionality of a worldwide bulk collection operation.

30. The Respondents also seek to rely on the decision of the Tribunal in IPT 01/77, the complaint that led to *Liberty v UK*. In that case the Tribunal concluded that the alleged interception operation was in accordance with the law. The ECtHR held

that the Tribunal's conclusion was incorrect. In that case, the Tribunal also made the following comments about bulk interception under section 8(4) at [20.1]:

> "The basis of the two warrants is obviously different. This is because it is the more necessary for additional care to be taken with regard to interference with privacy by a Government in relation to domestic telecommunications, with regard to which it has substantial potential control; but also because its knowledge of, and certainly its control over, external communications is likely to be dramatically less. As a result, the domestic regime, so far as permitted interception is concerned, is considerably tighter."

31. This argument is (a) does not apply to TEMPORA; and (b) is wrong:

    a. TEMPORA involves the interception of fibre optic cables landing in the UK. They are physically within the jurisdiction and HM Government has the opportunity to exercise full control over such cables. There is no reason why a proper selection by reference to a person or premises could not be made, as would be required under section 8(1) of RIPA.

    b. HM Government's knowledge of the relevant communications will be identical if the same communications were between two UK internet or telephone users. Telephone calls and the internet operate on well-known and universal protocols. Communications across borders now follow standards promulgated by organizations such as the Internet Engineering Task Force (IETF) and the Institute of Electrical and Electronics Engineers (IEEE). For instance, all devices connected to the internet must use a "network protocol" in order to communicate. The most common network protocol, which is almost universally deployed, is the Internet Protocol (the IP in "IP address"). In addition, applications that function over the internet deploy protocols on top of the IP to facilitate their interactions. These protocols include the recognizable HTTP/HTTPS for web pages, IMAP, SMTP and POP for email, and SIP for Voice over IP (VOIP) phones. The parameters of all of these protocols are public and widely known and universally used throughout the world. Accordingly, the knowledge needed to access such communications, whether they are intercepted in Cornwall or Cairo, is identical. There

is no difference between intercepting internal and external internet communications.

c. If a particular person or premises must be identified for internal interception, there is no good reason why such a limitation is not imposed for external interception. The requirement to identify a person or premises is a crucial safeguard: it prevents bulk surveillance of the kind done under the TEMPORA operation. It ensures that surveillance is confined to a specific place or person. This greatly reduces the degree of intrusion involved in surveillance. The absence of this safeguard as applied to external communications amounts to unjustified discrimination, contrary to the general principles of EU law, the EU Charter of Fundamental Rights and Article 15(1) of Directive 2002/58/EC[5] and Article 14 ECHR read with Articles 8and 10 [6] . The discriminatory effect will fall overwhelmingly on foreign nationals, who are more likely to be engaging in external communications. See *A v SSHD (No. 1)* [2005] 2 AC 68.

Procedural issues

32. The Tribunal is invited to rule that the blanket claim to NCND should be rejected and the Respondents should produce an open Defence setting out their case on the TEMPORA operation and the full reasons why it is alleged that it is prescribed by law and proportionate.

33. The Tribunal should then hold an open public hearing of the complaints on their merits. The Claimants will wish to call evidence, and to cross-examine any witnesses called by the Respondents. Important issues of fact arise, in particular the extent to which the differences between external and internal communications

[5] Article 15(1) of Directive 2002/58/EC provides that telephone tapping is only permissible when it complies with requirements of necessity and proportionality and the general principles of EU law. This is a harmonising measure and expressly prohibits discrimination contrary to the Charter of Fundamental Rights or the ECHR. Tempora is based on a discriminatory law involving unjustified indirect discrimination against non UK nationals.

[6] The suggestion at footnote 54 that *Huber v Germany* can be distinguished because the German database only covered non-nationals is incorrect. It is clear that the distinction between internal and external communications is indirectly discriminatory on grounds of nationality and therefore requires justification.

can be factually justified in the modern world, the privacy harms that can be caused by the bulk collection and analysis of metadata and the safeguards applicable before information is transferred to a foreign intelligence service.

34. The Respondents' proposed issues of law are inappropriate:

    a. The central issues (e.g. when should Respondents be permitted to collect all data flowing across its borders and use technical means to process and analyse it, and freely share data with foreign states), which have been openly disclosed and debated in reporting throughout the world, are omitted. Much of the evidence on these issues can and should be dealt with in open.

    b. The issue of proportionality is not addressed at all, even on the basis of assumed facts.

35. The Respondents resist the appointment of a Special Advocate (Defence [224]). They rely on IPT ruling IPT/01/62 and IPT/01/77 ("the Procedural Ruling") and *Kennedy v UK* (2011) 52 EHRR 4. Those cases made no ruling on whether the IPT has a power to appoint special advocates or the circumstances in which that power should be exercised. Indeed in the Procedural Ruling, the Respondents are recorded as expressly accepting that the IPT has the power to appoint special advocates [155].

36. A Special Advocate ought to be appointed. In a case such as this, a Special Advocate is an essential procedural safeguard. The appointment of a *amicus curiae* is not sufficient. There ought to be an advocate advancing the Claimant's position in respect of material it is not permitted to see. In contrast to an *amicus*, the Claimants can select their own Special Advocate (from a panel appointed by the Attorney General), meet with a Special Advocate on a privileged basis before he or she sees any closed material, can give him or her instructions, and continue to send privileged information, advice and instructions throughout the case. Further, the Special Advocate can call witnesses. Given the context, complexity and importance of the instant case it is very difficult to see any good reason why a Special Advocate should not be appointed (and no reasons are put forward by the Respondents).

37. The Tribunal is invited to give the Special Advocate permission to appoint an investigator, to assist him or her to understand any relevant technical material, and to give expert evidence to the Tribunal.

38. The Tribunal is invited to exercise caution before inviting the Commissioners to give assistance. An issue before the Tribunal is the extent to which the Commissioners have been able to act as an effective oversight mechanism. In these circumstances, the Commissioners should only participate in these proceedings (if at all) as witnesses.

39. The Claimant agrees to the joinder of the Liberty claim.

DAN SQUIRES

BEN JAFFEY

BHATT MURPHY

20 December 2013