App. No. 58170/13

IN THE EUROPEAN COURT OF HUMAN RIGHTS
BETWEEN:

(1) BIG BROTHER WATCH
(2) OPEN RIGHTS GROUP
(3) ENGLISH PEN
(4) DR CONSTANZE KURZ

Applicants

- v -

UNITED KINGDOM

Respondent

JOINT APPLICATION UNDER ARTICLE 34

Solicitors to the Applicants	Counsel for the applicants
Deighton Pierce Glynn Solicitors Centre Gate Colston Avenue Bristol BS1 4TR Tel: 0117 317 8133 Fax: 0117 317 8093 www.deightonpierceglynn.co.uk	Helen Mountfield QC Matrix Chambers Gray's Inn London WC1R 5LN Tel: 020 7404 3447 Fax: 020 74043448 Tom Hickman Ravi Mehta Blackstone Chambers Temple London EC4Y 9BW Tel: 020 7583 1770 Fax: 020 7822 7350

CONTENTS

I. SUMMARY

1. The secret interception of communications by the State goes to the heart of the freedoms protected by Article 8 of the Convention (hereafter the "**ECHR**"). Provided its use is adequately circumscribed by published legal standards and proportionately used, such interception can be justified to protect the rights and freedoms of others. However, the necessarily secret nature of interception, coupled with the range and sensitivity of some internet communication creates serious risks of arbitrary state intrusion in many aspects of private life and correspondence, which necessarily include highly intimate aspects of the private sphere. Recent technical

developments mean that the State's capacity to capture, store and use private communications is greater than ever before.

2. In *Kennedy v United Kingdom* (2011) 52 EHRR 4 at [93], this Court recognised that the evident risk of arbitrariness in a secret power to intercept communications rendered it "essential" to have clear, detailed rules on interception, especially as the technology available for doing so is becoming continually more sophisticated. It observed at [94] that it would be contrary to the rule of law for the legal discretion granted for interception to be expressed in terms of an unfettered power. It also observed (at [160]) that "*indiscriminate capturing of vast amounts of communications is not permitted under the internal communications provisions of the Regulation of Investigatory Powers Act 2000*" ("**RIPA**"). The Court has also held that Article 8 jurisprudence must adapt to technological developments in *Weber v Germany* (2008) 46 EHRR SE5 at [93], and observed that in the context of rapidly developing telecommunications technology, legislative frameworks governing the safeguarding of private information and electronic correspondence must be "*particularly precise*" (*Uzun v Germany* (2012) 54 EHRR 121 at [61]).

3. This Application is made because recent reporting in the news media around the world indicates that technologies have now been developed, and have for some time been in use, which *do* permit the indiscriminate capture of vast quantities of communication data, which can then be passed between States, and which is not subject to any sufficiently precise or ascertainable legal framework and is beyond effective legal scrutiny.

4. The two programmes which are challenged by this Application are:
   4.1. The soliciting or receipt and use by the UK intelligence services ("**UKIS**"), of data obtained from foreign intelligence partners, in particular the US National Security Agency's "PRISM" and "UPSTREAM" programmes (hereafter "**receipt of foreign intercept data**"); and

4.2. The acquisition of worldwide and domestic communications by the Government Communications Head Quarters ("**GCHQ**") for use by UK Intelligence Services ("**UKIS**") and other UK and foreign agencies through the interception, under global and rolling warrants, of electronic data transmitted on transatlantic fibre-optic cables (the "**TEMPORA**" programme). (hereafter "**generic GCHQ intercept**"). As to generic GCHQ intercept based on tapping transatlantic cables, this is a form of *"external"* communication interception (although it can and does include persons in the UK) so that the general prohibition in RIPA on indiscriminate capture (at issue in *Kennedy*) does not apply.

5. There is now considerable information in the public domain about the operation of PRISM/UPSTREAM and TEMPORA. What is known about their operation is explained in the expert witness statements of Cindy Cohn, Legal Director of the Electronic Frontier Foundation, and Dr Ian Brown, Senior Research Fellow at the Oxford Internet Institute at the University of Oxford. This information has given rise to widespread concerns that have been voiced in a number of European States as well as in the US **[Annex 2/IB1/682-685; 983]**.

6. In summary, the Applicants contend that, in violation of Article 8 of the ECHR

6.1. In relation to receipt of foreign intercept material—i.e. the receipt, use, retention and dissemination of information received by UKIS from foreign intelligence partners which have themselves obtained it by communications intercept—the legal framework is inadequate to comply with the "*in accordance with the law*" requirement under Article 8(2).

6.2. In relation to GCHQ's own generic interception capability, the provisions contained in RIPA relating to external communications warrants allow UKIS to obtain general warrants permitting indiscriminate capturing of vast amounts of communication,

effectively on an indefinite basis. The legal provisions which permit generic warrants in relation to such external communications are insufficiently protective to provide an ascertainable check against arbitrary use of secret and intrusive state power.

6.3. Such legal provisions do not enable persons to foresee the general circumstances in which external communications may be the subject of surveillance (other than that any use may be made of communications if considered in the interests of national security—a concept of very broad scope in UK law); they do not require authorisations to be granted in relation to specific categories of persons or premises; they permit indiscriminate capture of communications data by reference only to its means of transmission; and they impose no significant restrictions on the access that foreign intelligence partners may have to such intercepted material. In short, there are no defined limits on the scope of discretion conferred on the competent authorities or the manner of its exercise. Moreover, there is no adequate degree of independent or democratic oversight. Indiscriminate and generic interception and the legal provisions under which it is carried out thereby breach the requirements that interferences with Article 8 must be "*in accordance with the law*" and must be proportionate.

7. This Court, and the former Commission, have found violations of Article 8 ECHR in the past in the context of surveillance and intelligence service activity by UK authorities, on the basis that UK law has not been sufficiently transparent, clear and precise. These judgments have driven reform in the UK: e.g. *Malone v UK* (1985) 7 EHRR 14; *Hewitt & Harman v UK* (1992) 14 EHRR 657; *Halford v UK* (1997) 24 EHRR 523; *Khan v UK* (2001) 31 EHRR 45; and *Liberty v UK* (2009) 48 EHRR 1.

8. In *Liberty*, this Court considered the *previous* law in the UK governing interception of "*external communications*" under the *Interception of Communications Act 1985*, and found the law to be insufficiently protective.

The Court has not yet had the opportunity to consider the current legislative regime under RIPA in the context of external communications. (As noted, *Kennedy* related to the interception of "*internal*" communications).

9. For the detailed reasons set out below, it is submitted that the Application should be declared admissible and the Court should find that violations of Article 8 are established in the circumstances set out in the Application.

II. STATEMENT OF FACTS

A. The Applicants

10. **Big Brother Watch** ("**BBW**") is a company limited by guarantee. It is a campaign group that was founded in 2009 to conduct research into, and challenge policies which threaten privacy, freedoms and civil liberties, and to expose the scale of surveillance by the state. It campaigns for more control over personal data, and better accountability mechanisms to hold to account those who fail to respect individual privacy, whether private companies or public authorities.

11. BBW is based in London. Its staff regularly liaise and work in partnership with similar organisations in other countries. They often communicate with persons and bodies around the world by email and Skype. As a vocal critic of excessive surveillance, and a commentator on sensitive topics relating to national security, BBW believes that its staff and directors may have been the subject of surveillance by or on behalf of the UK government. Moreover, it has contact with internet freedom campaigners and those who wish to complain to regulators around the world, so it is conscious that some of those with whom it is in contact may also fall under surveillance.

12. **English PEN** is a registered charity. It is the founding centre of a worldwide writers' association and has 145 centres in over 100 countries. It promotes freedom to write and read, and campaigns around the world on freedom of expression, and equal access to the media.

13. English PEN is based in London, and works in partnership with sister organisations around the world. It also works closely with individual writers at risk and in prison. Most of its internal and external communications are by email and by Skype and they are pan-global. Since many of those for and whom with English PEN campaigns express views on governments which may be controversial, English PEN believes that it, and those with whom it communicates, may be the subject of UK government surveillance, or may be the subject of surveillance by other countries' security services which may pass such information to the UK security services (and vice-versa). They work closely with writers and dissidents in many countries including, amongst others, Syria, Belarus, Turkey, Vietnam and Cameroon, and are gravely concerned that these persons' right to freedom of expression and security may be put at risk by surveillance.

14. **Open Rights Group** (**"ORG"**) is a company limited by guarantee. It was founded in 2005 and is one of the UK's leading campaign organisations defending freedom of expression, innovation, creativity and consumer rights on the internet. It is based in London and regularly liaises and works in partnership with other organisations in other countries. It is a member organisation of European Digital Rights (EDRi), a network of 35 privacy and civil rights organisations founded in June 2002, with offices in 21 different countries in Europe. Most of its internal and external communications are by email and Skype. For similar reasons to those expressed by BBW and English PEN, it believes that its electronic communications and activities may be subject to foreign intercept conveyed to UK authorities, or intercept activity by UK authorities.

15. **Dr Constanze Kurz** is based in Berlin. She holds a doctoral degree in computer science and works at the University of Applied Sciences in Berlin. She is an expert on surveillance techniques and has co-authored technical analyses for the German Constitutional Court in controversial cases concerning data retention, anti-terrorism databases and computerised

voting. From 2010 to 2013, she was a member of the "*Internet and Digital Society*" Commission of Inquiry of the German Bundestag.

16. Dr Kurz is also spokeswoman of the German "Computer Chaos Club" (CCC) which campaigns to highlight weaknesses in computer networks which risk endangering the interests of the public. It undertakes direct action. For example, it drew public attention to the security flaws of the German *Bildchirmtext* computer network by hacking into it and causing it to debit DM 134,000 in a Hamburg bank in favour of the club. The money was returned the next day in front of the press. On another occasion, on 8 October 2011, the CCC published an analysis of the Staatstrojaner sofware, which was a 'trojan' computer surveillance programme used by the German police. Former Wikileaks spokesman Daniel Domscheit-Berg was a member of CCC for a number of years, though he was expelled in 2011.

17. Dr Kurz has been outspoken in relation to the recent disclosures regarding UK internet surveillance activities, which continue to be a subject of significant concern in the German media. She fears that she may well have been the subject of surveillance either directly by GCHQ or by US or other foreign security services who may have passed that data to the UK security services, not only because of her activities as a freedom of expression campaigner and hacking activist, but also because GCHQ and others may wish to learn from her and persons with whom she communicates, habitually in encrypted communications.

B. Circumstances of the Case

i. Background to Complaint Concerning Receipt of Foreign Intercept Data: Media Disclosures Concerning Receipt of PRISM and UPSTREAM Data by the United Kingdom Government

18. The UKIS is able to receive intelligence obtained by intercept from security services in other States. The Applicants' concern in relation to this has been triggered by recent media coverage of the existence of an extraordinarily

wide surveillance capability on the part of the US National Security Agency ("**NSA**") and the apparent sharing of the product of US intercept with the UK security services.

19. This coverage was generated by a leak of NSA documentation by Edward Snowden, a former NSA systems administrator. The existence of the programmes referred to in those slides has been confirmed by President Obama and by James Clapper, the US Director of National Intelligence.[1]

PRISM

20. PRISM is an intelligence-gathering operation run by the NSA which enables it to access a wide range of internet communication content (such as emails, chat, video, images, documents, links and other files) and metadata from US corporations including some of the largest internet service providers such as Microsoft, Google, Yahoo, Apple, Facebook, Youtube and Skype.

21. Metadata consists of "*structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource*".[2] In the context of private communications this includes, but is not limited to, information which allows a person or location to be identified as well as the time, length and date of the communication to be determined. By piecing different items of such information together, it is possible to build-up a detailed picture of a person's life (as noted by Dr Ian Brown at §§9-14 of his witness statement **[Annex 2/511-513]**).

22. The scale of the PRISM operation is potentially vast, because global internet data takes the cheapest, not the most physically direct path. Thus a substantial volume of *worldwide* data passes through the servers of United States communications providers, even if neither party to a communication is located in the United States. This is illustrated by the following model in the NSA Slides:

[1] "*Transcript: Obama's Remarks on NSA Controversy"*, 7 June 2013 **[Annex 1/CC1/202-207]**; and "*DNI Statement on Activities Authorized Under Section 702 of FISA*" 6 June 2013 **[Annex 1/CC1/121D]**

[2] See "*Understanding Metadata*" (2004), the United States National Information Standards Organization, at p.1. **[Annex 3/1084-1103]**

Newspaper reports indicate that over 2,000 PRISM-based "*reports*" of communications are issued every month by the NSA and more than 77,000 intelligence reports had been made based on that data by June 2013 **[Annex 1/CC1/134-140]**[3]. It is also reportedly of great value to the NSA as the slides acknowledge that PRISM is the resource "used most" in NSA reporting **[Annex 1/CC1/134]**.

23. The US government has confirmed the existence of the programme, and states that such interception has a basis in United States law: section 702 of the *Foreign Intelligence Surveillance Act 1978* (**"FISA"**) (US Code §1881(a)) **[Annex 1/CC1/304-314]**. That provision permits the making of renewable one year authorisations for generalised foreign surveillance without a warrant, in circumstances where the intended target is not believed to be "a US person" – i.e. a person in the United States. Ms Cindy Cohn, Legal Director of the Electronic Frontier Foundation, has given a witness statement in support of this application [**Annex 1**] in which she explains the

[3] "*NSA Prism program taps in to user data of Apple, Google and others*", Glenn Greenwald and Ewen MacAskill, *The Guardian*, 7 June 2013 **[Annex 1/CC1/134-140]**

limitations of the legal protections of privacy in that statute. In summary, these apply solely to persons in the US or "*US Persons*" (citizens and certain residents), and are aimed at ensuring that such persons are not intentionally or inadvertently targeted by the programme. However, FISA does not limit the extent of permitted state surveillance of non-US persons at all—any surveillance of such persons which has been authorised (on a generic basis) is permitted. Thus, any surveillance of communications between two persons both located outside the United States, whose communication happens to be routed through the United States, is permitted absolutely. Moreover, communication where one party is located inside the United States and is thus a US-person is also permitted, without any requirement to show "*probable cause*" in respect of such an individual, provided the accessing of data falls within a broadly-framed section 702 "*authorisation*" for data collection.

UPSTREAM

24. The NSA also operates a second interception programme under section 702 of FISA called "UPSTREAM". This provides access to nearly all the traffic passing through fibre optic cables owned by US communications services providers such AT&T and Verizon.

25. As Ms Cohn states [**Annex 1/70**], between them, PRISM and UPSTREAM provide very broad access to the communications content and metadata of non-US Persons, to which the provisions of the Fourth Amendment (the US Constitution privacy guarantee) do not apply.[4] These two programmes provide for the bulk seizure, acquisition, collection and storage of all or nearly all of the considerable quantity of global communications content and metadata of non-US persons that passes through the US. They also provide for the searching of that content and metadata with little or no restriction once the material is determined not to be related to a US person, and in the case of many exceptional categories, even if it does.

[4] Under the FISA law, 50 U.S.C. §1801 (i) "United States person" means "a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101 (a)(20) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section."

Receipt of PRISM and UPSTREAM intercept by the UKIS

26. The Edward Snowden documents made public by *The Guardian* newspaper show that GCHQ has had access to PRISM material since at least June 2010. It has also reported that GCHQ generated at least 197 intelligence reports from that material in 2012 alone. The NSA documents made public by *The Guardian* state for instance that, "*special programmes for GCHQ exist for focused Prism processing*"[5] [**Annex 2/IB1/605B**].

27. It is unclear whether GCHQ's access to this material is limited to solicited material (i.e. where GCHQ specifically requests information from the NSA) or whether it includes unsolicited information-sharing. It appears that both are possible. There is no publicly available information about what is done with such material once received.

28. The PRISM and UPSTREAM disclosures have exposed the absence of legal controls on GCHQ and the other UKIS in relation to the receipt of data from overseas intelligence partners which have themselves obtained the data by intercepting communications

29. GCHQ has not denied the use of PRISM generated material. It has merely stated that it:

> "takes its obligations under the law very seriously. Our work is carried out in accordance with a strict legal and policy framework which ensures that our activities are authorised, necessary and proportionate, and that there is rigorous oversight, including from the Secretary of State, the interception and intelligence services commissioners and the intelligence and security committee."[6]

30. However, it has not specified the "*legal* [...] *framework*" which in its view governs receipt of material from NSA interceptions.

[5] "*UK gathering intelligence via covert NSA operation*", Nick Hopkins, *The Guardian*, 7 June 2013 **[Annex 2/IB1/605A-605D]**

[6] "*GCHQ tapped fibre-optic cables for data, says newspaper*", *The Guardian*, 22 June 2013 **[Annex 2/IB1/678A-678C]**

ii. Background to Complaint Concerning Generic GCHQ Intercept: the TEMPORA Programme

31. The disclosures based on Edward Snowden's leaked documentation have also provided details about a UK surveillance programme called TEMPORA. TEMPORA is a means by which GCHQ can access electronic traffic passing along fibre-optic cables running between the UK and North America. The data collected include both internet and telephone communications. GCHQ is able to access not only metadata but also the content of emails, Facebook entries and website histories[7]. Data is accessed without the need for reasonable suspicion in relation to the activities of any particular targeted persons. It is referred to as "*special source exploitation*" and has reportedly been operational for 18 months.

32. In a process known as "*buffering*" GCHQ is said to be authorised by the Secretary of State to store information for 3 days for content and 30 days in the case of data (although the Applicants presume that these periods are extended if the data is considered to have intelligence value)[8].

33. The TEMPORA programme is authorised by certificates issued under section 8(4) of RIPA, granted to GCHQ. This relates to "*external communications*", being communications that are either sent or received outside the British Isles.

34. GCHQ has confirmed that the programme has 10 "*basic*" certificates including one "*global*" certificate relating to GCHQ's support station at Bude in Cornwall. These certificates are said to be reviewed and apparently have been renewed every 6 months. This creates a "*broad, overall legal authority which has to be renewed at intervals*"[9].

35. However, the certificates upon which this "*broad, overall*" authority are said to be based reportedly authorise the interception of *any* transatlantic cable

[7] "*GCHQ taps fibre-optic cables for secret access to world's communications*", Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, *The Guardian*, 21 June 2013 **[Annex 2/IB1/658-663]**
[8] *Ibid*
[9] "*The legal loopholes that allow GCHQ to spy on the world*", Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, *The Guardian*, 21 June 2013 **[Annex 2/IB1/664-668]**

data as long as the purpose of the intercept comes within one of a number of very broadly framed criteria such as "*terrorism*", "*organised crime*" and the "*economic well-being*" of the UK. Media reports suggest that the authorisation certificates do not list the search terms or impose any detailed restrictions on the information that can be intercepted or searched. *The Guardian* has reported that:

> "The categories of material have included fraud, drug trafficking and terrorism, but the criteria at any one time are secret and are not subject to any public debate. GCHQ's compliance with the certificates is audited by the agency itself, but the results of those audits are also secret.
>
> An indication of how broad the dragnet can be was laid bare in advice from GCHQ's lawyers, who said it would be impossible to list the total number of people targeted because "*this would be an infinite list which we couldn't manage.*"[10]

36. There is also a suggestion that private companies have been cooperating with GCHQ on the basis of licence conditions which compel them to co-operate, and to refrain from revealing the existence of any such warrant or certificate of authorisation[11].

37. The scale of the TEMPORA programme is unprecedented. As reported by *The Guardian,* in a paper written for NSA analysts entitled "*A Guide to Using Internet Buffers at GCHQ*", the author noted that TEMPORA "*represents an exciting opportunity to get direct access to enormous amounts of GCHQ's special source data*"[12].

38. In a presentation in 2011, a GCHQ legal adviser told NSA analysts t*hat a reason f*or using TEMPORA material was that, "[the UK] *ha[s] a light oversight regime compared with the US*."[13] Indeed, *The Guardian* reported on internal GCHQ documents from 2011 which recorded one of the UK's *"unique selling points" as* being "*the UK's legal regime*", given that GCHQ is "*less constrained by NSA's concerns about compliance*"[14].

---

[10] See n.7 above.
[11] "*BT and Vodafone among telecoms companies passing details to GCHQ*", James Ball, Luke Harding and Juliette Garside, *The Guardian*, 2 August 2013 **[Annex 2/IB1/719-722]**. These requirements were presumably imposed under RIPA ss.11-12 and *Interception of Communications*, Code of Practice (2007), paragraphs 2.7-2.10
[12] See n.7 above.
[13] See n.7 above.
[14] "*GCHQ: Inside the Top Secret World of Britain's Biggest Spy Agency*", Nick Hopkins, Julian Borger and Luke Harding, *The Guardian*, 1 August 2013 **[Annex 2/IB1/723-736]**

39. US agencies have been given extensive access to TEMPORA information. Reportedly, at least 250 and as many as 850,000 US Government employees and private companies working in partnership with the US Government have access to this information[15]. One US training slide revealed by *The Guardian* newspaper stated: "*... You are in an enviable position – have fun and make the most of it*."[16]

40. The NSA is also reported to have had 250 analysts working full-time on TEMPORA-derived data as of May 2012[17]. No information has been made available as to whether there are appropriate safeguards for this international data-sharing. As explained below, none are included in the relevant legislative provisions. Further disclosures have revealed that the NSA has paid up to £100 million over three years to GCHQ to secure access to its programmes. Accordingly "*GCHQ must pull its weight and be seen to pull its weight*" (as noted in a GCHQ strategy briefing)[18]. In *The Guardian* newspaper for 21 June 2013 it was reported that GCHQ had set over 40,000 search terms for trawling TEMPORA-obtained data, and the NSA had itself set over 31,000 search terms relating to matters and persons of interest to the US Government[19].

iii. Public Statements by the UK Government

41. Following some of the disclosures referred to above, the Secretary of State for Foreign and Commonwealth Affairs (the Rt. Hon. William Hague MP) gave a statement to Parliament on 10 June 2013. (Hansard HC, 10 June 2013, Col. 32-42) **[Annex 2/IB1/826-830]**. In relation to use of PRISM-generated data by GCHQ, Mr Hague stated:

> "It has been suggested that GCHQ uses our partnership with the United States to get around UK law, obtaining information that it cannot legally obtain in the United Kingdom. I wish to be absolutely clear that that

[15] See n.7 & n.14 above.
[16] See n.7 above.
[17] See n.7 above.
[18] "*Exclusive: NSA pays £100m in secret funding for GCHQ*", Nick Hopkins and Julian Borger, *The Guardian*, 1 August 2013 **[Annex 2/IB1/714-718]**
[19] See n.7 above.

> accusation is baseless. Any data obtained by us from the United States involving UK nationals are subject to proper UK statutory controls and safeguards, including the relevant sections of the Intelligence Services Act, the Human Rights Act 1998, and the Regulation of Investigatory Powers Act." (emphasis added)

42. By reference to this statement, the Secretary of State was asked, by the Rt. Hon. Douglas Alexander MP, the Shadow Foreign Secretary, to:

> "set out the relevant sections of those Acts, and confirm whether this explanation means that any data obtained by us from the US, involving UK nationals, are authorised by ministerial warrants and overseen by the intercept commissioner, as set out by RIPA?" (Col. 35)

43. The Secretary of State responded:

> "The right hon. Gentleman was right to say that he supports information sharing with our allies. The position on the legal framework is exactly as I set out in my statement: any data obtained by us from the United States about UK nationals are subject to the full range of Acts, including section 3 of the Intelligence Services Act 1994 and the RIPA provisions, set out in sections 15 and 16, which regulate that information gathering must be necessary and proportionate and regulate how the agencies must handle information when they obtain it."

44. Mr Alexander also asked some specific questions:

> "Specifically, what legal framework applies in the following two cases?
>
> First, when a request is made by the UK to an intelligence agency of an international ally for the interception of the content of private communications, will he confirm whether this process is governed by individual warrants signed by the relevant Secretary of State and approved by the intercept commissioner as set out in part I of RIPA?
>
> Secondly, will he address the specific issue of when a request is made by the UK to an intelligence agency of an international ally, not to seek intercept, but instead to search existing data held by that agency on the contents of private communications, and, in particular, the legal process that will be adopted in such an instance? In that circumstance, will he confirm whether this process is also governed by individual warrants signed by the relevant Secretary of State and approved by the intercept commissioner as set out in part I of RIPA?" (Cols. 35 – 36)

45. The Secretary of State refused to provide any information as to the legal regime that applies in relation to these matters. He answered the questions in the following terms:

> "On the right hon. Gentleman's further questions about how authority is given, I cannot give him, for reasons that I cannot explain in public, as detailed an answer as he would like. I would love to give him what could actually be a very helpful answer, but because circumstances and procedures vary according to the situation, I do not want to give a categorical answer— in a small respect circumstances might differ occasionally. But I can say that

> ministerial oversight and independent scrutiny is there, and there is scrutiny of the ISC in all these situations, so, again, the idea that operations are carried out without ministerial oversight, somehow getting around UK law, is mistaken. I am afraid that I cannot be more specific than that."

46. The First and Second Applicants wrote a letter to the Secretary of State and other UK Government agencies dated 3 July 2013 **[Annex 3/1056-1079]** setting out the alleged breaches of the Convention referred to herein (see further paragraphs 181-182 below). In a response to that letter dated 26 July 2013 **[Annex 3/1081-1083]**, the Treasury Solicitor on behalf of the UK Government stated that,

> "As regards your complaints relating to the possible receipt of intelligence from the United States intelligence agencies: in addition to the statutory scheme in RIPA, SIS and GCHQ must also comply with the Intelligence Services Act 1994, and must in particular do so when obtaining and disclosing information. The agencies must also act compatibility with the HRA and the Data Protection Act 1998."

iv. Report of the Intelligence and Security Committee, 17 July 2013

47. On 17 July 2013, the Intelligence and Security Committee of Parliament ("**ISC"**) published a "*Statement of GCHQ's Alleged Interception of Communications under the US PRISM Programme*" **[Annex 2/IB1/831-833]**. The report confirmed GCHQ access to PRISM material. It stated:

> "1. Over the last month, details of highly classified intelligence-gathering programmes run by the US signals intelligence agency – the National Security Agency (NSA) – have been leaked in both the US and the UK. Stories in the media have focussed on the collection of communications data and of communications content by the NSA. These have included the collection of bulk 'meta-data' from a large communications provider (Verizon), and also access to communications content via a number of large US internet companies (under the PRISM programme)."
>
> …
>
> 4. Stories in the media have asserted that GCHQ had access to PRISM and thereby to the content of communications in the UK without proper authorisation. It is argued that, in so doing, GCHQ circumvented UK law. This is a matter of very serious concern: if true, it would constitute a serious violation of the rights of UK citizens."

48. The report continued:

> **"Our investigation**
> 5. The ISC has taken detailed evidence from GCHQ. Our investigation has included scrutiny of GCHQ's access to the content of communications, the

legal framework which governs that access, and the arrangements GCHQ has with its overseas counterparts for sharing such information. We have received substantive reports from GCHQ, including:

- a list of counter-terrorist operations for which GCHQ was able to obtain intelligence from the US in any relevant area;
- a list of all the individuals who were subject to monitoring via such arrangements who were either believed to be in the UK or were identified as UK nationals;
- a list of every 'selector' (such as an email address) for these individuals on which the intelligence was requested;
- a list of the warrants and internal authorisations that were in place for each of these individual being targeted;
- a number (as selected by us) of the intelligence reports that were produced as a result of this activity; and
- the formal agreements that regulated access to this material.

We discussed the programme with the NSA and our Congressional counterparts during our recent visit to the United States. We have also taken oral evidence from the Director of GCHQ and questioned him in detail."

49. The ISC concluded, without providing any further information as to the applicable legal regime or safeguards, that there had been no violation of UK law.

"• We have reviewed the reports that GCHQ produced on the basis of intelligence sought from the US, and we are satisfied that they conformed with GCHQ's statutory duties. The legal authority for this is contained in the Intelligence Services Act 1994.

• Further, in each case where GCHQ sought information from the US, a warrant for interception, signed by a Minister, was already in place, in accordance with the legal safeguards contained in the Regulation of Investigatory Powers Act 2000."

50. In a section on "Next Steps" the ISC recorded that:

"6. Although we have concluded that GCHQ has not circumvented or attempted to circumvent UK law, it is proper to consider further whether the current statutory framework[FN] governing access to private communications remains adequate.

7. In some areas the legislation is expressed in general terms and more detailed policies and procedures have, rightly, been put in place around this work by GCHQ in order to ensure compliance with their statutory obligations under the Human Rights Act 1998. We are therefore examining the complex interaction between the Intelligence Services Act, the Human Rights Act and the Regulation of Investigatory Powers Act, and the policies and procedures that underpin them, further. We note that the Interception of Communications Commissioner is also considering this issue."

The footnote reference in the above passaged identified the *Intelligence Services Act 1994* (c.5) ("**ISA**"), RIPA and the HRA.

51. The ISC report thus raised expressly questions about the adequacy of the applicable regime.

52. Moreover, the terms of the ISC report were necessarily limited since the ISC had only looked at intelligence information which GCHQ had specifically requested from the US, in relation to particular individuals who were subject to interception warrants in the UK. It did not look at other information received from the NSA by GCHQ or other UK government agencies. This was not clear from the terms of the ISC report, but was confirmed by the ISC's Chairman, Sir Malcolm Rifkind MP, in a subsequent press briefing[20].

C. Relevant Domestic Law and Practice

53. The relevant legislative provisions are provided in full in Annex 4 to this application.

i. The Intelligence Services Act 1994 and Security Service Act 1989

54. The UKIS are comprised of three agencies: the Secret Intelligence Service ("**SIS**"), Government Communications Headquarters ("**GCHQ**") and the Security Service.

55. Section 1 of the *Intelligence Services Act 1994* ("**ISA**") (see Annex 4) provides a statutory basis for the operation of the SIS and inter alia provides a statutory basis for the receipt of information from foreign agencies:

> "**1. The Secret Intelligence Service.**
> (1) There shall continue to be a Secret Intelligence Service (in this Act referred to as "the Intelligence Service") under the authority of the Secretary of State; and, subject to subsection (2) below, its functions shall be—
> (a) to obtain and provide information relating to the actions or intentions of persons outside the British Islands; and
> (b) to perform other tasks relating to the actions or intentions of such persons.

[20] "*Inquiry into snooping laws as committee clears GCHQ*", Julian Borger, *The Guardian*, Thursday 18 July 2013 **[Annex 2/IB1/834-836]**

(2) The functions of the Intelligence Service shall be exercisable only—

(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or

(b) in the interests of the economic well-being of the United Kingdom; or

(c) in support of the prevention or detection of serious crime."

56. Section 2 of ISA provides for the control of SIS operations by a Chief of the service appointed by the Secretary of State. He is responsible for the efficiency of the service and section 2(2) provides that:

"... it shall be his duty to ensure -

(a) that there are arrangements for securing that no information is obtained by the Intelligence Service except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary -

(i) for that purpose;

(ii) in the interests of national security;

(iii) for the purposes of the prevention or detection of serious crime; or

(iv) for the purpose of any criminal proceedings ..."

Subsection 2(4) requires the Chief of the Intelligence Service to make an annual report on the work of UKIS to the Prime Minister and Secretary of State, but these reports are not published.

57. Section 3 of ISA sets out the authority for the operation of GCHQ:

"**3. The Government Communications Headquarters.**

(1) There shall continue to be a Government Communications Headquarters under the authority of the Secretary of State; and, subject to subsection below, its functions shall be—

(a) to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material; and

(b) to provide advice and assistance about—

(i) languages, including terminology used for technical matters, and

(ii) cryptography and other matters relating to the protection of information and other material,

to the armed forces of the Crown, to Her Majesty's Government in the United Kingdom or to a Northern Ireland Department or to any other organisation which is determined for the purposes of this section in such manner as may be specified by the Prime Minister.

(2) The functions referred to in subsection (1)(a) above shall be exercisable only—

(a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or

(b) in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands; or

(c) in support of the prevention or detection of serious crime.

(3) In this Act the expression "GCHQ" refers to the Government Communications Headquarters and to any unit or part of a unit of the armed forces of the Crown which is for the time being required by the Secretary of State to assist the Government Communications Headquarters in carrying out its functions."

58. Section 4(2) ISA requires the Director of GCHQ

"... to ensure -

(a) that there are arrangements for securing that no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings ..."

59. Section 1 of the *Security Service Act 1989* (see Annex 4) provides statutory foundation for the Security Service and *inter alia* provides a power for the receipt of information from foreign intelligence agencies:

"**1.— The Security Service.**

(1) There shall continue to be a Security Service (in this Act referred to as "the Service") under the authority of the Secretary of State.

(2) The function of the Service shall be the protection of national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means.

(3) It shall also be the function of the Service to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands.

(4) It shall also be the function of the Service to act in support of the activities of police forces, the Serious Organised Crime Agency and other law enforcement agencies in the prevention and detection of serious crime.

(5) Section 81(5) of the Regulation of Investigatory Powers Act 2000 (meaning of "prevention" and "detection"), so far as it relates to serious crime, shall apply for the purposes of this Act as it applies for the purposes of the provisions of that Act not contained in Chapter I of Part I."

60. Section 2 is a similar provision to s.2 ISA, in that it provides for a Director-General, charged with a:

> "**2.— The Director-General.**
> […]
> (2) […] duty to ensure—
> (a) that there are arrangements for securing that no information is obtained by the Service except so far as necessary for the proper discharge of its functions or disclosed by it except so far as necessary for that purpose or for the purpose of the prevention or detection of serious crime or for the purpose of any criminal proceedings; and […]"

Similarly, subsection 2(4) requires the Director-General to make an annual report on the work of Security Service to the Prime Minister and Secretary of State.

ii. The Regulation of Investigatory Powers Act 2000

61. The domestic law regulating the interception and reception of communications is principally set out in RIPA (see Annex 4). The "*main purpose*" of RIPA, as stated in the accompanying Explanatory Notes to that Act, is to "*ensure that the relevant investigatory powers are used in accordance with human rights*". A summary of the statute's key provisions is set out at paragraphs 43-49 of the *Liberty* case.

62. Part I of RIPA regulates "*communications*". Chapter I of Part I RIPA regulates the interception of communications. Chapter II of Part I regulates the obtaining of "*communications data*" from telecommunications providers.

Part I, Chapter I RIPA:

63. The scope *rationae materiae* of Chapter I is set out in three provisions. Section 1(1) RIPA provides:

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

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

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

65. Section 2(4) sets out the geographical reach of Chapter I:

> "For the purposes of this Act the interception of a communication takes place in the United Kingdom if, and only if, the modification, interference or monitoring … is effected by conduct within the United Kingdom."

66. Section 1(5) defines "*lawful authority*" as follows:

> "(5) Conduct has lawful authority for the purposes of this section if, and only if–
>
> (a) it is authorised by or under section 3 or 4;
>
> (b) it takes place in accordance with a warrant under section 5 ("an interception warrant"); or
>
> (c) it is in exercise, in relation to any stored communication, of any statutory power that is exercised (apart from this section) for the purpose of obtaining information or of taking possession of any document or other property."

67. Thus, interception of communications is not unlawful if it is authorised by a warrant issued by the Secretary of State under section 5.

68. Section 8 sets out the requirements of the content of warrants:

> "**8.— Contents of warrants.**
>
> (1) An interception warrant must name or describe either–
>
> (a) one person as the interception subject; or
>
> (b) a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place.
>
> (2) The provisions of an interception warrant describing communications the interception of which is authorised or required by the warrant must comprise one or more schedules setting out the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications that may be or are to be intercepted.

(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."

(emphasis added)

69. The combined effect of sections 8(4) and 8(5)(a) RIPA is that the limitations and safeguards on the ambit of an interception warrant for interception of *internal* communications, which satisfied this Court in Kennedy, do not apply in relation to a warrant for interception of *external* communications which may be generic by reference to a described class of intercept material. This is explained further by Ian Brown at §§52-55 of his Witness Statement **[Annex 2/530-32]**.

70. Moreover, such a generic warrant has a long shelf-life. By virtue of s.9(1)(a) and 9(6)(ab) RIPA, a standard warrant endorsed under the hand of the Secretary of State with a statement "*that the issue of the warrant is believed to*

be necessary on grounds falling within section 5(3)(a) or (c)", lasts for a period of six months. Without such a statement, it lasts 3 months (s.9(6)(c)). This can be renewed for further periods of six months (s.9(1)(b)) so long as the Secretary of State certifies that the warrant remains necessary.

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

72. Section 16(1) and (2) RIPA provide that an interception warrant in respect of "*external communications*" may only be "*referable to an individual*" in the UK or "*have as its purpose, or one of its purposes, the identification of material contained in communications sent by him, or intended by him*" if the Secretary of State certifies that this is necessary.

73. Section 17 restricts the disclosure of the existence or content of warrants granted under Chapter I. Section 18(1)(c) disapplies this restriction in relation to proceedings in the Investigatory Powers Tribunal (set out below).

Chapter II RIPA:

74. Chapter II of RIPA concerns the "*acquisition and disclosure of communications data*". The scope *rationae materiae* of Chapter II is set out in section 21. Section 21(1) RIPA provides:

> "This Chapter applies to (a) any conduct in relation to a […] telecommunications system for obtaining communications data, other than conduct consisting in the interception of communications in the course of their transmission by means of such a service or system, and (b) the disclosure to any person of communications data."

75. Chapter II of RIPA only applies to conduct in relation to a telecommunications system for obtaining (i) metadata (under section 21(4)(a) or (b)) or (ii) other data, including content data, which is held by a person providing a "*telecommunications service*" (under section 21(4)(c)). It does not apply to content data which is provided by any other type of

person, such as a foreign intelligence agency. Content data and metadata are explained in the Witness Statement of Ian Brown at §§8-14, 31 **[Annex 2/510-513, 521-522]**

Scrutiny of Investigatory Powers:

76. Part IV of RIPA provides for "scrutiny" of investigatory powers.

77. RIPA provides for the appointment of two Commissioners to supervise the activities of the intelligence services:

    77.1. Section 57 RIPA provides for the appointment of an "*Interception of Communications Commissioner*". The Commissioner is charged with supervising the exercise of functions under – *inter alia* - Chapters I and II of the Act, and notifying the Prime Minister by a report if he notes any contraventions of the Act (s.58). The Prime Minister must place such reports before the Houses of Parliament (s.58(6)) although he may redact information which he considers sensitive (s.58(7)).

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

78. The Intelligence Services Commissioner has also accepted an extra-statutory role in monitoring compliance with the "*Consolidated Guidance to Intelligence Officers and Service Personnel on the Detention and Interviewing of Detainees Overseas, and on the passing and Receipt of Intelligence Relating to Detainees*". ("**Consolidated Guidance**"). The Consolidated Guidance was published by the UK Government in July 2010.

79. In his 2011 Annual Report, (13 July 2012 (HC 497) p.28 **[Annex 3/1104-1154]**, the Commissioner stated that by agreement his extra-statutory role had been limited to occasions where UKIS or the Armed Forces had,

> "- been involved in the interviewing of a detainee held overseas by a third party (this may include feeding in questions or requesting the detention of an individual).
> - had received information form a liaison service (solicited or not) where there is reason to believe it originated from a detainee.
> - Had passed information in relation to a detainee to a liaison service."

80. As stated at p.11 of the 2011 Annual Report, the Intelligence Service Commissioner's extra-statutory remit can be extended by direction from the Prime Minister. However, it presently does not so extend and therefore does not apply to the receipt or use of intelligence from foreign intelligence partners.

81. Section 65 provides for a Tribunal, the Investigatory Powers Tribunal ("**IPT**"), which is given jurisdiction for determining claims related to the conduct of the intelligence services, including proceedings under the *Human Rights Act 1998* ("**HRA**") (s.65(2)). In *R(A) v B* [2009] UKSC 12; [2010] 2 AC 1, the Supreme Court of the United Kingdom held that the IPT has exclusive and final jurisdiction for such proceedings (p.36 at [38] per Lord Brown of Eaton-under-Heywood JSC).

82. Section 68(1) provides that the IPT shall have power to determine its own procedure. Section 68(4) provides that,

> "Where the Tribunal determine any proceedings, complaint or reference brought before or made to them, they shall give notice to the complainant which (subject to any rules made by virtue of section 69(2)(i)) shall be confined, as the case may be, to either—
> (a) a statement that they have made a determination in his favour; or
> (b) a statement that no determination has been made in his fabour."

83. Section 69(1) provides for the Secretary of State to make rules governing the exercise of the IPT's jurisdiction. The rules (the *Investigatory Powers Tribunal Rules S.I. 2000/2665*) provide for a statement of reasons to be provided to a

complainant only where a complaint is upheld and this is subject to the obligation not to disclose any information that is contrary to the public interest to disclose:

> **"Disclosure of Information**
> **6.—(1)** The Tribunal shall carry out their functions in such a way as to secure that information is not disclosed to an extent, or in a manner, that is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of the United Kingdom or the continued discharge of the functions of any of the intelligence services.
> […]
>
> **Notification to the complainant**
> 13.—(1) In addition to any statement under section 68(4) of the Act, the Tribunal shall provide information to the complainant in accordance with this rule.
> (2) Where they make a determination in favour of the complainant, the Tribunal shall provide him with a summary of that determination including any findings of fact.
>
> (3) Where they make a determination:
> (a) that the bringing of the section 7 proceedings or the making of the complaint is frivolous or vexatious;
> (b) that the section 7 proceedings have been brought, or the complaint made, out of time and that the time limit should not be extended; or
> (c) that the complainant does not have the right to bring the section 7 proceedings or make the complaint;
> the Tribunal shall notify the complainant of that fact.
>
> (4) The duty to provide information under this rule is in all cases subject to the general duty imposed on the Tribunal by rule 6(1)."

84. The IPT rarely upholds complaints. The official figures are as follows:

Year	Complaints	Complaints Upheld
2012	168	0
2011	180	0
2010	164	6 (5 were joint complainants)
2009	157	1
2008	136	2
2007	66	0
2006	86	0
2005	80	2 (joint complainants)
2004	90	0
2003	110	0
2002	137	0
2001	95	0
TOTAL	**1469**	**11 (7 complainants were joint complainants in 2 cases)**

Sources: Hansard HC Debates, 23 April 2009: Column 858W;
Hansard HC Debates, 11 January 2010: Column 701W;
Annual Reports of the Investigatory Powers Tribunal (2010-2012);

Codes of Practice:

85. Section 71 RIPA requires the Secretary of State to issue Codes of Practice relating to the exercise and performance of the powers and duties under, *inter alia*, Chapters I and II of the Act. These Codes shall be taken into account by persons exercising the powers under the Act or by Commissioners or the IPT (s.72).

86. The Secretary of State has issued such codes, including the *Interception of Communications: Code of Practice* **[Annex 2/IB1/921]** and the *Acquisition and Disclosure of Communications Data: Code of Practice* **[Annex 3/1161-1222]**.

87. Chapter 6 of the *Interception of Communications* Code concerns "*Safeguards*". It states, *inter alia*, as follows:

> "6.1 All material (including related communications data) intercepted under the authority of a warrant complying with section 8(l) or section 8(4) of the Act must be handled in accordance with safeguards which the Secretary of State has approved in conformity with the duty imposed upon him by the Act. These safeguards are made available to the Interception of Communications Commissioner, and they must meet the requirements of section 15 of the Act which are set out below. In addition, the safeguards in section 16 of the Act apply to warrants complying with section 8(4). Any breach of these safeguards must be reported to the Interception of Communications Commissioner.
> […]
> *Dissemination of Intercepted Material*
> 6.4 The number of persons to whom any of the material is disclosed, and the extent of disclosure, must be limited to the minimum that is necessary for the authorised purposes set out in section 15(4) of the Act. This obligation applies equally to disclosure to additional persons within an agency, and to disclosure outside the agency. It is enforced by prohibiting disclosure to persons who do not hold the required security clearance, and also by the need-to-know principle: intercepted material must not be disclosed to any person unless that person's duties, which must relate to one of the authorised purposes, are such that he needs to know about the material to carry out those duties. In the same way only so much of the material may be disclosed as the recipient needs; for example if a summary of the material will suffice, no more than that should be disclosed." (emphasis added)

88. The latter Code provided guidance in relation to the provision of information *to* foreign agencies:

> "**Acquisition of communication data on behalf of overseas authorities**
>
> 7.11 Whilst the majority of public authorities which obtain communications data under the Act have no need to disclose that data to any authority

outside the United Kingdom, there can be occasions when it is necessary, appropriate and lawful to do so in matters of international co-operation.

7.12 There are two methods by which communications data, whether obtained under the Act or not, can be acquired and disclosed to overseas public authorities:

- Judicial co-operation
- Non-judicial co-operation

Neither method compels United Kingdom public authorities to disclose data to overseas authorities. Data can only be disclosed when a United Kingdom public authority is satisfied that it is in the public interest to do so and all relevant conditions imposed by domestic legislation have been fulfilled.

[…]

Non-judicial co-operation

7.15 Public authorities in the United Kingdom can receive direct requests for assistance from their counterparts in other countries.

These can include requests for the acquisition and disclosure of communications data for the purpose of preventing or detecting crime. On receipt of such a request the United Kingdom public authority may consider seeking the acquisition or disclosure of the requested data under the provisions of Chapter II of Part I of the Act.

7.16 The United Kingdom public authority must be satisfied that the request complies with United Kingdom obligations under human rights legislation. The necessity and proportionality of each case must be considered before the authority processes the authorisation or notice.

Disclosure of communications data to overseas authorities

7.17 Where a United Kingdom public authority is considering the acquisition of communications data on behalf of an overseas authority and transferring the data to that authority it must consider whether the data will be adequately protected outside the United Kingdom and what safeguards may be needed to ensure that. Such safeguards might include attaching conditions to the processing, storage and destruction of the data.

[…]

7.21 The DPA recognises that it will not always be possible to ensure adequate data protection in countries outside of the European Union […] and there are exemptions to the principle […] There may be circumstances when it is necessary, for example in the interests of national security, for communications data to be disclosed to a third party country, even though that country does not have adequate safeguards in place to protect the data. That is a decision that can only be taken by the public authority holding the data on a case by case basis." (emphasis added)

iii. The Data Protection Act 1998

89. The *Data Protection Act 1998* (c.29) ("the **DPA**") (see Annex 4) transposes into the law of the UK Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with

regard to the processing of personal data and on the free movement of such data (Official Journal of the European Communities, L.281 of 23.11.1995) ("**Data Protection Directive**"). The DPA applies to the "*processing*" of "*personal data*" of "*data subjects*", by "*data controllers*" or "*data processors*".

90. The "processing" of data includes (s.1(1)):

> "obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including … (b) retrieval, consultation or use of the information or data, (c) disclosure of the information or data by transmission, dissemination or otherwise making available…".

91. The Act's key principles (known as "*the data protection principles*"), are set out in Part I of Schedule 1 (s.4(1)), which must be interpreted in accordance with Part II of Schedule 1 (s.4(2)). The principal rule of the Act is that, "[…] *it shall be the duty of a data controller to comply with the data protection principles in relation to all personal data with respect to which he is the data controller*" (s.4(4)).

92. The data protection principles are, in summary (as set out in Schedule 1 of the DPA):

> "**1.** Personal data shall be processed fairly and lawfully;
> **2.** Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
> **3.** Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
> **4.** Personal data shall be accurate and, where necessary, kept up to date.
> **5.** Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
> **6.** Personal data shall be processed in accordance with the rights of data subjects under this Act.
> **7.** Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
> **8.** Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."

93. However, section 28 provides an exclusion in the context of national security matters:

> "**28.— National security.**
> (1) Personal data are exempt from any of the provisions of—
> (a) the data protection principles,
>
> (b) Parts II, III and V, and
>
> (c) sections 54A and section 55,
>
> if the exemption from that provision is required for the purpose of safeguarding national security.
>
> (2) Subject to subsection (4), a certificate signed by a Minister of the Crown certifying that exemption from all or any of the provisions mentioned in subsection (1) is or at any time was required for the purpose there mentioned in respect of any personal data shall be conclusive evidence of that fact.
> […]"

94. The Data Protection Directive itself provides in Article 13.1(a) for an exception in respect of measures necessary to safeguard national security. This reflects Article 4.2 of the Treaty on the European Union (Official Journal C 83/13) that "*national security remains the sole responsibility of each Member State*".

iv. The Human Rights Act 1998

95. Section 1 of the *Human Rights Act 1998* (see Annex 4) gives legal effect to Convention rights in UK law. It defines the Convention Rights as those scheduled to the Act, which include Article 8 ECHR. Section 2 requires a court or tribunal determining a question which has arisen in connection with a Convention right to take into account any judgment, decision, declaration or advisory opinion of this Court.

96. Section 3 requires that so far as it is possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with Convention rights. If, however, in any proceedings in which a court is determining whether a provision is compatible with a Convention right, and is satisfied that it is not, it may make a declaration of that incompatibility under section 4.

97. A declaration of incompatibility can only be made by the judicial bodies defined at s.4(5):

> "(5) In this section "court" means —
> (a) the Supreme Court;
> (b) the Judicial Committee of the Privy Council;
> (c) the Court Martial Appeal Court;
> (d) in Scotland, the High Court of Justiciary sitting otherwise than as a trial court or the Court of Session;
> (e) in England and Wales or Northern Ireland, the High Court or the Court of Appeal;
> (f) the Court of Protection, in any matter being dealt with by the President of the Family Division, the Vice-Chancellor or a puisne judge of the High Court."

98. Section 6 provides that it is unlawful for a public authority to act in a way which is incompatible with the Convention save in circumstances identified in section 6(2). A person who claims a public authority has acted or proposed to act in a way which is made unlawful by section 6(1) may bring proceedings against the authority under this Act in the appropriate court or tribunal.

v. The Justice and Security Act 2013

99. Section 10 ISA (repealed) established the ISC to oversee the work of the UKIS, including the three main intelligence agencies. The Committee was made up of Parliamentarians appointed by the Prime Minister but was not a Committee of Parliament. It was formally part of the Cabinet Office and was insufficiently independent to provide effective oversight.

100. In its 2010/2011 Annual Report the ISC undertook a "*root-and-branch*" examination of its powers, processes and the legislative framework and concluded that "*the current arrangements are significantly out of date and it is time for radical change. The status quo is unsustainable*" (§22). When examining the ISA, it concluded that "[t]*he legislation* […] *contains safeguards that – whilst they were thought necessary in 1994 – are now outdated* […]. *The 1994 Act therefore requires updating*" (§273).

101. Part I of the *Justice and Security Act 2013* ("**JSA**") (see Annex 4) has made some reforms. Section 1 provides:

> "**1.— The Intelligence and Security Committee of Parliament**
> (1) There is to be a body known as the Intelligence and Security Committee of Parliament (in this Part referred to as "*the ISC*").
>
> (2) The ISC is to consist of nine members who are to be drawn both from the members of the House of Commons and from the members of the House of Lords.
>
> (3) Each member of the ISC is to be appointed by the House of Parliament from which the member is to be drawn.
>
> (4) A person is not eligible to become a member of the ISC unless the person—
> (a) is nominated for membership by the Prime Minister, and
> (b) is not a Minister of the Crown.
>
> (5) Before deciding whether to nominate a person for membership, the Prime Minister must consult the Leader of the Opposition.
>
> (6) A member of the ISC is to be the Chair of the ISC chosen by its members."

102. Section 2 JSA identifies the functions of the ISC:

> **"2.— Main functions of the ISC**
> (1) The ISC may examine or otherwise oversee the expenditure, administration, policy and operations of—
> (a) the Security Service,
> (b) the Secret Intelligence Service, and
> (c) the Government Communications Headquarters.
>
> (2) The ISC may examine or otherwise oversee such other activities of Her Majesty's Government in relation to intelligence or security matters as are set out in a memorandum of understanding.
>
> (3) The ISC may, by virtue of subsection (1) or (2), consider any particular operational matter but only so far as—
> (a) the ISC and the Prime Minister are satisfied that the matter—
> (i) is not part of any ongoing intelligence or security operation, and
> (ii) is of significant national interest,
> (b) the Prime Minister has asked the ISC to consider the matter, or
> (c) the ISC's consideration of the matter is limited to the consideration of information provided voluntarily to the ISC (whether or not in response to a request by the ISC) by—
> (i) the Security Service,
> (ii) the Secret Intelligence Service,
> (iii) the Government Communications Headquarters, or
> (iv) a government department.
> (4) The ISC's consideration of a particular operational matter under subsection (3)(a) or (b) must, in the opinion of the ISC and the Prime

Minister, be consistent with any principles set out in, or other provision made by, a memorandum of understanding.

(5) A memorandum of understanding under this section—

(a) may include other provision about the ISC or its functions which is not of the kind envisaged in subsection (2) or (4),
(b) must be agreed between the Prime Minister and the ISC, and
(c) may be altered (or replaced with another memorandum) with the agreement of the Prime Minister and the ISC.

(6) The ISC must publish a memorandum of understanding under this section and lay a copy of it before Parliament."

103. Section 3 provides that the ISC must provide an annual report to Parliament, which it must send to the Prime Minister beforehand (s.3(3)) and which it must redact if the Prime Minister considers that sensitive information is at risk of being disclosed (s.3(4)).

104. Schedule 1 to the JSA sets out further rules concerning the ISC's procedures and constitution. Paragraph 4 also establishes the rules in relation to access to information by the ISC.

vi. Definition of "national security"

105. For the purposes of this Application, it is important to appreciate that English courts have taken an extensive view of the definition of "*national security*" which goes beyond the general international understanding of that term. In considering whether to make a warrant in the interests of national security, a British Minister will naturally apply the broad definition adopted by the English courts.

106. In *Secretary of State for the Home Department v Rehman* [2003] 1 AC 153 the House of Lords considered the question of what constitutes "national security" in UK law. The Special Immigration Appeals Commission had upheld Mr Rehman's appeal form a deportation order on the basis that in alleging that Mr Rehman was associated with an organization involved in terrorism activities on the Indian sub-continent, the Secretary of State had failed to show that he was a threat to the national security of the UK. The Court of Appeal and the House of Lords overturned this finding, holding

that the concept of "*national security*" is "*protean*" and a question of "*policy*" that falls to be determined by the Secretary of State. As such, under English law 'national security' is capable of including action taken to assist other countries to combat risks *to them* and therefore overlaps with foreign policy.

107. Giving the judgment of the Court of Appeal, Lord Woolf stated that the Government, "*correctly submitted that "national security" is a protean concept, "designed to encompass the many, varied and (it may be) unpredictable ways in which the security of the nation may best be promoted*"." (at §35).

108. Lord Slynn stated at §17 (at p.183A):

> "I would accept the Secretary of State's submission that the reciprocal co-operation between the United Kingdom and other states in combatting international terrorism is capable of promoting the United Kingdom's national security, and that such co-operation itself is capable of fostering such security "by, inter alia, the United Kingdom taking action against supporters within the United Kingdom of terrorism directed against other states". There is a very large element of policy in this which is, as I have said, primarily for the Secretary of State."

109. Lord Hoffmann stated at §53 (at p.193A):

> "The decision as to whether support for a particular movement in a foreign country would be prejudicial to our national security may involve delicate questions of foreign policy. And, as I shall later explain, I agree with the Court of Appeal that it is artificial to try to segregate national security from foreign policy. They are all within the competence of responsible ministers and not the courts."

110. The English courts have continued to rely upon this broad definition of national security, and went further to elide it with the concept of 'good foreign relations' in *R (Corner House) v Director of the Serious Fraud Office* [2009] 1 AC 756. That case concerned a decision to terminate a criminal investigation into serious allegations of bribery against a UK company involved in selling weapons to Saudi Arabia. The Saudi Arabian Government had indicated that the criminal investigation would adversely affect intelligence and diplomatic cooperation with the UK. The Court of Appeal accepted that this constituted a threat to national security. In the judgment of the Court at §139 it was stated:[21]

[21] The issue was directly addressed by the House of Lords, though see Baroness Hale at §53

> "National security is, to a significant extent, dependent upon co-operation with other states. That co-operation is dependent on fostering or maintaining good relations. … It is all too easy for a state which wishes to maintain good relations with another state whose official is under investigation to identify some potential damage to national security should good relations deteriorate, all the more so where that other state is powerful and of strategic importance."

111. During the recent parliamentary debates on the Justice and Security Bill, Baroness Manningham-Buller, the former Director General of the Security Service, explained that the UK Government's conception of what constitutes a threat to national security has considerably broadened and includes, for instance, action taken to combat pandemics and energy security:

> "When I joined the Security Service, national security meant to us something pretty narrow following the Attlee instructions at the end of the war to the intelligence community. It involved the military protecting the UK from the threat of military attack and the security and intelligence services protecting it from espionage, sabotage, terrorism and threats to parliamentary democracy from the extreme right and extreme left—fascism and communism. That understanding of national security, articulated in the Attlee declaration, informed the first tranche of legislation: the Security Service Act, the first Interception of Communications Act, the Intelligence Services Act and Regulation of Investigatory Powers Act. It was an understanding which certainly was not articulated in law but was well understood within the community.
> The previous Government—and I do not blame them for this—said, "Hold on, the security and safety of the citizen is much wider than these issues". Therefore they drew up, under the previous Prime Minister, a national security strategy which was much broader and included things such as pandemics and added cyberthreats, energy security and so on and this Government have built on that early national security strategy and now have quite a long national security strategy that covers a wide range of issues." (HC. Deb 17 July 2012 Hansard Col. 124)

112. Resisting efforts to define the term in the Bill, the Government Minister, James Brokenshire, stated that:

> "It has been the considered policy of successive Governments and the practice of Parliament not to define the term "national security". That is in order to retain the flexibility needed to ensure that the term can adapt to changing circumstances." (HC. Deb 31 Jan 2013 Hansard Col 130).

III. STATEMENT OF VIOLATIONS OF THE CONVENTION

A. Applicability of Article 8

113. This Application concerns two distinct but related interferences with the right protected by Article 8 ECHR. Firstly, in relation to receipt of foreign intercept. In that regard, the obtaining or receiving, analysis, use, storage and disposal of intercept data by UK agencies as part of the operation of secret surveillance constitutes an interference with an individual's private life: e.g. *Hewitt & Harman v UK* at [34]-[35]; *Liberty v United Kingdom* at [56]. Secondly, in relation to GCHQ's own generic intercept, obtaining this data is obviously an interference with Article 8, but so too is "*transmission of data to and their use by other authorities*". This constitutes a "*separate interference with the applicants' rights under Art.8*" (e.g. *Weber v Germany*, at [78]).

114. The present challenge relates to the inadequacies of the protection afforded by the legal regime in the UK which is said to govern these two strands of activity, which *prima facie* interfere with rights protected by Article 8 ECHR. For reasons set out in paragraphs 11-18 above, all the Applicants in this case have reasonable grounds for believing that they are likely to have been subject to generic surveillance by GCHQ and/or that the UK security services may be in receipt of foreign intercept which relates to their electronic communications.

115. In any event, in such circumstances, the Court has held that general challenges to the legislative regime under Article 8 are permitted:

> "… in recognition of the particular features of secret surveillance measures and the importance of ensuring effective control and supervision of them, the Court has permitted general challenges to the relevant legislative regime" (*Kennedy v United Kingdom* (2011) 52 EHRR [119], emphasis added)

The Applicants also bring this claim on behalf of others affected by the surveillance of which they complain.

116. The Applicants do not therefore need to establish that their communications have actually been the subject of interception or that their information has otherwise been obtained by agencies of the UK Government.

B. The Requirements of "in accordance with law" in this Context

117. The requirement that any interference with private life must be in "*accordance with the law*" under Article 8(2) will only be met where three conditions are satisfied. First, the measure must have some basis in domestic law. Secondly, the domestic law must be compatible with the rule of law and thirdly the person must be able to foresee the consequences of the domestic law for him.

118. In the context of interception of communications by a security service, the Court has recognised (e.g. in *Kennedy* at [152]) that such surveillance is necessarily secret, so the requirement of foreseeability cannot mean the ability of an individual to foresee precisely whether or not he or she will be subject to surveillance or the precise terms which will be used to determine subjects of surveillance. However, what is required is a framework which enables a citizen to understand with sufficient particularity the types of person and conduct in relation to whom surveillance may occur; the safeguards which exist and govern dissemination and sharing of such material; the framework which exists to guard against arbitrary or disproportionate use of such material; and checks on the authority required to permit such surveillance and limits on the time for which such surveillance may occur. What is required is a legal framework which provides an ascertainable check against arbitrary use of secret and intrusive state surveillance.

C. Why Receipt of Foreign Intercept Material by the United Kingdom is not 'in accordance with the law'

i. Absence of Sufficient Legal Basis

119. The receipt, analysis, use and storage of data received from foreign intelligence agencies that has been obtained by interception do not have an adequate basis in UK law.

120. In his statement to Parliament on 10 June 2013, the Foreign Secretary asserted that such a legal basis exists in domestic law. He said that "*any data obtained*" from third countries relating to UK nationals was subject to "*statutory controls and safeguards*" (above §41-45). He identified sections 15 and 16 of RIPA; the HRA and the ISA. The ISC made a similar statement (above §49-50). In a letter to the First and Second Applicants, the UK Government has also identified the DPA.

121. However the legal provisions identified fail to provide any basis for the regulation of the receipt of information from foreign intelligence agencies:

121.1. Sections 1 (SIS) and 3 (GCHQ) of the ISA and section 1 of the *SSA 1989* (Security Service) provide powers for those agencies to "obtain and provide" information, including to and from foreign intelligence services. However, the legal safeguards which attend those powers are very limited. There is no direct legal control on the purposes for which they may be used other than that the heads of the agencies are under duties to ensure that there are arrangements for securing that no information is obtained except insofar as "necessary" for purposes specified in s2(2)(a) and s4(2)(a) ISA and s.2 SSA 1989 respectively.

121.2. However, these purposes are extremely broadly defined. For the Chief of SIS, they include (a) the purposes of discharging the functions of SIS; (b) the interests of national security; (iii) for the purposes of prevention or detection of serious crime; or "*for the purposes of any*

criminal proceedings" (emphasis added). The functions of the SIS are obtaining and providing information in the interests of national security, the economic wellbeing of the UK, or in support of the prevention or detection of serious crime. For the Director-General of the Security Service they include (a) the purposes of discharging the functions of the Security Service; (b) the purposes of (i) the prevention or detection of serious crime or (ii) "*the purpose of any criminal proceedings*". (The breadth of the concept of national security is addressed below.)

121.3. The legal framework contains no check on the Chief of SIS or the Director-General's assessment of what may be regarded as "necessary". For example, neither needs a warrant to receive material.

121.4. Nor do the ISA, SSA give any information as to what the "*arrangements to secure*" that no information is obtained for unlawful purposes should consist of, or how any person is to establish if such arrangements exist. Unlike the position in relation to an individual warrant, it is hard to see why a person should not be able to know what the arrangements are to safeguard against arbitrariness or misuse of this secret power to obtain information. There are no Codes of Practice that regulate this power.

121.5. Contrary to what the UK Government suggests, Chapter 1 of RIPA does not apply to the receipt of intercept evidence from the NSA. Its provisions are restricted to interception of communications by UK authorities. The Foreign Secretary expressly referred to sections 15 and 16 of RIPA. However these sections set out restrictions on the interception of communications contained in Chapter I of RIPA which do not apply. Moreover, contrary to the apparent suggestion of the ISC (§50 above) there is no requirement for a warrant for the receipt of such information under Chapter 1 of RIPA.

121.6. Chapter 2 of RIPA also does not apply to the receipt of intelligence from foreign agencies as it only concerns "*communications data*", which is defined in section 21(4) of the Act as data which is held by a person providing a telecommunications service (i.e., usually, metadata). Moreover, the power relates to obtaining information from a "*postal or telecommunications operator*": s.22(4), 25(1). Foreign Government agencies are not postal or telecommunications operators.[22]

121.7. Although the Treasury Solicitor on behalf of the UK Government has also claimed that the DPA provides protections (above at §46), that statute contains an explicit exemption from the data protection principles in the context of processing data in the interests of national security (section 28). The Treasury Solicitor's reference to this legislation does not, therefore, identify any basis in law for the regulation of the receipt and use of communications, as required by Article 8.

121.8. Article 8 of the Convention, as given effect by the HRA, does not itself prescribe any law regulating how information is procured, received, stored, disseminated, used or disposed of. On the contrary, Article 8 has been interpreted as requiring that domestic legislation sets out such restrictions in an open and transparent form: *Halford v UK* 1997 24 EHRR 523, *Khan v UK* (2001) 31 EHRR 45, *Liberty v UK* (2009) 48 EHRR 1; *Kennedy v UK* (2011) 52 EHRR 4.

122. The consequence is that in UK law there is an absence of legislative controls or safeguards in relation to:

122.1. The circumstances in which UKIS can request foreign intelligence agencies to intercept communications to provide information to UKIS.

[22] Further, the data which has been supplied by the NSA is content data as well as metadata. It includes, for example, information about internet users' search history and the content of their e-mails. Chapter II only applies to metadata.

122.2. The circumstances in which UKIS can request access to stored data held by foreign intelligence agencies that has been obtained from interception.

122.3. The extent to which UKIS can use, analyse, disseminate, store (etc) intercept data solicited and/or received from foreign intelligence agencies and the circumstances in and process by which such data must be destroyed.

123. The Foreign Secretary's refusal to provide any answer to the two questions asked by the Rt. Hon. Douglas Alexander MP (§§42-45 above) reinforces the conclusion that *if* any regulations or guidelines exist in relation to (a) requests of foreign Governments to carry out interception of communications under their law (the first question); and (b) requests for information held by foreign Governments (the second question), such provisions are secret and unpublished.

124. The absence of legal safeguards is particularly concerning in the context of the receipt of data such as that obtained under the PRISM and UPSTREAM programmes, because US law itself contains no significant safeguards in relation to communications outside the US not relating to US persons (see statement of Cindy Cohn at §§54-55, 60 **[Annex 1/87-88, 90]**).

125. In these circumstances the requirements that an interference with Article 8 rights be 'in accordance with the law' are not made out.

126. In *Halford v United Kingdom* (1997) 24 EHRR 523 §50-51 a telephone interception was held not to be in accordance with law because "*domestic law did not provide any regulation of the interceptions of calls made*". In *MM v United Kingdom*, App. No. 24029/07 13 November 2012, the Court described its finding in *Khan v. the United Kingdom*, no. 35394/97, § 27, ECHR 2000 V as a case where it found a violation of Article 8 *"because there existed no statutory system to regulate their use and the guidelines applicable at the relevant*

time were neither legally binding nor directly publicly accessible". These observations are directly applicable.

127. In its report in July 2013 the ISC recognised that there is a question as to whether "*the current statutory framework … remains adequate*". It drew attention to the fact that in some areas the legislation was "*expressed in general terms and more detailed policies and procedures*" have had to be put in place (above §50-52). These concerns, although grossly understated, represent an implicit acknowledgement of the absence of applicable safeguards in the governing statutory regimes.

ii. Quality of Law

128. In *Telegraaf Media Nederland Landelijke Media BV v The Netherlands*, App. No. 39315/06, 22 Nov 2012, the Court summarised the law at §90:

> ""in accordance with the law" not only requires the impugned measure to have some basis in domestic law, but also refers to the quality of the law in question, requiring that it should be accessible to the person concerned and foreseeable as to its effects. The law must be compatible with the rule of law, which means that it must provide a measure of legal protection against arbitrary interference by public authorities with the rights safeguarded by Article 8 § 1 and Article 10 § 1. Especially where, as here, a power of the executive is exercised in secret, the risks of arbitrariness are evident. Since the implementation in practice of measures of secret surveillance is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power."

129. It follows that,

> "the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference (see *Weber and Saravia*, cited above, §§ 93-95 and 145; *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, § 76, ECHR 2006-VII; *Liberty and Others v. the United Kingdom*, no. 58243/00, §§ 62-63; 1 July 2008; *Kennedy v. the United Kingdom*, no. 26839/05, § 152, 18 May 2010)."

130. For the reasons given above, UK law does not comply with these requirements insofar as it relates to the receipt of information from foreign intelligence partners, that has been obtained by means of interception. The discretion to obtain, retain and share the product of foreign intercept gives

the individual inadequate protection against arbitrary and disproportionate interference with his right to respect for private life.

131. There are, moreover, no restrictions on the UKIS by-passing the legal safeguards required in respect of the interception of communications data set out in Chapter 1 of RIPA, by obtaining information derived from interception from foreign agencies, such as the NSA, even where this could have been obtained by the UK agency pursuant to a warrant under sections 5 and 8(1). Indeed, RIPA actually encourages UK agencies to consider this: section 5(5) requires that when considering whether a warrant is necessary, consideration must be given to "*whether the information … could reasonably be obtained by other means*."

132. The ISC report stated that "*in each case where GCHQ sought information from the US*" a UK warrant had also been issued, presumably in relation to specific individuals within the UK (above §49). This appears to have been entirely fortuitous, and is not said to be the product of any legal requirement. Moreover, the warrant would not, of course, have extended to or necessarily referred to the receipt of information from US intelligence services and therefore could not have imposed any restrictions on the receipt or use of such material. Indeed, the warrant may have been restricted in ways that could be by-passed by the method of obtaining information on a target from the PRISM or UPSTREAM programmes. In short, the fact that warrants may have been in place in relation to individuals who were the subject of specific requests for information from the NSA does not provide any comfort that adequate restrictions are in place on the obtaining and use by the UKIS of material from the NSA or other foreign intelligence agencies. See further Witness Statement of Ian Brown at §20 **[Annex 2/516-517].**

133. Insofar as there are any safeguards in place relating to receipt of information from foreign agencies these are unpublished. The UK Government has refused to provide any details about the internal

procedures that apply. In *Liberty v UK*, the Court noted, in finding a violation of Article 8, that:

> "66. … According to the Government (see paragraphs 48-51 above), there were at the relevant time internal regulations, manuals and instructions applying to the processes of selection for examination, dissemination and storage of intercepted material, which provided a safeguard against abuse of power. The Court observes, however, that details of these "arrangements" made under section 6 were not contained in legislation or otherwise made available to the public.
>
> 67. The fact that the Commissioner in his annual reports concluded that the Secretary of State's "arrangements" had been complied with (see paragraphs 32-33 above), while an important safeguard against abuse of power, did not contribute towards the accessibility and clarity of the scheme, since he was not able to reveal what the "arrangements" were. In this connection the Court recalls its above case-law to the effect that the procedures to be followed for examining, using and storing intercepted material, *inter alia*, should be set out in a form which is open to public scrutiny and knowledge."

134. In *MM v United Kingdom*, op cit, the Court stated:

> "194 In *Malone*, cited above, §§ 69-80, it found a violation of Article 8 because the law in England and Wales governing interception of communications for police purposes was "somewhat obscure and open to differing interpretations" and on the evidence before the Court, it could not be said with any reasonable certainty what elements of the powers to intercept were incorporated in legal rules and what elements remained within the discretion of the executive. As a result of the attendant obscurity and uncertainty as to the state of the law the Court concluded that it did not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities (see also *Liberty and Others*, cited above, §§ 64-70).
>
> 195. The Court considers it essential, in the context of the recording and communication of criminal record data as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures; as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness (see *S. and Marper*, cited above, § 99, and the references therein).

135. None of these requirements of Article 8 have been complied with in this case.

136. There is only one context in which policies relating to the use and receipt of foreign intelligence have been made published: the *Consolidated Guidance* regulating the procurement and receipt of information from foreign

intelligence agencies in the context of risks of torture and other serious human rights abuses. This was drawn-up and published following allegations of UK complicity in torture and ill-treatment of detainees after the terrorist attacks on 11 September 2001 (above §78). This detailed policy sets out, for instance, the circumstances in which approval for the receipt of information obtained from a person held in foreign custody, or where such information is solicited. However, this policy is limited and does not extend to the receipt of information obtained by foreign intelligence agencies by intrusive intercept or surveillance, such as under section 702 of FISA.

137. Furthermore, there is no effective oversight of the receipt, use, storage etc. of information so obtained:

137.1. The Intelligence Services and the Interception of Communications Commissioners' jurisdictions are limited to assessing compliance with certain provisions of RIPA and, in the case of the former, the *Consolidated Guidance*. The Prime Minister could widen the remit of the Intelligence Commissioner's jurisdiction to cover receipt of information from foreign interception, but he has not done so. Moreover, the findings of their reports are not binding.

137.2. The ISC's jurisdiction is also limited. It had never addressed the issue in any of its reports until the PRISM information was make public in the UK and US media. Indeed, it appears that it was not aware of it (see Witness Statement of Ian Brown §45 **[Annex 2/527-528]**). Its function is reactive, and it does not approve or even necessarily know about, the matters that are the subject of complaint in these proceedings. Moreover, its report demonstrates the severe limitations on the ISC's role and function. In particular,

a. The ISC failed to identify with any clarity what legal provisions it considers to be applicable, other than a general reference to the ISA, the HRA and RIPA.

b. It did not identify any internal processes or safeguards, relating to authorization, storage, dissemination, disposal etc. of data. Nor were such issues identified in its report even in general terms.

c. It did not provide any reasoned basis for its conclusion that GCHQ had complied with its statutory duties or for its conclusion that it had not "*circumvented or attempted to circumvent*" UK law.

d. It did not invite or consider any representations other than those of the Intelligence Services and the NSA.

e. It is a Committee made up of Members of Parliament who are not themselves necessarily lawyers (and who are not judges) and therefore not in a position to pronounce authoritatively on the legality of GCHQ's practices.

f. It chose not to examine the conduct of SIS or the Security Service despite the fact that it is such agencies that are likely to have principal responsibility for using the data received by GCHQ, and being in a position to obtain information from foreign agencies themselves. There is no means of requiring the ISC to examine such matters.

For these reasons, the ISC's jurisdiction is clearly incapable of compensating for clear and published legal safeguards.

138. The IPT likewise does not provide any sufficient legal protection. The limits role are address at paragraphs 171-173 below.

139. In summary, there is no legislation (or other legal provisions) in the UK that can be said to "*give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort*" to the measures referred to (*Uzun v Germany* (2012) 54 EHRR 121).

D. Breach of Article 8 in Respect of Generic GCHQ Intercept on the Basis of Non-Specific Blanket, Rolling Warrants for Interception of External Communications

i. Quality of Law

140. Although RIPA section 8(1) and (2) sets out protections and requirements for targeting of interception warrants, section 8(4) of RIPA dis-applies the protections in subsections 8(1) and 8(2) to external communications. External communications are defined as those sent or received outside the UK, whether or not they relate to British nationals. Section 8(4) thus permits, what has been described as generic intercept of communications, simply on the basis of the means by which it happens to have been transmitted.

141. The TEMPORA programme has been established under warrants issued under RIPA section 8(4) relating to external communications. As explained above, this programme involves GCHQ accessing all external communications passing along transatlantic fibre-optic cables without restriction. Media reports (set out in Dr Brown's evidence at §52 **[Annex 2/ 531]**) indicate that this surveillance is undertaken on the basis of ten generic warrants. The authority for this GCHQ generic surveillance is apparently renewed at six monthly intervals.

142. Whether taken separately or together, the effect of the following features of the statutory regime that applies to external communication warrants is that it is not compliant with Article 8:

142.1. The restrictions and safeguards that apply to internal warrants are not applicable to external warrants.

142.2. They are not approved by a judge or an authority that is independent of the UKIS whether before or after they have been issued and / or the oversight regime does not provide an adequate

guarantee that interception and use of the data does not go beyond what is strictly necessary.

(a) Insufficiency of statutory restrictions and safeguards

143. The Court has developed the following "*minimum standards*" that should be set out in "*statute law*" as "*clear, detailed rules*", rather than internal or other forms of law; (i) the nature of the offences which may give rise to an interception; (ii) a definition of the categories of people liable to have their communications intercepted; (iii) a limit on the duration of interception; (iv) the procedure to be followed for examining, using and storing the data obtained; (v) the precautions to be taken when communicating the data to other parties; (vi) the circumstances in which communications must be destroyed. See *Weber* at [92] and [95]. See also *Huvig v France* (1990) 12 EHRR 528; *Aman v Switzerland* (2000) 30 EHRR 843; *Valenzuela Contreras v Spain* (1999) 28 E.H.R.R. 483; and *Prado Bugallo v Spain* (App. 58496/00, 18 February 2003).

144. Whilst there are some, minimal, statutory conditions applicable to external communications warrants, upon analysis and as demonstrated by the public disclosures about the TEMPORA regime, the provisions of RIPA fail to comply with the requirements of Article 8.

145. First, the requirements of targeting on a person or place set out in sections 8(1)-(3) are disapplied. Section 8(4) therefore permits, "*blanket strategic monitoring*" of communications where at least one sender or recipient of the communication is outside the British Isles: C. Walker, *Terrorism and the Law* (OUP, 2011) at [2.58] p.70 [**Annex 3/1155-1156**].

146. Secondly, whilst the Secretary of State is required to provide "*the descriptions of material the examination of which he considers necessary*"(s.8(4)(b)(i)) there are no limits on the breadth of this description. The description could therefore be that of "all traffic passing along a specified cable running between the UK and the US": see Ian Brown §52

[Annex 2/531]. It does not have to be limited to particular individuals, a particular group, a particular threat or a particular time period. In practice, all communications are being intercepted, as if the UK Government was opening every letter that was sent from or passed through the British Isles. This is no different to the breadth of descriptions under the previous legislation, examined in the *Liberty* case (at [64]).

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

147.1. The UK courts have described the concept of national security as "*protean*" and have accepted a very broad definition that includes damage to international relations. They have held that it overlaps with foreign policy and that there is a very large area of discretion for the Government to determine what constitutes action that is in the interests of national security (see §§107-110 above). For its part, the UK Government has afforded an increasingly wide meaning to the concept of national security and has indicated that it will not provide any definition because it should be able to adapt to changing circumstances (see §§111-112 above). As such, the concept of national security, as a matter of UK law, is obscure, not defined in law or in policy, and its scope and application are vague and unforeseeable.

147.2. The effect is that UKIS can intercept communications and use such communications for purposes that go far wider that the protection of the UK against threats of terrorism, espionage or military action. It appears to be capable of being used, for example, to assist foreign

Governments in order to maintain good relations with them, or to advance the UK's policy in relation to protection from disease. There is no requirement that the individuals whose communications are intercepted and analysed are suspected of any conduct which amounts to a crime in the UK or are directed at the UK.

147.3. In Kennedy v UK, the Court held that the term "*national security*" had an understood meaning and, for instance, was used in the Convention itself (at [159] cf. the criticism of the term in Liberty v UK at [65]). However, with respect, the Court in that case did not consider the authorities referred to in §§107-110 above, or the stated position of the UK Government referred to at §§111-112. Reliance was placed on a definition offered by the Interception of Communications Commissioner in his Annual Report for 1986, which (i) is not authoritative or binding and, (ii) which is out of date. It is not the case that national security has any understood meaning in UK law and, on the contrary, is deliberately vague and 'protean'.

147.4. Furthermore, the definition of "*serious crime*" is insufficiently clear to enable subjects to know the type of activity which may attract authority to intercept or subject to surveillance.

148. Fourthly, whilst section 9(1) provides for the expiry of an interception warrant unless renewed, in practice this is no control on warrants for blanket strategic warrants, which will always be renewed as they are not based on any particular individuals or specific threat, but general threats to national security (etc): Ian Brown §53 **[Annex 2/531]**. As in the case of Gillan and Quinton v UK (2010) 50 EHRR 45, (at [81]) the alleged statutory temporal restriction has failed, so that a "*rolling programme*" of indefinite authorisation is effectively in place.

149. Fifthly, the "*general safeguards*" contained in section 15 RIPA are of very limited scope. They require the Secretary of State to ensure that arrangements are in place to secure that the number of persons to whom

intercepted material is disclosed and the extent of copying is "*limited to the minimum that is necessary for the authorised purposes*": section 15(1), (2). The material must be destroyed if there are no longer grounds for retaining it for "*authorised purposes*": s.15(3) However, "*authorised purposes*" are extremely wide (s.15(4)) and include where the information is or "*is likely to become*" necessary for any of the purposes specified in s.5(3). These include the interests of national security.

150. Thus, information can be used for any purpose relating to national security and can be kept even if it is not of any current utility. Moreover, it does not require the continuing or future utility of the information to be connected to the particular basis on which it was obtained, but can be retained so long as it is thought likely to be of any future utility to national security in general. There is also no requirement, in RIPA or the Code, which stipulates when the material should be reviewed (the Code refers to review "*at appropriate intervals*" §6.8).

151. Sixthly, the "*safeguards*" contained in section 16 are limited in scope to protecting persons who are within the British Isles who are the intelligence target by limiting the reach of a section 8(4) warrant with respect to such persons. Section 16 is intended to ensure that material obtained under a section 8(4) warrant is not examined if it is material that could be obtained by obtaining a section 8(1) warrant (i.e. it is material relating to an individual in the British Isles). However, section 16:
    - imposes no restrictions on the interception or examination of data that has been sent by a person in the UK where the examination is not targeted at that person – the communications of persons who are communicating *with* the target from within the UK can be freely examined so long as this falls within the general umbrella of "national security".
    - imposes no restrictions on the examination of personal data of persons not present in the UK, whether they are British citizens or citizens of other states, including where the selection of data is targeted at them.

- permits (by section 16(3)) the examination of material targeted at a person in the UK—that is, material that could be obtained by a warrant under section 8(1)—where the Secretary of State certifies this is necessary for national security for a permitted maximum period of 6 months. No guidance is given as to how the Secretary of State will assess such "necessity".
- The implications of these points are made clear in the evidence of Ian Brown at §§40-42, 53-55 **[Annex 2/524-526; 531-532]** and by the examples he gives.

152. It is therefore clear that the "*safeguards*" in RIPA that relate to external warrants are manifestly deficient. The broad nature of "national security" means that they do not define with any precision the nature of the offences which may give rise to an interception or examination of communications or the categories of people liable to have their interceptions intercepted. There is no effective limit on the interception and the law does not set out the procedure to be followed for examining the communications or the precautions to be taken when supplying them to third parties, such as the NSA. The circumstances in which the communications must be destroyed, whilst specified, are so broad as to effectively permit the retention of enormous amounts of intercepted information.

153. This Court's judgment in *Liberty v UK* points strongly to the provisions under consideration being incompatible with Article 8. In that case, the Court considered the analogous provisions under section 3(2) *Interception of Communications Act 1985* ("ICA") relating to external communications which applied before RIPA came into effect (described in the Court's judgment at §§22-27). Those provisions were in materially identical terms to RIPA and in two respects were more protective.[23]

[23] Section 3(3) of the ICA contained an additional limitation on an external interception warrant: such a warrant could not specify an address in the in the British Isles for the purposes of including communications to or from that address in the certified material, unless,

> "3(3)(a) [T]he Secretary of State considers that the examination of communications sent to or from that address is necessary for the purpose of preventing or detecting acts of terrorism; and
> (b) communications sent to or from that address are included in the certified material only in so far as they are sent within such a period, not exceeding three months, as is specified in the certificate."

154. The Court held that the provisions of the ICA relating to interception of external communications were insufficient to comply with Article 8. The Court first accepted that the power to intercept external communications contained in section 3(2) (now RIPA s.8(4)) "*allowed the executive an extremely broad discretion*" (at §§64-65). Warrants could cover "*very broad classes*" of communication such as all submarine cables having one terminal in the UK carrying external communications to Europe (or the United States). Thus any person who sent or received any form of telecommunication outside the British Isles could have such communication intercepted. The discretion granted was, therefore, "*virtually unfettered*". Precisely the same reasoning applies in this case.

155. Following the judgment in *Liberty v UK*, the Joint Parliamentary Committee on Human Rights wrote to the Home Secretary asking what steps the Government was taking to comply with the judgment and, moreover, whether it was satisfied that the new legislation, RIPA, had rectified the deficiencies identified by the European Court on Human Rights. The Home Secretary's response stated that he was satisfied that RIPA together with the Code of Practice rectified the defects but that it would continue to keep the matter under review.

156. The Joint Committee on Human Rights also asked **[Annex 3/1157-1159]**:

> "In particular, is the Government is satisfied that publicly accessible information on the current procedure for "selecting for examination, sharing, storing and destroying intercepted material" is available, and if so where can it be found?"

157. The Home Secretary's answer was that, "*Information is found with the Act itself, the code of practice, and the Interception Commissioner's annual reports*."

158. However, as explained above, RIPA is in material the same effect in relation to external communications as was the legislation at issue in *Liberty v UK*,

---

Furthermore, the maximum period that material targeted on a person in the British Isles could be examined pursuant to an external communications warrant was three months (rather than six months) in national security cases.

and the Court in that case also dismissed the Interception Commissioner's Annual reports as being capable of rectifying the deficiencies in the legal regime (at §67).

159. There is, in any event, no reference in the Commissioner's annual reports to the TEMPORA programme. The question therefore arises whether the Code of Practice, issued under section 71 of RIPA, is sufficient to compensate for the deficiencies in the legal regime in *Liberty v UK*. The answer to that is clearly that it is not.

160. Chapter 5 of the Code relates to external warrants. Much of Chapter 5 sets out the provisions of the RIPA. It does provide some additional requirements which, in the context of targeted warrants, might be of some protection to innocent individuals affected by a warrant, such as that applications for a warrant must identify any "*unusual degree of collateral intrusion*": §5.2. However these are not of any protection in the context of warrants issued under section 8(4): Ian Brown §53 **[Annex 2/531]**.

161. The Code does not require search terms to be set out or information that could indicate the extent of a data trawl that will be involved. Nor is there any restriction on search terms being specified by foreign intelligence partners such as the NSA or search results being shared with them. There is no process for the approval of search terms or the oversight of the use of the authorization given under section 8(4) by intelligence operatives in the UK or in foreign agencies. There is thus, "*a lack of regulations specifying with an appropriate degree of precision the manner of screening of the intelligence obtained through surveillance….*": *Association for European Integration and Human Rights v Bulgaria* (App. No. 62549.00, 28 June 2007), §86.

162. Chapter 6 of the Code sets out conditions on storage, dissemination and destruction of information but these do not impose any limits on the scope and duration of the warrants.

163. In *Kennedy v UK* the Court considered RIPA in the context of *internal* communications. It found that those provisions did not violate Article 8. However at §160 and §162 the Court made clear that its reasoning was limited to internal communications. Central to its conclusion was that,

> "in internal communications cases, the warrant itself must clearly specify, either by name of by description, one person as the interception subject or a single set of premises as the premises in respect of which the warrant is ordered. Names, addresses, telephone numbers and other relevant information must be specified in the schedule to the warrant. Indiscriminate capturing of vast amounts of communications is not permitted under the internal communications provisions of RIPA." (at [160], emphasis added).

164. The RIPA regime relating to interception of external communications remains, therefore, defective and insufficient to comply with Article 8 in that "*indiscriminate capturing of communications*" is permitted. Adequate changes have not been made since *Liberty v UK*.

(b) Absence of independent authorization / effective oversight

165. As the Court recently reaffirmed in the *Telegraaf Media* case, op cit at §98, "*[i]n a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge*". In an appropriate context, and where other safeguards are sufficient, the Court has been prepared to accept that "*independent supervision*" is adequate.

166. In *Klass and Others v Germany* (1978) 2 EHRR 214, the Court held that the practice of seeking prior consent for surveillance measures from the G10 Commission, an independent body chaired by a body chaired by a president who was qualified to hold judicial office and which had power to order immediate termination of the measure, was adequate. The Commissioners under RIPA are not comparable to this practice. Indeed, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (Frank La Rue), in a report to the UN Human Rights Council in April 2013, recently noted the lack of judicial oversight in the UK (at §54) and the attendant risk of "*de facto* [] *arbitrary*

approval of law enforcement requests" (UN Doc. A/HRC/23/40 at §56 **[Annex 2/IB1/1016]**).

167. Given the inadequate nature of the safeguards, as set out above, in this context only judicial approval of an external communications warrant could satisfy Article 8. But in any event, there is no approval of such warrants before or after they have been issued. It is a matter that is entirely within the province of the executive.

168. The approach taken under RIPA is also to be contrasted with the approach taken in the US under FISA. Whilst the regime also suffers from deficiencies, it is at least the case that external communications interceptions under section 702 of FISA are subject to approval by the FISA Court, an independent judicial body, as described in the witness statement of Ms Cindy Cohn §39 **[Annex 1/82]**

169. In *Kennedy*, this Court was impressed by the ability for warrants to be challenged in the IPT and the oversight offered by the Interception of Communications Commissioner. However, at least in the context of external warrants, such protections cannot satisfy the requirements of Article 8 (§§166-167).

170. The role of the Interception of Communications Commissioner is supervisory and he has no powers to prohibit or quash an interception warrant. It relates to all bodies who have powers to intercept communications and not just to the UKIS [24]. He examines, *ex post*, warrants on a random basis. There is no evidence that the Interception of Communications Commissioner has ever examined the TEMPORA programme and he has not set out any conditions on the use and examination of material obtained from bulk collection of all external communications. Whilst the Commissioner fulfills a valuable 'watchdog'

[24] As the Special Rapporteur noted in April 2013, "over 200 agencies, police forces and prison authorities are authorized to acquire communications data under the Regulation of Investigatory Powers Act, 2000. As a result, it is difficult for individuals to foresee when and by which State agency they might be subjected to surveillance" (A/HRC/23/40) (§56) **[Annex 2/IB1/1003-1055]**.

role, he cannot be said to compensate for the absence of judicial or independent authorisation of extremely intrusive interception warrants, particularly in the context of external communications that are subject to minimal statutory conditions and limitations.

171. The IPT does have the power to quash an interception warrant or require data to be destroyed. However, it does not constitute a substitute for independent approval of external communications warrants. Under section 65(2) of RIPA the jurisdiction of the tribunal is limited to determining complaints referred to them by members of the public. Since the granting of external communications warrants under section 8(4) such as under the TEMPORA system are not disclosed, individuals are not in a position to challenge such warrants. It is only in the highly unusual circumstances of a leak of information relating to such a warrant that the tribunal could be seized of the matter; and in such a case the individuals whose communications have in fact been examined would not know of this or be likely to challenge it.

172. Indeed, notwithstanding the leaks relating to the TEMPORA programme, the UK Government has refused to confirm or deny the existence of the program or provide any information about external communications warrants granted (in contrast to the approach of the US Government in respect of the PRISM programme).

173. Furthermore, other than a very small number of judgments relating to points of law, the IPT has not published any of its 1469 determinations. Where it dismisses a complaint—as it has done in all but 7 of the cases (see §84 above) —it is precluded from giving any reasons for its decision: RIPA section 68(4) and IPT Rules s.13(1). If it upholds a complaint, its reasons must not reveal any information that is contrary to the public interest which, given the UK Government's policy of neither confirming or denying the existence of any interception warrants obtained by UKIS, would in all likelihood mean that no reasons would be given for such a finding.

174. Nothing which is publicly available suggests that there are any safeguards on the use or further dissemination of data which GCHQ has intercepted and which it or the UK security services share with the NSA or others, who are not themselves bound by Convention standards.

175. Finally, the ISC has not examined the TEMPORA issue. Pursuant to section 2(1) JSA, the ISC has limited authority to examine ongoing operational matters. Its report in July 2013 was limited to consideration of the issue of receipt of information from the PRISM programme by GCHQ.

ii. Generic GCHQ intercept of external communications:
Lack of proportionality

176. The generic GCHQ intercept of external communications merely on the basis of the happenstance that they have been transmitted by transatlantic fibre-optic cables is an inherently disproportionate interference with the private lives of the thousands - perhaps millions - of people whose private data has been intercepted and examined by the UKIS for no better reason than its means of transmission.

177. The following are all facts and matters which illustrate the obvious disproportionality of the generic interception of external communications:

177.1. The absence of safeguards analogous to those set out in section 8(1) and 8(2) RIPA in relation to intercept of internal communications, which require authorisation to be targeted on a particular individual or individuals or premises;

177.2. The absence of sufficiently precise criteria for determining when intercepted external communications will be further analysed does not allow such intercept to be used only for targeted and sufficiently important purposes;

177.3. The excessive number of search terms reportedly used and persons reportedly with access to TEMPORA material is inherently disproportionate and the absence of any limits on these or who may supply or authorise them in the legislation;

177.4. Intercept of communication simply because of the means by which it has been transmitted is excessively broad and insufficiently linked with the ostensible purposes for which such intercept occurs. For example, communications sent by persons and from locations not under suspicion are intercepted and then subjected to the search machinery, rendering their communications liable to be further analysed, reported upon and subject to further action;

177.5. Generic external intercept occurs on the basis of an over-broad definition of national security which elides the concept with 'good international relations';

177.6. There are no sufficiently clear safeguards to guard against abuse of the power to intercept and use external communications data either by GCHQ or by foreign security service counterparts, some of whom have been granted direct access to TEMPORA material, who may not be bound by Convention standards; and

177.7. There is no judicial oversight of this process or other satisfactory independent accountability for the reasons set out above.

178. In effect, the power to obtain and use external communications data by means of intercept is unfettered in published law, as long as it is thought broadly to be in the interests of nation security or other of the specified generic purpose. There are no adequate criteria by which a court or tribunal could assess the legality of use of any particular intercept material even if the courts had jurisdiction to do so, which they do not.

IV. STATEMENT RELATIVE TO ARTICLE 35 (1) OF THE CONVENTION

179. The Applicants do not have any effective remedy for the complaints raised in this application in the UK.

180. The first two Applicants sought to bring a claim in the Administrative Court of England and Wales challenging the UK Government's reliance on sections 1 and 3 of the ISA as providing the legal basis for receipt and use of information from foreign intelligence partners. They contended that those provisions provide insufficient protection to comply with Article 8 of the Convention.

181. As required by the UK's Civil Procedure Rules, they sent a "*pre-action protocol*" letter to the UK Government on 3 July 2013 setting out the complaints raised herein and seeking declarations of incompatibility under section 4 of the HRA relating to inadequacies in sections 1 and 3 of the Intelligence Services Act, section 1 of the Security Service Act and/or section 8 of RIPA **[Annex 3/1056-1079]**.

182. In a letter of response dated 26 July 2013 **[Annex 3/1081-1083]**, the UK Government stated that the Applicants could not bring any complaint before the UK courts alleging a violation of Article 8 ECHR because the effect of section 65(2) of RIPA is to exclude the High Court's jurisdiction to hear complaints against UKIS under the HRA. The Government contended that the Article 8 complaints could only be raised in the IPT and, moreover, the High Court would decline to exercise jurisdiction in relation to any associated common law claims that the Applicants might seek to bring given the IPT's statutory jurisdiction. The Treasury Solicitor's letter relied upon *R (A) v B* [2010] 2 AC 1 in which the UK Supreme Court held that the effect of section 65(2) is that the IPT has exclusive jurisdiction to consider complaints under section 7 HRA.

183. Given the position of the UK Government, and the Supreme Court authority of *R (A) v B*, the Applicants were not required to instigate

proceedings in the Administrative Court to exhaust their domestic remedies under Article 35.

184. Article 35 also does not require the Applicants to bring their complaints before the IPT. This court has previously held that the IPT does not provide an effective remedy for complaints concerning the adequacy of the legislative regime in the UK and is not a 'remedy' that has to be exhausted before complaint can be made to this Court. In *Kennedy v. UK* the Court held that applicants did not need to bring complaints in the IPT before making a complaint to this Court. The Court,

> "109 … recall[ed] that where the Government claims non-exhaustion it must satisfy the Court that the remedy proposed was an effective one available in theory and in practice at the relevant time, that is to say, that it was accessible, was capable of providing redress in respect of the applicant's complaints and offered reasonable prospects of success. While the Government relies on the *British-Irish Rights Watch* case to demonstrate that the IPT could have issued a general ruling on compatibility, it does not address in its submissions to the Court what benefit, if any, is gained from such a general ruling. The Court recalls that it is in principle appropriate that the national courts should initially have the opportunity to determine questions of the compatibility of domestic law with the Convention in order that the Court can have the benefit of the views of the national courts, as being in direct and continuous contact with the forces of their countries. However, it is important to note in this case that the applicant's challenge to the RIPA provisions is a challenge to primary legislation. If the applicant had made a general complaint to the IPT, and if that complaint been upheld, the tribunal did not have the power to annul any of the RIPA provisions or to find any interception arising under RIPA to be unlawful as a result of the incompatibility of the provisions themselves with the Convention.
>
> No submissions have been made to the Court as to whether the IPT is competent to make a declaration of incompatibility under s.4(2) of the Human Rights Act . However, it would appear from the wording of that provision that it is not. In any event, the practice of giving effect to the national courts' declarations of incompatibility by amendment of offending legislation is not yet sufficiently certain as to indicate that s.4 of the Human Rights Act is to be interpreted as imposing a binding obligation giving rise to a remedy which an applicant is required to exhaust. 26 Accordingly, the Court considers that the applicant was not required to advance his complaint regarding the general compliance of the RIPA regime for internal communications with art.8(2) before the IPT in order to satisfy the requirement under art.35(1) that he exhaust domestic remedies."

185. The Court continued:

> "110 The Court takes note of the Government's argument that art.35(1) has a special significance in the context of secret surveillance given the extensive powers of the IPT to investigate complaints before it and to access confidential information. While the extensive powers of the IPT are relevant

> where the tribunal is examining a specific complaint of interception in an individual case and it is necessary to investigate the factual background, their relevance to a legal complaint regarding the operation of the legislative regime is less clear. In keeping with its obligations under RIPA and the Rules, 27 the IPT is not able to disclose information to an extent, or in a manner, contrary to the public interest or prejudicial to national security or the prevention or detection of serious crime. Accordingly, it is unlikely that any further elucidation of the general operation of the interception regime and applicable safeguards, such as would assist the Court in its consideration of the compliance with the regime with the Convention, would result from a general challenge before the IPT."

186. The Court noted in *Kennedy* that no submissions had been made to it as to whether the IPT could make a declaration of incompatibility under the HRA. In fact, it is clear from section 4(5) of the HRA (see §97 above) that the IPT is not included on the list of bodies that can make such a declaration and the Applicants would need to make an application to the High Court, which avenue, as the UK Government has asserted, has been removed by s.65(2) of RIPA.

187. Furthermore, such a declaration does not in any event result in the invalidation of the legislation in question, and this Court has held that it therefore does not constitute an effective remedy in any event: *Burden v United Kingdom* (2008) 47 EHRR 38. This was confirmed in *Malik v United Kingdom* (Application no.32968/11) [2013] ECHR 794 (28 May 2013) in which the Court held that complaints about the general compatibility of powers set out in primary legislation and the adequacies of the statutory regime do not have first to be ventilated in the UK courts or tribunals where the remedy of invalidation is sought.

188. The passages cited above explain why the IPT would not have provided an effective remedy for the Applicants' complaints and why a complaint to that tribunal did not have to be made before bringing this application.

189. In addition to these points, there are also further compelling considerations:

189.1. The IPT, although chaired by a High Court judge, is not a court of law. And RIPA s.67(8) provides that, "*determinations, awards, orders and*

other decisions of the Tribunal … shall not be subject to appeal or be liable to be questioned in any court." In R (A) v B the Supreme Court recognised that s.67(8), "*constitutes an ouster* (and, indeed, unlike Anisminic, an unambiguous ouster) *of any jurisdiction of the courts over the IPT*." (at [23] (Lord Brown of Eaton-under-Heywood). Therefore, there is no appeal or means of judicially reviewing any decision of the IPT even on the interpretation of the Convention. No authoritative determination of a point of law or compliance of UK law with the Convention can therefore be obtained from the IPT.

189.2. In any event, in its letter dated 26 July 2013, the UK Government pointed out that the IPT has previously considered section 8(4) of RIPA and in an open ruling dated 9 December 2004 (IPT/01/77) has expressed the view that it is compatible with the Convention. Therefore this Court already has the benefit of the IPT's views on this issue, and there is no value in the Applicants pursuing a complaint to obtain a further ruling on that point. Indeed, this ruling was expressly provided to the Court in Liberty and examined in detail at paragraphs [13]-[15] and [40] of that judgment.

189.3. Moreover, insofar as the complaint may be said to relate to the absence of primary legislation setting out adequate safeguards on the use of surveillance powers, and the failure of the UK Parliament to enact such laws, there is likewise no remedy available in UK law. As a matter of UK Constitutional Law, the UK Parliament is not to be equated with the British Government. (see for example *Halsbury's Laws of England*, Constitutional Law & Human Rights vol. 8(2) para 15 **[Annex 3/1160]**). The Government is not responsible as a matter of national law for the absence of legislation. An action cannot therefore be maintained against a Secretary of State for Parliament's failure to legislate. This is reflected in the HRA. The cause of action established by section 6 of the HRA for acts or omissions by public authorities that are contrary to Convention rights, "*does not include either Houses of Parliament or a person exercising functions connected with proceedings in*

Parliament": s.6(3). Therefore an action against Parliament for failure to ensure that an adequate regime of primary legislation is in place is not permitted under the HRA.

190. For all these reasons, and on the authority of *Kennedy* and *Malik*, *op cit*, the Applicants are not required to pursue actions in the High Court in England or in the IPT and have satisfied the requirements of Article 35(1).

V. STATEMENT OF THE OBJECT OF THE APPLICATION

191. The Applicants seek:

(i) declarations that their rights under Article 8 of the Convention have been violated and that UK law is not in conformity with the Convention in the respects set out herein; and

(ii) payment of their legal costs and expenses both in the domestic proceedings and in these proceedings under the Convention.

VI. OTHER INTERNATIONAL PROCEEDINGS

192. None.

VII. LIST OF ANNEXED DOCUMENTS

1. Annex 1 – Witness Statement of Cindy Cohn and Exhibit CC1
2. Annex 2 – Witness Statement of Ian Brown and Exhibit IB1
3. Annex 3 – Additional Materials Referenced in Application
4. Annex 4 – Statutory Materials

VIII. DECLARATIONS AND SIGNATURES

193. See Application Form.

30 September 2013