Case No. IPT/13/77/H

IN THE MATTER OF A CLAIM IN
THE INVESTIGATORY POWERS TRIBUNAL
Under section 7 of the Human Rights Act 1998

BETWEEN:

LIBERTY
(THE NATIONAL COUNCIL FOR CIVIL LIBERTIES)

Claimant

and

(1) GOVERNMENT COMMUNICATIONS HEADQUARTERS
(2) THE SECRET INTELLIGENCE SERVICE
(3) THE SECURITY SERVICE

Respondents

GROUNDS OF CLAIM

A. INTRODUCTION AND SUMMARY

1. The Claimant is a leading human rights organisation in the UK. It brings this claim pursuant to section 7(1)(a) of the Human Rights Act 1998 ("HRA").

2. There is, at the very least, a reasonable likelihood that the Respondent has interfered with the Claimant's private communications, contrary to the Claimant's rights under Article 8 and Article 10 of the European Convention on Human Rights ("ECHR").

3. The claim is based on the Respondents' use of two programmes:

   (1) **PRISM**: A programme carried out by the US National Security Agency ("NSA") to obtain, access, analyse, store and share private communications content and/or data from service providers.

   (2) **Tempora**: A programme apparently carried out by the UK's Government Communications Headquarters ("GCHQ") that intercepts vast amounts of communications content and/or data, through fibre optic cables, entering and leaving the UK.

4. In summary, the Claimant alleges that:

   (1) In relation to PRISM, the Respondents acted unlawfully by receiving information from the NSA in a manner that was in breach of section 6 HRA and Articles 8 and 10 of ECHR.

   In particular, the full extent of the Respondents' engagement with the NSA through PRISM takes place outside of any adequate legal framework and/or is not "in accordance with law".

   (2) In relation to Tempora, the Respondents acted unlawfully by intercepting the content of communications to and from the Claimant, and accessing communications data in relation to the Claimant. Such activity was in breach of section 6 HRA and Articles 8 and 10 of ECHR. Further or alternatively, such activity was in breach of sections 1(5)(c), 5(2)(b), 20 and 22(5) of the Regulation of Investigatory Powers Act 2000 ("RIPA").

   In particular, there is no clear legal framework, within RIPA or otherwise, that permits the vast collection and storage of communications carried out by Tempora. Such activity is not in accordance with law. Further, even if it is possible that such activity falls within RIPA, the scale of communications being obtained was in breach of the provisions of RIPA and could not sensibly be described as either necessary in a democratic society or proportionate.

   (3) In relation to Tempora, the Respondents acted unlawfully by granting NSA officials access to the content of communications to and from the Claimant as well as communications data relating to the Claimant (whether or not that material was originally obtained by the Respondents through the Tempora programme or otherwise).

   In particular, there is no recognisable legal framework permitting the Respondents to collect and share communications in the way Tempora makes available potentially vast amounts of private communications to the NSA. Accordingly, the Respondents' conduct was not in accordance with law and was in breach of the Claimant's rights under section 6 HRA and Articles 8 and 10 ECHR.

5. In order to provide a fair hearing of this claim, the Claimant seeks a public *inter partes* hearing on the following issues:

(1) What, if any, legal framework governs the receipt of intercepted communications and/or communications data from a foreign intelligence service in respect of communications originating from and/or received in the UK? If such a framework does exist, is it compatible with Article 8?

(2) What, if any, legal framework governs the granting of access of intercepted communications and/or communications data to a foreign intelligence service? If such a framework does exist, is it compatible with Article 8?

(3) Does RIPA, through the definition of "external communication" in section 20 or otherwise, provide sufficient clarity concerning the conditions and circumstances in which UK residents are liable to have their communications intercepted?

(4) Is the power to access "stored communications" under section 1(5)(c) RIPA without an interception warrant compatible with Article 8 ECHR?

6. Following that public hearing, the Claimant seeks an open ruling on those issues of law.

7. The Claimant sets out at Part F of these grounds how this Tribunal's own procedure not only permits distinct legal issues to be determined in a public hearing (followed by an open ruling), but in some circumstances will require that such a hearing takes place.

8. For the avoidance of doubt, the Claimant submits that considering those matters in a public hearing would involve this Tribunal considering legal principles without the need to reveal specific sensitive information.

9. The Claimant brings this claim but a number of other international organisations, which work in partnership with the Claimant, are interested in the issues raised. These include the American Civil Liberties Union ("ACLU"), the Canadian Civil Liberties Association ("CCLA"), the Irish Council for Civil Liberties ("ICCL"), the Hungarian Civil Liberties Union ("HCLU") and the Egyptian Initiative for Personal Rights ("EIPR").

B. FACTS

The Background to the Claim

10. On 6 June 2013, *The Guardian* and *Washington Post* published details of PRISM. They revealed that PRISM is a programme operated by the NSA, an intelligence agency of the United States Department of Defense.

11. According to those reports - which have never been specifically denied - the purpose of PRISM is to enable the NSA to access individuals' communications data from leading service providers. Those providers include Google, Facebook, Twitter, YouTube and Apple, and potentially include communications by hundreds of millions of individuals across the world.

12. On 21 June 2013, *The Guardian* published details of a different programme, Tempora. It was described as "a GCHQ programme to create a large-scale 'Internet buffer', storing internet content for three days and metadata [communications data] for up to 30 days". Tempora involves direct access by GCHQ to more than 200 fibre optic cables, enabling it to access both communications data and the content of the communications themselves.

Liberty

13. The Claimant, Liberty (the National Council for Civil Liberties), was formed in 1934 and is an independent, non-political body whose principle objectives are the protection of civil liberties and the promotion of human rights in the UK. The focus of much of the Claimant's work in recent years has been those human rights issues arising from the US-led "War on Terror" following the events of 11 September 2001, including:

    a) The Claimant's campaigns that challenge both UK and US government practices including, the collection of communications content and data:
        - Campaigning against UK complicity in the US' extraordinary rendition programme ("*No Torture, No Compromise"*);
        - Campaigning against the Draft Communications Data Bill ("*No Snooper's Charter")*;

- Opposing the introduction of closed material procedures in civil claims under the Justice and Security Act 2013 ("*For Their Eyes Only*");[1]
- Campaigning against the use of control orders under the Prevention of Terrorism Act 2005 and, more recently, the introduction of Terrorism Prevention and Investigation Measures ("TPIMs") ("*Unsafe, Unfair*"); and
- Ongoing campaigns to reform the Extradition Act 2003 and the 2003 US-UK extradition treaty ("*Extradition Watch*").

b) The Claimant's representation of Katherine Gun, a GCHQ employee accused of disclosing to the public details of a US request to the UK intelligence services to intercept the communications of UN Security Council members in the run-up to the Iraq War in 2003;

c) The Claimant's challenge before the European Court of Human Rights ("ECtHR") to the power of the UK intelligence services to intercept communications to and from the UK under the Interception of Communications Act 1985 (*Liberty and others v United Kingdom* (2009) 48 EHRR 1);

d) The Claimant's interventions in various, high-profile cases involving human rights issues arising from the "War on Terror" including *A and others v Secretary of State for the Home Department* [2004] UKHL 56; *A and others v United Kingdom* (2009) 49 EHRR 29; *Binyam Mohamed v Secretary of State for Foreign and Commonwealth Affairs* (2010) EWCA Civ 65 and 158; *Al Rawi and others v Security Service and others* [2011] UKSC 34; *Bank Mellat v HM Treasury (No 1)* [2013] UKSC 3; *McKinnon v Government of the United* States [2008] UKHL 59; *Norris v United States of America* [2010] UKSC 9 and *Bermingham v Serious Fraud Office* [2006] EWHC 200 (Admin).

14. Against that background, the Claimant believes its communications are highly likely to be caught by any broad use of powers to access UK / US communications:

[1]These measures appear to have been prompted, in part, by purported US government's concerns at the potential disclosure of intelligence material in civil proceedings in UK Courts: see, for example, the testimony of David Anderson QC, the reviewer of terrorism legislation, to the Joint Committee on Human Rights, 16 October 2012, Q72, describing his meetings with US officials concerning the proposed measures in the Justice and Security Green Paper: "There was an American stake in closed material procedure that I had not entirely appreciated until I went over there, because of course some of this closed material will be American-sourced material, just as some of it will be sourced from other countries as well. I am certainly not going to be too specific here, but my sense was that there are some people in America who probably took a bit of persuading that the closed material procedure was an adequate way of protecting their secrets".

- In the course of its work, individual members of the Claimant's staff use a variety of phone and internet services, this includes landlines, fax machines and mobile phones but also smartphones such as iPhones and Blackberrys, video-link services, Skype, Google, Gmail, YouTube, Hotmail, Facebook and Twitter.

- While using those services, members of the Claimant's staff are regularly in contact with, and contacted by, an extremely broad range of groups and individuals, both within and without the UK.

- Those persons may be senior government ministers, senior civil servants, MPs and peers, including the heads of various parliamentary committees. But they also include a wide range of groups and individuals in the US and UK, including the ACLU, lawyers acting on behalf of individuals subject to control orders and TPIMs, and those bringing claims against the UK government in respect of its alleged complicity in their detention and ill-treatment abroad; as well as various grassroots organisations in the UK working on behalf of those individuals and communities affected by counter-terrorism measures.

- The Claimant is a member of an international network of human rights organisations working on counter-terrorism issues, including the ACLU, the CCLA, the ICCL, the HCLU and the EIPR. Insofar as the communications of any of those organisations may have been intercepted or collected, the Claimant's communications with them would also have subjected to interference.

- In the context of its work, outlined above, the Claimant receives a large amount of sensitive information in confidence, both from public officials but also from members of the public. In addition, some of the Claimant's communications are subject to legal advice privilege and litigation privilege. Accordingly, the potential interest that the Respondents or US authorities may have in communications others have with the Claimant is self-evident. Similarly, the likelihood that the broad use of powers to gather such communications is likely to include the Claimant's communications is a matter of obvious and significant concern.

PRISM

15. On 6 June 2013, *The Guardian* and *The Washington Post* published 4 slides from an internal NSA PowerPoint presentation dated April 2013, which gave details of an NSA programme entitled PRISM/US-984XN ("PRISM") as follows:

    (i) The first slide stated that PRISM is the Signals Intelligence Activity Designator ("SIGAD") used most frequently in reporting by the NSA, indicating that the programme is responsible for a plurality (if not necessarily an outright majority) of intelligence data being gathered by the NSA.

    (ii) The second slide noted that "much of the world's communications flow through the US", that the path taken by electronic communications is not always possible to predict, but that "your target's communications could easily be flowing into and through the US".

    (iii) The third slide was headed "PRISM Collection Details" and listed Microsoft, Google, Yahoo, Facebook, YouTube, Skype and Apple as "providers" in the programme, and stated that the product of "collection (surveillance and Stored Comms) … varies by provider". Among the types of material it identified as available through the programme are email, chat (including video and voice), videos and video conferencing, photos, stored data, VoIP, file transfers, logins, and online social networking details.

    (iv) The fourth slide displayed a graph under the heading "Dates When PRISM Collection Began For Each Provider", with specific dates given as follows: Microsoft (11 September 2007), Yahoo (12 March 2008), Google (14 January 2009), Facebook (3 June 2009), YouTube (24 September 2010), Skype (6 February 2011) and Apple (October 2012).

16. A further report by the Guardian dated 12 July 2013, ("How Microsoft handed the NSA access to encrypted messages") provided details of how one of the providers worked with the NSA to provide technical assistance in circumventing the encryption provided by its own software and email services, including Outlook and Hotmail, and the voice and video service Skype.

17. The information concerning PRISM is amongst a range of classified material that has been leaked to the newspapers by Edward Snowden, an NSA contractor. The NSA has never denied the authenticity of the slides.

18. On 8 June, the US Director of National Intelligence issued a statement entitled "Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act", which stated among other things:

> PRISM is not an undisclosed collection or data mining program. It is an internal government computer system used to facilitate the government's statutorily authorized collection of foreign intelligence information from electronic communication service providers under court supervision, as authorized by Section 702 of the Foreign Intelligence Surveillance Act (FISA) (50 U.S.C. § 1881a). This authority was created by the Congress and has been widely known and publicly discussed since its inception in 2008.
>
> Under Section 702 of FISA, the United States Government does not unilaterally obtain information from the servers of U.S. electronic communication service providers. All such information is obtained with FISA Court approval and with the knowledge of the provider based upon a written directive from the Attorney General and the Director of National Intelligence. In short, Section 702 facilitates the targeted acquisition of foreign intelligence information concerning foreign targets located outside the United States under court oversight. Service providers supply information to the Government when they are lawfully required to do so.
>
> The Government cannot target anyone under the court-approved procedures for Section 702 collection unless there is an appropriate, and documented, foreign intelligence purpose for the acquisition (such as for the prevention of terrorism, hostile cyber activities, or nuclear proliferation) and the foreign target is reasonably believed to be outside the United States. We cannot target even foreign persons overseas without a valid *foreign intelligence purpose.*

Tempora

19. On 21 June 2013, *The Guardian* published details of Tempora, which it described as "a GCHQ programme to create a large-scale 'Internet buffer', storing internet content for three days and metadata [communications data] for up to 30 days". According to *The Guardian*, Tempora has been operational "for some 18 months" and involves access to more than 200 fibre-optic cables carrying data at 10 gigabits per second. This is said to allow GCHQ to extract both content and communications data. It went on to state that, according to internal NSA documents shown to the journalists by Edward Snowden, GCHQ was handling 600 million "telephone events" each day in 2012.

20. In addition, *The Guardian* reported that GCHQ gave NSA officials access to material obtained by Tempora:

> By May last year 300 analysts from GCHQ, and 250 from the NSA, had been assigned to sift through the flood of data. The Americans were given guidelines for its use, but were told in legal briefings by GCHQ lawyers: "We have a light oversight regime compared with the US". When it came to judging the necessity and proportionality of what they were allowed to look for, would-be American users were told it was "your call". *The Guardian* understands that a total of 850,000 NSA employees and US private contractors with top secret clearance had access to GCHQ databases.

21. The report went on to note that:

> There is an investigatory powers tribunal to look into complaints that the data gathered by GCHQ has been improperly used, but [GCHQ] reassured NSA analysts in the early days of the programme, in 2009: "So far they have always found in our favour".

22. In a subsequent report ("MI5 feared GCHQ went 'too far' over phone and internet monitoring" by Nick Davies, *The Guardian*, 22 June 2013), one member of the Security Service "who has been directly involved in GCHQ operations" described what appears to be circumvention of RIPA through the use of Tempora by one or more of the Respondents:

> The source claimed that even the conventional warrant system has been distorted – whereas police used to ask for a warrant before intercepting a target's communications, they will now ask GCHQ to intercept the target's communications and then use that information to seek a warrant.

C. RELEVANT LEGAL FRAMEWORK

US Law

The protection for private communications under the Fourth Amendment

23. The Fourth Amendment to the US Constitution provides:

> The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized.

In *Katz v United States* 389 US 347 (1967), the US Supreme Court found that the FBI's covert interception of the petitioner's telephone conversations, made from a public phone booth, constituted a "search" for the purposes of the Fourth Amendment. Accordingly, the Court held that the interception was unlawful because it had been carried out without prior judicial authorisation, "a constitutional precondition of the kind of electronic surveillance involved in this case" (359).[2]

24. In the year following *Katz*, Congress enacted the Omnibus Crime Control and Safe Streets Act 1968, Title III of which provides the federal framework for the domestic interception of electronic communications for law enforcement purposes.[3] Subsequent amendments to Title III by the Electronic Communications Privacy Act 1986 ("ECPA") and Communications Assistance for Law Enforcement Act 1994 ("CALEA") have extended the scope of 'electronic communications' to include text messages, email, faxes and other internet transmissions.

25. The Fourth Amendment protects access to the content of communications for law enforcement purposes, but has been interpreted so as not to protect access to communications data. The principle emerged in early cases relating to phone call data: in *Smith v Maryland* 442 US 735 (1979), the US Supreme Court concluded that there was no reasonable expectation in respect of numbers dialled:

> Telephone users ... typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.

Accordingly, the Court held, the use of the "pen register" (a record of numbers dialled to and from a phone number) did not constitute a search under the Fourth Amendment.[4]

[2] See also *ibid* at 353: "The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth, and thus constituted a "search and seizure" within the meaning of the Fourth Amendment".

[3] US Code, Title 18, Chapter 119. The corresponding framework for the interception of foreign communications for intelligence purposes is provided by the Foreign Intelligence Surveillance Act 1978.

[4] Note that the Electronic Communications Privacy Act 1986 subsequently introduced the requirement for law enforcement bodies to obtain a court order in order to install a pen register or track and trace device (a device that records outgoing numbers).

26. More recently, the same approach has been taken by the Ninth Circuit Court of Appeals in *United States v Forrester* 512 F.3d 500 (9th Cir. 2008) in respect of data gathered by an Internet Service Provider concerning individual internet usage:

> … e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.

27. Fourth Amendment protection is also limited in another significant way: US courts have interpreted the Fourth Amendment not to include non-US citizens outside the territorial US. In *United States v Verdugo-Urquidez* 494 US 259 (1990), Rehnquist CJ, writing for the majority, noted:

> … the purpose of the Fourth Amendment was to protect the people of the United States against arbitrary action by their own Government; it was never suggested that the provision was intended to restrain the actions of the Federal Government against aliens outside of the United States territory. There is ... no indication that the Fourth Amendment was understood by contemporaries of the Framers to apply to activities of the United States directed against aliens in foreign territory or in international waters (266-267).

28. In summary, foreign persons whose communications are collected by a US government agency have very limited protection of their rights, for the following reasons:
    - The covert interception of the content of communications by US public officials for law enforcement purposes, does constitute a "search", within the meaning of the Fourth Amendment.
    - However, access to communication data by public officials for law enforcement purposes does not.
    - In any event, the scope of the Fourth Amendment does not extend to the communications of non-resident aliens outside the territorial US.

Foreign Intelligence Surveillance Act 1978 (US)

29. Whereas Title III, above, sets out the US federal law governing the interception of US domestic communications for law enforcement purposes, the Foreign Intelligence Surveillance Act 1978

("FISA")[5] provides the relevant legal framework for the interception of communications for foreign intelligence purposes.[6]

30. FISA provides only limited protection to foreign persons who may be the subject of surveillance or have their communications intercepted and stored by the NSA:

- Section 702 of FISA (50 USC § 1881(a)) provides that the US Attorney General and the Director of National Intelligence may authorise jointly, for a period of up to 1 year, "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information".

- §1801(e) defines "foreign intelligence information" as follows:

(1) information that *relates to*, and if concerning a United States person is necessary to, the ability of the United States to protect against—

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that *relates to*, and if concerning a United States person is necessary to—

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

An authorisation generally requires an order from the FISA Court, made on an *ex parte* basis in closed proceedings.[7]

[5] US Code, Title 50, Chapter 36.

[6] Prior to the PATRIOT Act 2001, Title III also provided the exclusive legal framework for the interception of domestic communications for domestic security (as opposed to law enforcement) purposes: see *United States v United States District Court for the Eastern District of Michigan* 407 US 297 (1972).

[7] An authorisation may only be made following either (i) an order of the FISA Court, following written certification by the Attorney or the Director (§ 1881a(i)(3)); or (ii) a determination by the Attorney and the Director that it is necessary to act without an order first being obtained because "intelligence important to the national security of the United States may be lost or not timely acquired" (§ 1881a(c)(2)). § 1881a(g)(2) sets out various requirements that a certification must meet, including that "a significant purpose of the acquisition is to obtain foreign intelligence information" (§ 1881a(g)(2)(A)(v))

- On 6 July 2013, the *New York Times* reported that the scope of FISA has been significantly expanded by a series of closed judgments issued by the FISA Court that had subsequently been leaked:

> The judges have concluded that the mere collection of enormous volumes of "metadata" — facts like the time of phone calls and the numbers dialled, but not the content of conversations — does not violate the Fourth Amendment, as long as the government establishes a valid reason under national security regulations before taking the next step of actually examining the contents of an American's communications.
>
> ("In Secret, Court Vastly Broadens Powers of NSA", New York Times, 6 July 2013)

and "the acquisition involves obtaining foreign intelligence information from or with the assistance of an electronic communication service provider" (§ 1881a(g)(2)(A)(vi)). If the FISA Court finds that a certification contains all the required elements and is otherwise consistent with the requirements of § 1881a(d) and (e) and with the Fourth Amendment, the Court "shall enter an order approving the certification". § 1881a(b) similarly provides various limitations in respect of an acquisition, including the requirement that an acquisition shall be "conducted in a manner consistent with" the Fourth Amendment (§ 1881a(b)(5)). .Just as § 1881a provides for the interception of communications of non-US citizens outside the US for the purpose of gathering foreign intelligence, § 1842(a)(1) similarly provides that the Attorney General may apply for an order authorising or approving the installation and use of a pen register (as defined in 18 USC § 3127(3)) or trap and trace device (as defined in 18 USC § 3127(4)) used to obtain communications data "for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism". All applications for FISA warrants are heard by the Foreign Intelligence Surveillance Court ("the FISA Court"), which is empowered to hold closed proceedings and deliver closed judgments. Appeals are heard by the Foreign Intelligence Surveillance Court of Review.

UK Law

The Security Service Act 1989

31. The relevant functions of the Security Service are set out under section 1 of the 1989 Act, which provides materially as follows:

(1) .. 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.[8]

(2) ... to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands.[9]

(3) … to act in support of the activities of police forces, the National Criminal Intelligence Service, the National Crime Squad and other law enforcement agencies in the prevention and detection of serious crime.[10]

32. Section 2 imposes various duties on the Director-General of the Security Service, including that under section 2(2)(a) which provides that it shall be his duty to ensure that:

> there are arrangements for securing that no information is obtained by the Service except so far as is 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[.]

There has been no indication as to what, if any, arrangements have been made. If they have been made, they have never been made public. Nor has any reference been made in successive annual reports of the Intelligence Services Commissioner to indicate that the Commissioner is satisfied that the arrangements in question are adequate, or even that he had considered them.

[8] Section 1(2)
[9] Section 1(3)
[10] Section 1(4)

The Intelligence Services Act 1994

33. The functions of the Secret Intelligence Service ("the Intelligence Service") are set out under section 1(1) of the 1994 Act materially as follows:

    (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.

34. Section 1(2) further provides that these functions 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 the support of the prevention or detection of serious crime.

35. Section 2(2) imposes a duty on the Chief of the Intelligence Service to ensure, among other things:

    (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 purpose of the prevention or detection of serious crime; or
        (iv) for the purpose of any criminal proceedings...

36. Section 3(1)(a) sets out the functions of GCHQ materially as follows:

    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...

37. Section 3(2) further provides that this function 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.

38. Section 4(2)(a) imposes a duty on the Director of GCHQ to ensure:

> 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.

39. As with the 1989 Act, however, there has been no indication as to what, if any, such arrangements have ever been made. If they have, they have never been published. Nor is there any reference in successive annual reports of the Intelligence Services Commissioner to indicate that he was satisfied that the arrangements were adequate, or even that he had considered them.

The Human Rights Act 1998

40. Section 6(1) of the HRA provides that it is unlawful for a public authority to act in a way which is incompatible with a Convention right.

41. Article 8 of the ECHR states that:

1) Everyone has the right to respect for his private and family life, his home and correspondence.

2) There shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the right and freedoms of others.

42. Section 2 of the HRA requires a court or tribunal determining a question that has arisen in connection with a right pursuant to the ECHR to 'take account of any judgment or decision of the ECtHR.

43. In accordance with that requirement, the following principles established by a number of ECtHR judgments fall to be taken account of by this tribunal, when considering the Claimant's claims:

(1) A public authority's interference with communications including telephone calls and emails falls within the Article 8(1).[11]

(2) A person alleging a breach of their Article 8 rights through the interception or interference with their personal communications need not demonstrate that the impugned measure had actually been applied to her: "The mere existence of legislation which allows a system of secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicant's rights under Article 8, irrespective of any measures actually taken against them…".[12]

(3) "Where actual interception was alleged, the ECtHR has held that in order for there to be an interference it has to be satisfied that there was a reasonable likelihood that surveillance measures applied to the applicant. The Court will make its assessment in light of all the circumstances of the case and will not limit its review to the existence of direct proof that surveillance has taken place given that such proof is generally difficult or impossible to obtain."[13]

(4) A person will suffer an interference with their Article 8 rights not merely through the collection of the content of their communications, but also the data relating to their communications, and the storage of that data for access by public authorities (see *Malone v UK* (1985) 7 EHRR 14).[14]

(5) In order for an interference with a person's communications through secret interceptions pursuant to Article 8(1) to be justified under Article 8(2), it must be "in accordance with the law". This requires that the relevant law "must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which

[11] For example, *Kennedy v UK* (2011) 52 EHRR 4 at [118]
[12] See *Liberty v UK* (2008) 48 EHRR 1 at [56]
[13] *Kennedy v UK* at [123]
[14] At [84]. The use of a device called a mater check printer which registered the numbers dialled on a particular telephone and the time and duration of each call was found to "contain information, in particular the numbers dialled, which is an integral element in the communications made by the telephone."

public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence."[15]

(6) The need for such interference to be in accordance with the law, also applies to the disclosure, copying and storage of intercepted material[16]. The law must "indicat[e] with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications" and, in particular, "set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material".[17]

(7) The "in accordance with the law" requirement also relates to the quality of the law in question. There must be sufficient safeguards to avoid the risk of abuse of power or arbitrariness, in particular abuse of widely-phrased discretionary powers.[18] Further, "…it would be contrary to the rule of law, one of the basic principles of a democratic society enshrined in the Convention, for a legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate with sufficient clarity the scope of any such discretion conferred on the competent authorities and the manner of its exercise. The level of precision required of domestic legislation – which cannot in any case provide for every eventuality – depends on a considerable degree to the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed".[19]

The Regulation of Investigatory Powers Act 2000

Interception of communications

44. Section 2(2) of RIPA provides materially as follows:

> 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,

[15] *Malone v UK* at [67]
[16] *Liberty v UK* at [57]
[17] *Liberty v UK* at [69]
[18] *Huvig v France* (1990) 12 EHRR 528 at [29] – [35]
[19] *Gillan v UK* (2010) 50 EHRR 45 at [77].

(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 transmitted, to a person other than the sender or intended recipient of the communication.

Interception of communications by warrant

45. Under section 5(1) of RIPA the Secretary of State may issue a warrant authorising or requiring the person to whom it is addressed, by any such conduct as may be described in the warrant, to secure any one or more of the following:

(a) the interception in the course of transmission by means of a postal service or telecommunications system described in the warrant;

(b) the making, in accordance with an international mutual assistance agreement, or a request for the provision of such assistance in connection with, or in the form of, an interception of communications as may be so described;

(c) the provision, in accordance with an international mutual assistance agreement, to the competent authorities of a country or territory outside the United Kingdom of any such assistance in connection with, or in the form of, an interception of communications as may be so described;

(d) the disclosure, in such manner as may be so described, of intercepted material obtained by any interception authorised or required by the warrant, and of related communications data.

Interception of domestic communications

46. Section 8(1) of RIPA requires that an interception warrant must name or describe either (a) a single person; or (b) a single set of premises as the subject of the interception. Section 8(2) further requires that a warrant must comprise 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".[20]

47. There is, however, no corresponding requirement to specify the person or premises being targeted in respect of warrants directed towards the interception of "external communications"

[20]Section 8(3) stipulates that a "factor or combination of factors" under s8(2) must identify those communications to and from the person or premises being targeted.

under sections 8(4) and (5), so long as the Secretary of State is satisfied that such a warrant is necessary on the grounds set out at section 5(3)(a) – (c):

a) in the interests of national security;.

b) for the purpose of preventing or detecting serious crime;.

c) for the purpose of safeguarding the economic well-being of the United Kingdom.[21]

As with the interception of domestic communications, the Secretary of State must also believe that "the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct" (s5(2)(b)), including taking into account whether the information sought by the interception of external communications "could reasonably be obtained by other means" (s5(4)).

Section 20 defines an "external communication" as "a communication sent or received outside the British Islands". However, section 71(1) requires a person exercising or performing any power or duty under a provision covered by a code of practice to "have regard" to its provisions, so far as they are applicable, and paragraph 5.1 of the Interception of Communications Code of Practice (2007) further explains how "external communications" are defined (emphasis added):

> [External communications] include those which are both sent and received outside the British Islands, whether or not they pass through the British Islands in course of their transit. <u>They do not include communications both sent and received in the British Islands, even if they pass outside the British Islands en route.</u>

48. Section 15 imposes upon the Secretary of State a general duty to ensure in relation to all interception warrants "such arrangements … as he considers necessary for securing" that intercepted material is not disclosed more widely than is necessary for the authorised purpose (s15(2)) and that it is likewise not retained any longer than is necessary (s15(3)). In respect of warrants for the interception of external communications under s8(4), the intercepted material may only be "read, looked at or listened to" by relevant persons to the extent that it has been certified, and excluding material relating to individuals "known to be for the time being in the British Islands" (sections 16(2)-(6)).

[21] See also section 5(5): "A warrant shall not be considered necessary on [the grounds of safeguarding the UK's economic well-being] unless the information [relates] to the acts or intentions of persons outside the British Islands".

Interception without warrant

49. Section 1(5)(c) of RIPA provides that an interception warrant is not required in relation to any 'stored communication' where the interception is "in exercise ... of any statutory power (apart from this section) for the purpose of obtaining information or of taking possession of any document or other property".

Access to communications data

50. "Communications data" is defined by section 21 to include traffic data, service user data, and subscriber data (s21(4)(b)). Among other things, "traffic data" includes data which identifies:[22]

- the locations where a communication is taking place (origin and destination)
- the persons involved (sender/caller and recipient); or
- any equipment used to transmit, receive or route the communication.

51. Pursuant to section 22(2), a designated person within a relevant public body (including each of the Respondents) may authorise members of the same body to obtain communications data if he believes it is necessary:

(a) in the interests of national security;

(b) for the purpose of preventing or detecting crime or of preventing disorder;

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

(d) in the interests of public safety;

(e) for the purpose of protecting public health;

(f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

(g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or

[22] Section 21(6)

(h) for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State.

52. Alternatively, where it appears to the designated person that a telecommunications operator "is or may be in possession of, or be capable of obtaining" any communications data, the designated person may by notice require that operator to either (i) obtain the data or (ii) disclose all of the data in his possession or subsequently obtained by him (s22(4)).

53. Section 22(5) prohibits the grant of any authorisation under s22(3) or the giving of a notice under s22(4) unless the designated person "believes that obtaining the data in question by the conduct authorised or required … is proportionate to what is sought to be achieved by so obtaining the data".

The Interception of Communications Commissioner

54. Section 57(2) of RIPA requires the Commissioner to keep under review, among other things, the Secretary of State's exercise and performance of his powers and duties in respect of interception warrants (s57(2)(a)), in relation to information obtained under Part I of the Act (s57(2)(c)), and the adequacy of the arrangements made by the Secretary of State under section 15 (s57(2)(d)(i)).

55. Section 57(3) further provides that the Commissioner shall give the Tribunal "all such assistance … as the Tribunal may require -

a) in connection with the investigation of any matter by the Tribunal; or

b) otherwise for the purposes of the Tribunal's consideration or determination of any matter."

The Counter-Terrorism Act 2008

56. Section 19 of the 2008 Act provides materially as follows (emphasis added):

(1) A person may disclose information to any of the intelligence services for the purposes of the exercise by that service of any of its functions.

(2) Information obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions.

…

(3) Information obtained by GCHQ for the purposes of any of its functions may be disclosed by it-

a) for the purpose of the proper discharge of its functions, or
b) for the purpose of any criminal proceedings.

(4) A disclosure under this section does not breach –

a) any obligation of confidence owed by the person making the disclosure, or
b) <u>any other restriction on the disclosure of information (however imposed)</u>.

57. The provisions of section 19 are subject to those in section 20 (see s19(7)). Section 20 provides among other things that the provisions of section 19 "do not affect the duties with respect to the obtaining or disclosure of information imposed … on the Director of GCHQ by section 4(2) of that Act" (s20(1)(c)). Section 20(2) provides:

Nothing in that section authorises a disclosure that-

a) …
b) is prohibited by Part 1 of the Regulation of Investigatory Powers Act 2000…

58. Section 20(3) provides that (emphasis added):

The provisions of that section are <u>without prejudice</u> *to* any rule of law authorising the obtaining, use or disclosure of information by any of the intelligence services.

E. GROUNDS OF CLAIM

First Ground: In relation to PRISM, the Respondents acted unlawfully by receiving information from the NSA in a manner that was not in accordance with law, and in breach of section 6 HRA and Articles 8 and 10 of ECHR.

The interference by the Respondents' use of PRISM

59. There appears to be no dispute that the NSA is working with US-based electronic communications service providers such as Google, Facebook and Twitter in order to access data concerning foreign communications routed through the US. This potentially includes communications to and from millions of UK citizens and UK organisations, especially those engaged with issues that are part of the Claimant's work. The reports further indicate that this collection, retention and access to communications data by the NSA does, in fact, take place on a massive scale.

60. The NSA maintains that its activities involving the PRISM programme have been authorised under s702 FISA. The NSA has not denied that it has obtained the communications material from those providers identified in the media reports.

61. Media reports have detailed how communications material obtained by the NSA using PRISM has subsequently been passed to the Respondents. This is a matter of widespread public debate and concern

62. On 17 July 2013, partly in response to that public concern, the Intelligence and Security Committee issued a statement concerning its investigation of alleged GCHQ involvement concerning PRISM ("Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme").

63. Among other things, the Committee's statement referred to media reports "that GCHQ had access to PRISM and thereby to the content of communications in the UK without proper authorisation" (para 4). Although the Committee concluded that allegations that GCHQ "circumvented UK law by using the NSA's PRISM programme to access the content of private communication" are "unfounded" (para 5), it did not deny that GCHQ had access to PRISM or

that GCHQ received communications material from the NSA that had been obtained as a result of PRISM.

64. As detailed above, the Claimant's activities as a leading human rights NGO engaged in campaigns against such US practices as extraordinary rendition, torture and indefinite detention in Guantanamo Bay bring it squarely within the scope of s702 FISA: it is a "foreign-based political organisation"(§ 1801(a)(5)). Information connected with the Claimant may therefore constitute "foreign intelligence information" (§ 1801(e)).

65. The Claimant and its staff are regular users of most of the services that are comprised in the PRISM programme (Google, Twitter, Facebook). It is also in frequent email and telephone contact with groups and individuals in the US working on issues such as Guantanamo Bay and extraordinary rendition, not to mention groups and individuals in the UK and elsewhere who are liable to be considered persons of interest to the intelligence services (e.g. individuals subject to control orders).

The Claimant's communications caught by PRISM

66. Given the scale of NSA surveillance of foreign communications, the breadth of s702 FISA and the nature of the Claimant's own activities, there is, at the very least, a "reasonable likelihood" that the Claimant's communications have been intercepted and that data concerning those communications have been accessed and retained by the NSA.

67. In any event, it is important to emphasise that in order to pursue its claim the Claimant need not show that it has actually been the subject of that interference. If legislation (or the lack of legislation) permits significant interference with citizens' Article 8 rights, by way of covert surveillance, it is well established that the "mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them."[23]

[23] See *Liberty v UK* (2009) 48 EHRR 1 at [56], referred to at paragraph 43(2), above.

68. In its statement concerning its investigation of alleged GCHQ interception under PRISM, the Intelligence and Security Committee said that it had "taken detailed evidence from GCHQ", including "substantive reports" listing "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" (para 5), "a list of every 'selector' (such as an email address) for these individuals on which the intelligence was requested".

69. Notably, the statement did not contradict media reports that GCHQ in fact received from the NSA communications material relating to individuals "either believed to be in the UK or [who had been] identified as UK nationals".

70. The limited nature of the Committee's investigation is significant:

    (1) The Committee referred only to allegations of GCHQ's "alleged interception of communications" and "scrutiny of GCHQ's access to the content of communications" (para 5). It concluded that allegations that "GCHQ circumvented by UK law by using the NSA's PRISM programme to access the content of private communications" are "unfounded".

    However, it is conspicuous that the Committee did not deny the allegations that, through PRISM, the Respondents have received communications data related to UK communications (as opposed to merely the content of those communications).

    Nor did the Committee indicate that there were valid authorisations under s 22 RIPA in respect of any of the Respondents to access any such communications data that had been obtained as a result.

    (2) The Committee referred to "reports that GCHQ produced on the basis of intelligence *sought* from the US", and stated that it was satisfied "that they conformed with GCHQ's statutory duties" (para 5). The statement identified the legal authority for this as being "contained in the Intelligence Services Act 1994" (ibid). The Committee went on to state that "in each case where GCHQ *sought* information from the US, a warrant for interception, signed by a Minister, was already in place". It is again conspicuous that the Statement did not address the particular concern that – outwith any properly published legal framework - the Respondents have received, unsolicited, material in respect of UK communications obtained

by the NSA using PRISM or some similar programme. This material may include both content and communications data.

71. The Respondents' interference with the Claimant's communications both with regard to content and data, is only justified under Article 8(2) if it is in "accordance with the law":

(1) It is well-established that "in accordance with the law" under Article 8(2) requires that any interference with the right to privacy must have not only a sufficient legal basis but also one that is both accessible and sufficiently precise to enable a person reasonably to foresee the consequences which a given action may entail.

(2) In the context of covert surveillance, the Strasbourg Court has made clear that "foreseeability" does not require that "an individual should be able to foresee when the authorities are likely to intercept his communications that he can adapt his conduct accordingly" (*Weber and Savaria v Germany* (2006) Application No. 55878/00 (Admissibility Decision; Fifth Section), para 93).

(3) It does, however, require that the relevant law:

> must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures. (ibid)

(4) Moreover, given the obvious risks in granting to the authorities an unfettered discretion to intercept communications, the ECtHR held that the relevant law must (emphasis added):

> indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual <u>adequate protection against arbitrary interference</u>. (ibid, para 94)

(5) In respect to obtaining access to material *sought* from the NSA by GCHQ :

(a) Such access, does not fall within the parameters of RIPA, save that the Intelligence and Security Committee reported that GCHQ has "in each case where GCHQ sought information from the US, a warrant for interception by a Minister was already in place, in accordance with the legal safeguards contained in the Regulation of Investigatory Powers Act. It remains entirely unclear as to whether those warrants were themselves

based on material that was passed to the Respondents by the NSA, such that the obtaining warrants to seek information that has already been communicated becomes an artificial process."

(b) Further, and also in respect of communications content and data *sought* from the NSA by GCHQ, the Intelligence and Security Committee identified the Intelligence Services Act 1994 as the legal basis for GCHQ's actions. However, the 1994 Act provides no detail whatsoever as to how it would provide the legal basis for such sharing. It does not indicate the conditions and circumstances under which GCHQ or the Secret Intelligence Service may seek intelligence from the US in respect of UK communications. The statement of the Intelligence and Security Committee merely referred to having seen "the arrangements GCHQ has with its overseas counterparts for sharing information" as well as "the formal agreements that regulated access to this material". None of these arrangements, including those statutory arrangements required of the Director of GCHQ under the 1994 Act, have ever been made public.

(c) Accordingly, there appears to be no detailed primary legislation and no published framework within which Respondents' access to the Claimant's communications, through PRISM, takes place.

(6) The Claimant submits that the same principles apply to the receipt of intercepted domestic communications by intelligence agencies, through intelligence cooperation with foreign governments. Individuals may not be entitled to know when their communications are likely to be intercepted by foreign governments, but the law must at least provide individuals with an adequate indication of the circumstances in which and the conditions on which the Respondents may receive such material from those governments. It would otherwise be contrary to the rule of law - the core principle underlying this aspect of Article 8(2) - if the authorities could simply elect to sidestep the detailed requirements of their domestic law and instead obtain the very same content and data of domestic communications by way of cooperation with a foreign intelligence agency.

(7) In *Liberty and others v United Kingdom* the Secretary of State had by virtue of section 6 of the Interception of Communications Act 1985 been under a statutory duty to make arrangements concerning the disclosure, copying and storage of intercepted material. The

Court found that the existence of such powers constituted an interference with the applicants' rights under Article 8 (see para 57), and went on to hold that the domestic law at the relevant time did not:

> indicat[e] with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not, as required by the Court's case-law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material. (para 69)

(8) In the present case, the Claimant submits that the relevant law provides even less clarity than the provisions in issue in that case. Notwithstanding the provisions of the 1989, 1994 and 2008 Acts, there is a wholesale lack of legal certainty concerning the circumstances under which the Respondents may receive and process either the content of, or the data concerning, the private communications of UK residents that have been intercepted or access by the NSA under s702 FISA or otherwise. Nor does the relevant legislation provide any safeguards to prevent RIPA being circumvented in this manner.

(9) Even to the extent that any internal arrangements have in fact been made by any of the Respondents under the 1989 or 1994 Acts in respect of this issue, no details concerning these arrangements have ever been made public. Any such arrangements or guidance that do exist have never been made public and cannot therefore be said to be accessible, nor do they have the quality of "law".

(10) It is insufficient for GCHQ to assert that the 1994 Act - alongside Part 1 of RIPA - provides an adequate legal framework to receive, access and examine communications data on UK citizens from the NSA via PRISM. As a matter of principle, the law in question must "indicate with sufficient clarity the scope of any discretion conferred on the competent authorities and the manner of its exercise". This is especially important in the field of covert surveillance where, in the absence of a clear legal framework, the risk of abuse is high and the occurrence of excessive surveillance exceptionally difficult to discover.

(11) More generally, the sheer scale of NSA surveillance of foreign communications - taken together with the lack of equivalent protection for the privacy of those communications under US law - means that there is at the very least a real risk that the Respondents are

liable to receive material that they would otherwise be unable to obtain in accordance with RIPA and the requirements of Article 8 ECHR. Indeed, the volume of material reported to have been intercepted by the NSA using PRISM suggests that this risk may arise on something approaching a daily basis.

72. The Claimant therefore submits that the Respondents' receipt of the content and data of private communications obtained by the NSA under s702 FISA gives rise to a clear interference with its Article 8 rights, since the scale of the NSA's surveillance, the breadth of s702 and the nature of its activities mean that it is reasonably likely that its communications were the subject of such surveillance. The absence of a sufficient legal framework governing the Respondents' receipt of intercepted domestic communications and data from the NSA and other foreign intelligence agencies means, moreover, that any such interference could not have been in accordance with law, contrary to Article 8(2).

73. If the Respondents were to suggest that, notwithstanding the lack of UK legal framework, PRISM somehow operates in a manner which provides equivalent protection to the Claimant and other UK citizens pursuant to their Article 8 rights, the Claimant makes the following points:

(1) There is no realistic suggestion, nor could there be, that US law provides any statutory protection equivalent protection for the Claimant to that which it receive pursuant to Article 8 ECHR.

(2) Although FISA §1881a(b)(5) requires that an acquisition shall be "conducted in a manner consistent with" the outline of US case law, set out above, reveals that access to communications data does not fall within the Fourth Amendment.

(3) Additionally, the Fourth Amendment does not extend to the private communications of non-resident aliens, i.e. the Claimant and the overwhelming majority of UK residents.

(4) Neither s702 FISA nor the broader constitutional framework of US law, permit the FISA Court to take into account the rights of non-resident aliens to privacy in their communications. There is, therefore, no sense in which US law could be said to provide any meaningful safeguards against disproportionate, unsubstantiated or inappropriate communications interceptions when applied to UK organisations or nationals located in the UK.

74. The problem is further compounded by the lack of safeguards in relation to the sharing of material once it has been obtained. There is nothing in RIPA, the 1989 or 1994 Act that prohibits or restricts the receipt or processing of material gathered by a foreign intelligence body in respect of UK communications, whether by way of interception of their contents or access to their data. Indeed, s2(2)(a) of the 1994 Act, and ss 2(2)(a) and s4(2)(a), provide only a duty on the heads of the respective Respondents to make arrangements "securing that no information is obtained by [it] except so far as is necessary for the proper discharge of its functions". No details have ever been published concerning these arrangements, nor have the reports of the Intelligence Services Commissioner or the Intelligence and Security Committee given any indication of what they might be.

75. More generally, section 19(2) of the Counter-Terrorism Act 2008 provides that information obtained by any of the Respondents in connection with the exercise of any of its functions "may be used by that service in connection with the exercise of any of its other functions". Although section 20(1)(c) states that s19 does not affect the duties on the Director of GCHQ "with respect to the obtaining or disclosure of information imposed" by s4(2)(a) of the 1994 Act, and section 20(2)(b) provides that s19 cannot authorise a disclosure that is prohibited by Part 1 of RIPA, the saving provisions of s20 do not prevent GCHQ making *internal* use of the material for the purposes of subsequent RIPA authorisations.

Second Ground: In relation to Tempora, the Respondents acted unlawfully by intercepting the content of communications to and from the Claimant, and accessing communications data in relation to the Claimant

76. From the details of the Tempora programme that have been publicly disclosed, it is clear that GCHQ has obtained direct access to more than 200 fibre optic cables, carrying data at 10 gigabits per second. According to internal NSA documents shown to the journalists by Edward Snowden, GCHQ was handling 600 million "telephone events" each day in 2012.

77. In particular, it has become apparent that the Respondents have sought to exploit recent changes in the nature of communications technology - most notably, the transnational nature of the internet - in order to obtain domestic communications (i.e. those of UK residents) under the rubric of its external communications programme.

78. From the information available, it appears that the Tempora programme has been based on interception warrants made under s8(4) RIPA. However, in this ground, the Claimant will also address certain alternatives, namely the possibility of that Tempora involves the interception of stored communications without warrant under section 1(5)(c) and/or one or more authorisations to obtain communications data under section 22(5) RIPA.

Interception of external communications under section 8(4) RIPA

79. In *British Irish Rights Watch and others v Security Service, GCHQ and the SIS* (IPT/01/77, 9 December 2004), the Tribunal rejected the complaint that the process of filtering intercepted telephone calls made from the UK to overseas telephones under section 8(4) of RIPA breached Article 8(2) because it was not in accordance with law. Among other things, the Tribunal distinguished between the regime under Part I of RIPA for the interception of domestic communications (section 8(1)) and that for external communications (section 8(4)) as follows (emphasis added):

> The basis of the two warrants is obviously different. This is because it is the more necessary for additional care to be taken with regard to interference with privacy by a Government in relation to domestic telecommunications, with regard to which it has substantial potential control; but also because its knowledge of, and certainly its control over, external communications is likely to be dramatically less. (para 20.1)

It went on to conclude that the "right to intercept and access material covered by a s8(4) warrant, and the criteria by reference to which it is exercised" were "sufficiently accessible and foreseeable to be in accordance with law" (para 39).

80. In *Liberty v United Kingdom*, the ECtHR referred to the Tribunal's judgment without approving it. It noted, however, that "extensive extracts from the Code of Practice issued under section 71 of the 2000 Act are now in the public domain", which in the Court's view suggested that "it is possible for a State to make public certain details about the operation of a scheme of external surveillance without compromising national security" (para 68).

81. The Claimant submits, however, that the definition of "external communication" under section 20, even taken together with the plain terms of para 5.1 of the Interception of Communications Code of Practice (2007), fails to provide sufficient clarity as to when the communications of UK residents are liable to be intercepted as under section 8(4) as opposed to section 8(1). Specifically, an "external communication" is any communication "sent or received outside the British Islands". The Code of Practice adds the following (emphasis added):

> whether or not they pass through the British Islands in course of their transit. <u>They do not include communications both sent and received in the British Islands, even if they pass outside the British Islands en route</u>.

Although the language of the Code would appear to be sufficiently clear to deal with phone calls and emails, made or sent and received within the UK even if routed elsewhere, it fails to provide the necessary clarity in respect of most internet-based communications, such as a Google search, a YouTube link, a Facebook post or a direct message on Twitter, where the user is in the UK but where the relevant website is based in Northern California. The terms “transit” and “en route” are inadequate to deal with the majority of web-based services in 2013.

82. Apart from that 2007 Code of Practice, there continue to be no other details available about the conditions and circumstances under which the Respondents may intercept external communications under section 8(4). In particular, there is no separate reference to this in the most recent annual report of the Interception of Communications Commissioner (HC 496, 13 July 2012).

83. In light of reports of the Tempora programme operated by GCHQ, it appears that at least one of the Respondents has interpreted "external communications" in such a way as to encompass a great deal of communications originating from and received in the UK.

> There is a particular concern that the programme allows GCHQ to break the boundary which stopped it engaging in the bulk interception of internal UK communications. The Ripa requirement that one end of a communication must be outside the UK was a significant restriction when it was applied to phone calls using satellites, but it is no longer effective in the world of fibre-optic cables. "The point is that this is an island," the [Security Service] source said. "Everything comes and goes – nearly everything – down fibre-optic cables. You make a mobile phone call, it goes to a mast and then down into a fibre-optic cable, under the ground and away. And even if the call is UK to UK, it's very likely – because of the way the system is structured – to go out of the UK and come back in through these fibre-optic channels." Internet traffic is also liable to be routed internationally even if the message is exchanged between two people within the UK.
>
> "At one point, I was told that we were getting 85% of all UK domestic traffic – voice, internet, all of it – via these international cables."
>
> ["*MI5 feared GCHQ went 'too far' over phone and internet monitoring"* by Nick Davies, The Guardian, 22 June 2013].

84. Media reports of GCHQ having direct access to more than 200 fibre optic cables also undermines the rationale advanced by the Tribunal in *British Irish Rights Watch,* that it is "more necessary for additional care to be taken with regard to interference with privacy" in respect of domestic communications because of its relative lack of "knowledge of, and ... control over" external communications. If reports that GCHQ has access to 85% of all UK domestic traffic by way of international cables are accurate then, the Claimant submits, any distinction between the domestic and external interception regimes no longer appears to hold true.

85. If it is correct that GCHQ has direct and unmediated access to the contents of more than 200 fibre optic cables, this would involve an interception of that content within the meaning of section 2(2) of RIPA, whether or not GCHQ subsequently operated some filter to distinguish between access to communications data and the content of those communications. This is because the definition of "interception" makes plain that a communication is intercepted at the point at which some or all of the contents of the communication become "available, while being transmitted, to a person other than the sender or intended recipient of the communication". Therefore, any direct access to the fibre optic cables would necessarily involve an interception, whether or not GCHQ or another of the Respondents were only seeking to obtain communications data rather than the content of communications.

86. For the above reasons, the Claimant submits that the scheme for the interception of external communications under section 8(4) is not in accordance with law:

(1) RIPA fails to provide sufficient clarity concerning the conditions and circumstances in which persons in the UK, including the Claimant, are liable to have their communications intercepted.

(2) Consequently, the right to intercept and access material covered by a section 8(4) warrant, and the criteria by reference to which it is exercised can no longer be said to be sufficiently accessible and foreseeable to be in accordance with law as required by Article 8(2).

87. In addition, whether in breach of Article 8(2), or in breach of RIPA, it is apparent from the very scale of the material being obtained by the Respondents under Tempora (i.e. some 600m phone hits daily), that any warrant authorising such broad interception of millions of communications, including those of the Claimant, could not comply with the requirements of section 5(2)(b) RIPA or Article 8(2) ECHR. This is because it could not sensibly be described as either proportionate, or indeed necessary in a democratic society.

Interception of communications under section 1(5)(c) and/or access to communications data under section 22(5) RIPA.

88. While the available information indicates that Tempora has most likely been authorised by way of a warrant for the interception of external communications under section 8(4) RIPA, the Claimant anticipates that the Respondents may also seek to rely on certain other provisions of RIPA, namely:

(1) interception of stored communications (section 1(5)(c) of RIPA);

(2) one or more authorisations to access communications data (section 22 of RIPA).

89. Each of these potential justifications for accessing material through Tempora would be inadequate or flawed:

(1) If the Respondents suggest that accessing and obtaining communications content and data (including voice communications, emails, video conferencing etc.) stored on the servers of technology companies, through PRISM, Tempora or otherwise is lawful by virtue of section 1(5)(c) of RIPA, the Claimant submits:

- this is would be a misreading of the narrow scope of section 1(5)(c);

- further or alternatively, if section 1(5)(c) potentially does cover access to the numerous categories of communications content and data that may be stored on servers it does not comply with Article 8(2). This is because the extent to which and the manner in which it would permit access to material stored on servers would not be accessible or foreseeable and would contain no statutory safeguards against abuse.

(2) Secondly, it is possible that the Respondents have obtained one or more authorisations under section 22 RIPA to obtain communications data in respect of the Tempora material. Even if such authorisation was given, the process would involve daily access to the data and communications of millions of private individuals and is incapable of being justified under Article 8(2) ECHR. Such vast amounts of collection of personal communications could not be described as either necessary in a democratic society or proportionate.

Third Ground: In relation to Tempora, the Respondents acted unlawfully by granting NSA officials access to the <u>content</u> of communications to and from the Claimant as well as communications <u>data</u> relating to the Claimant

90. According to *The Guardian* report, dated 21 June 2013, the First Respondent gave 250 NSA analysts access to material obtained under the Tempora programme. The First Respondent also gave as many as 850,000 NSA employees and contractors access to GCHQ databases. "When it came to judging the necessity and proportionality of what they were allowed to look for," *The Guardian* reported, "would-be American users were told it was 'your call'."

91. In 2007, the Intelligence and Security Committee reported on intelligence-sharing arrangements between the UK and US in the context of extraordinary rendition (*Rendition* (Cm 7171, July 2007). Among other things, the Committee noted the extremely close working relationship

between the Respondents and the US intelligence community, particularly that between GCHQ and the NSA:

> We have been told by all three Agency Heads that their intelligence-sharing relationships with foreign liaison services are vital to counter the threat from international terrorism. The U.S. link is the most important, not least because of the resources the U.S. agencies command. The Chief of SIS told the Committee:
>
> > *The global resources of CIA, FBI and NSA [National Security Agency] are vast… The UK Agencies' long-developed relationships with U.S. intelligence agencies give them vital access to U.S. intelligence and resources. It is neither practical, desirable, nor is it in the national interest, for UK Agencies to carry out [counter-terrorism] work independently of the U.S. effort.*
>
> The Director of the Government Communications Headquarters (GCHQ) reiterated the value of the relationship to the UK, saying "Overall the benefit to the UK from this arrangement is enormous", and the Director General of the Security Service said "It is unimaginable that we could [cease sharing intelligence with the U.S.] because of the degree of importance of SIGINT and HUMINT and the intelligence they give us". (para 25)

92. At the same time, the Respondents also noted concerns over sharing information with foreign intelligence services where those services may be involved in serious wrong-doing. As the Director of the Security Service told the Committee:

> We have had to engage with countries which do not remotely – and I am not actually thinking of the United States – reach our standards of how we do things… The whole issue… of exchanging intelligence with foreign services with different standards and different laws is not new. It has become more acute and more difficult with our closest ally, but the principles apply across the board (ibid, para 162).

93. The report went on to describe, in outline only, the "control mechanisms" used by the Reports to govern their intelligence exchange with foreign liaison services, a combination of "caveats, assurances and Ministerial authorisations [para 170]" which give rise to a "system of safeguards to ensure that their intelligence does not result in torture or mistreatment" [para 171]. The Committee referred in particular to "extremely detailed" guidance issued to the Security Service and the Secret Intelligence Service in 2006, which was designed to "ensure that the Agencies' actions, where the possibility of torture or CIDT is foreseen, comply with their, and the UK's legal obligations" (para 175), and which also included a "comprehensive legal briefing, covering the

responsibilities of Agency staff under UK law and the responsibilities of the UK in international law" (para 174).[24]

94. The Committee noted that GCHQ "shares SIGINT collection data and intelligence reporting with the U.S. under a 60-year-old agreement" (*Rendition* (Cm 7171, July 2007) at para 178). In addition to applying the same mechanisms as the other Respondents, it reported that "GCHQ applies controls and safeguards tailored to its SIGINT function, to ensure that its actions are lawful and for the protection of sensitivities" (para 179), which it described as follows (emphasis added):

> 180. All SIGINT targeting is recorded and subject to regular external checks by independent commissioners. Furthermore, all end-product reporting is subjected to a sensitivity-checking process (known as "***") whenever there are concerns over legal, political or operational sensitivities. This process also ensures that the intelligence is accurate and its distribution is consistent with policy and legislative constraints.
>
> 181. GCHQ's long-established "***" process is the prime control mechanism by which GCHQ regulates the use of its intelligence by recipients. It requires all customers of GCHQ intelligence reports (***) to request authorisation from GCHQ to undertake executive action based upon the information they contain. The "***" process ensures that any use made of GCHQ reporting does not compromise sensitive SIGINT sources or relationships, and that it complies with UK policy and law.
>
> 182. GCHQ has provided to the Committee extracts from its guidance for "reporters" covering "***" and "***".131 This advises relevant staff of the steps they should take if they foresee a real possibility that unlawful behaviour might result from supplying intelligence to a foreign partner. It also sets out the safeguards for senior management to follow (such as the use of caveats) in such circumstances, including potential upward referral, ultimately to Ministerial level.
>
> 183. Sir David [Pepper, the Director of GCHQ] said:
>
> > *When we talk about use of intelligence, that would include passing it to liaison services. So <u>if anybody wants to do anything other than read the report and put it on a database,</u> they have to come to us for permission.*

95. The background outlined above indicates that there are insufficient safeguards in place for the sharing of personal communications data obtained from GCHQ with the NSA:

(1) From the ISC's description of relevant GCHQ safeguards, it is apparent that GCHQ's permission is not required in order for an NSA analyst to access or even retain and collect information passed to it by GCHQ.

[24] *Guidance on dealing with liaison services: Agency policy on liaison with overseas security and intelligence services in relation to detainees who may be subject to mistreatment.*

(2) Although the ISC report claims that "any use made of GCHQ report ... complies with UK policy and law", there is no indication as to how this compliance is overseen or ensured.

(3) Nor is there any reference to any allowance or additional safeguards being taken in light of the well-established US case law that communications data and the communications of foreign nationals generally do not receive the protection of the Fourth Amendment.

(4) In any event, the testimony of the GCHQ director provides corroboration for the situation described in *The Guardian* report, i.e. that it was left to NSA analysts to assess necessity and proportionality for themselves, with no allowance being made for the striking differences between US and UK law in relation to the privacy of communications.

(5) The ISC report concluded that:

> Theoretically, given the close working relationship between GCHQ and the National Security Agency (NSA), GCHQ intelligence could have been passed from the NSA to the CIA and could have been used in a U.S. rendition operation. However, GCHQ's legal safeguards and the requirement for explicit permission to take action based on their intelligence provide a high level of confidence that their material has not been used for such operations.

(6) In its statement on Alleged GCHQ Interception of Communications under the US PRISM Programme dated 17 July 2013, the Intelligence and Security Committee referred again to "the arrangements GCHQ has with its overseas counterparts for sharing information", as well as to substantive reports from GCHQ concerning "the formal agreements [between the NSA and GCHQ] that regulated access to [communications] material". It nonetheless concluded that it was satisfied that the arrangements governing information and intelligence sought from the US were lawful.

(7) In *R (Binyam Mohamed) v Secretary of State for Foreign and Commonwealth Affairs* [2010] EWCA Civ 65, however, Lord Neuberger noted serious concerns about the reliability of information provided by the Services in relation to intelligence-sharing:

> … it is also germane that the Security Services had made it clear in March 2005, through a report from the Intelligence and Security Committee, that "they operated a culture that respected human rights and that coercive interrogation techniques

> were alien to the Services' general ethics, methodology and training" (paragraph 9 of the first judgment), indeed they "denied that [they] knew of any ill-treatment of detainees interviewed by them whilst detained by or on behalf of the [US] Government" (paragraph 44(ii) of the fourth judgment). Yet, in this case, that does not seem to have been true: as the evidence showed, some Security Services officials appear to have a dubious record relating to actual involvement, and frankness about any such involvement, with the mistreatment of Mr Mohamed when he was held at the behest of US officials. I have in mind in particular witness B, but the evidence in this case suggests that it is likely that there were others. The good faith of the Foreign Secretary is not in question, but he prepared the certificates partly, possibly largely, on the basis of information and advice provided by Security Services personnel. Regrettably, but inevitably, this must raise the question whether any statement in the certificates on an issue concerning the mistreatment of Mr Mohamed can be relied on, especially when the issue is whether contemporaneous communications to the Security Services about such mistreatment should be revealed publicly. Not only is there some reason for distrusting such a statement, given that it is based on Security Services' advice and information, because of previous, albeit general, assurances in 2005, but also the Security Services have an interest in the suppression of such information (para 168).

It is notable that those concerns, highlighted by the Master of the Rolls, have never been publicly addressed by the Intelligence Services Commissioner in any of his annual reports.

96. The Claimant's third ground is the corollary of the first ground: just as there is no clear legal framework governing the Respondents' receipt of private communications from the NSA via PRISM; similarly, there is no such framework governing the Respondents' disclosure of private communications to the NSA and other foreign intelligence service liaisons.

97. Any such arrangements or guidance that do exist have not been made public. Nor do they have the necessary quality of "law". Accordingly, the Claimant submits that the interference to the privacy of its communications posed by the sharing of information between the Respondents and the NSA is not in accordance with law, contrary to Article 8(2) of ECHR.

Further Points

98. For the avoidance of doubt, the Claimant confirms the following:

    (1) Insofar as the Respondents' interference with the Claimant's communications not only interferes with its private life and correspondence, but also places a restriction on its right to

free expression, the points raised in relation to Article 8 of ECHR apply similarly with regard to Article 10.[25]

(2) Insofar as Tempora is principally focused on communications to and from foreign nationals or communicatons with persons outside the UK it is disproportionate and discriminatory. There is no rational basis for determining that such a measure is proportionate or necessary in a democratic society when directed at "external communications" by foreign nationals, if it would not be proportionate or necessary in relation to communications between persons located in the UK. Further or alternatively, such steps constitute unlawful discrimination of those foreign nationals.

F: PUBLIC HEARING ON PREMLIMINARY ISSUES

99. The Tribunal has the power to sit in public and to make public its preliminary rulings (*In the Matter of Applications Nos IPT/01/62 and IPT/01/77*, 23 January 2003, para 173). In certain circumstances, it is under a duty to do so:

> Indeed, purely legal arguments, conducted for the sole purpose of ascertaining what is the law and not involving the risk of disclosure of any sensitive information should be heard in public. The public, as well as the parties, has a right to know that there is a dispute about the interpretation and validity of the relevant law and what the rival legal contentions are (para 172).

100. The Claimant submits that this reasoning has been considerably strengthened by the judgment of the UK Supreme Court in *Bank Mellat v HM Treasury (No 1)* [2013] UKSC 38:

> The idea of a court hearing evidence or argument in private is contrary to the principle of open justice, which is fundamental to the dispensation of justice in a modern, democratic society. However, it has long been accepted that, in rare cases, a court has inherent power to receive evidence and argument in a hearing from which the public and the press are excluded, and that it can even give a judgment which is only available to the parties. Such a course may only be taken (i) if it is strictly necessary to have a private hearing in order to achieve justice between the parties, and, (ii) if the degree of privacy is kept to an absolute minimum...
>
> Even more fundamental to any justice system in a modern, democratic society is the principle of natural justice, whose most important aspect is that every party has a right to know the full case against him, and the right to test and challenge that case fully. A closed

[25] See, for example,. the *Joint Declaration On Surveillance Programs And Their Impact on Freedom of Expression*, dated 21 June 2013, issued by the UN Special Rapporteur on Freedom of Expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights.

hearing is therefore even more offensive to fundamental principle than a private hearing. At least a private hearing cannot be said, of itself, to give rise to inequality or even unfairness as between the parties. But that cannot be said of an arrangement where the court can look at evidence or hear arguments on behalf of one party without the other party ("the excluded party") knowing, or being able to test, the contents of that evidence and those arguments ("the closed material"), or even being able to see all the reasons why the court reached its conclusions. (Lord Neuberger at paras 2-3).

101. In *Bank Mellat,* the Supreme Court considered the circumstances in which "in certain limited and specified circumstances, a closed material procedure may, indeed must, be adopted by the courts" (para 8) - in that case, the position of a court hearing an appeal from closed proceedings dictated by CPR 79 pursuant to sections 66-67 of the Counter-Terrorism Act 2008. Delivering the majority judgment, the President of the Court set out certain conclusions regarding the use of closed proceedings, including:

68. First, where a judge gives an open judgment and a closed judgment, it is highly desirable that, in the open judgment, the judge (i) identifies every conclusion in that judgment which has been reached in whole or in part in the light of points made or evidence referred to in the closed judgment, and (ii) that the judge says that this is what he or she has done...

69. Secondly, a judge who has relied on closed material in a closed judgment, should say in the open judgment as much as can properly be said about the closed material which he has relied on. Any party who has been excluded from the closed hearing should know as much as possible about the court's reasoning, and the evidence and arguments it received. Further, the more the judge can say about the closed material in the open judgment, the less likely it is that a closed hearing will be asked for or accorded on an appeal. In cases where judges have to give a closed judgment, they should say in their open judgment, as far as they properly can, what the closed material has contributed to the overall assessment they have reached in their open judgment.

...

72. Fifthly, if the court decides that a closed material procedure appears to be necessary, the parties should try and agree a way of avoiding, or minimising the extent of, a closed hearing. This would also involve the legal representatives to the parties to any such appeal advising their clients accordingly, and, if a closed hearing is needed, doing their best to agree a gist of any relevant closed document (including any closed judgment below).

73. Sixthly, if there is a closed hearing, the lawyers representing the party who is relying on the closed material, as well as that party itself, should ensure that, well in advance of the hearing of the appeal, (i) the excluded party is given as much information as possible about any closed documents (including any closed judgment) relied on, and (ii) the special advocates are given as full information as possible as to the nature of the passages relied on in such closed documents and the arguments which will be advanced in relation thereto.

102. While the Claimant is mindful that the constraints upon the Tribunal are even greater than those imposed on other courts under CPR 79, it submits that the above conclusions apply *mutatis mutandis* to the Tribunal's own proceedings as follows:

(1) Any open rulings of the Tribunal should identify, so far as permissible, "every conclusion ... which has been reached in whole or in part in the light of points made or evidence referred to in the closed judgment";

(2) The Tribunal should say "as much as can properly be said about the closed material which [it] has relied on";

(3) Any party who has been excluded from the closed hearing should know as much as possible about the court's reasoning, and the evidence and arguments it received;

(4) Any open ruling should say as far as the Tribunal properly can, what the closed material has contributed to the overall assessment they have reached in their open judgment;

(5) The parties, under the direction of the Tribunal, should try and agree a way of avoiding, or minimising the extent of, closed hearing, including agreeing a gist of any relevant closed document;

(6) The lawyers representing the party who is relying on the closed material, as well as that party itself, should ensure that, well in advance of the hearing, the excluded party is given as much information as possible about any closed documents (including any closed judgment) relied on.

103. In addition, it is well-established that the Tribunal may also conduct open, *inter partes* proceedings addressing hypothetical assumptions of relevant facts: see e.g. *Frank-Steiner v Data Controller of the Secret Intelligence Service* (IPT/06/81/CH, 26 February 2008) at para 5:

> However in our judgment in IPT/01/62 and IPT/01/77 (referred to above) we concluded that there could and should be a public hearing in an appropriate case, for example where preliminary points of law were being canvassed, or where both parties wish to make submissions to the Tribunal, upon the basis of a hypothetical assumption of facts, which thus give away no actual information, as to what the Tribunal's approach should be to a given question. In accordance with that practice,

> we held a hearing on 21 September, at which Cherie Booth QC represented the Complainant and Jonathan Crow QC, leading Ben Hooper of Counsel, represented the Respondent. At that hearing it was assumed, for the purpose of that hearing only, that there are documents relating to Mr Rosbaud within the Respondent's files, and the arguments were presented on that basis. The Respondent had the opportunity to explain, on that hypothetical basis, not only the statutory scheme, but also why it is that the Respondent believes it has an obligation of confidence to an agent who has worked for or with the security services (as was assumed to be the case for the purposes of the argument), and that such confidence, absent any indication to the contrary, was not absolved by the death of the assumed agent. It is common ground in this case that if Mr Rosbaud was an agent he never disclosed this, even to his family, during his lifetime.

104. The Claimant submits that such an approach is clearly necessary in the present case. The disclosure of internal NSA documents revealing the sweeping extent of NSA and GCHQ surveillance of everyday communications has precipitated an international crisis, and has been of very substantial interest in the US, UK and Europe. It has prompted direct responses from the US President, the British Prime Minister, the British Foreign Secretary and many other very senior political figures.

105. If true, the allegations indicate that the Respondents have been complicit in unlawful surveillance on a scale unprecedented in human history. In its decision in the *Frank-Steiner* case, the Tribunal described itself as "an important bulwark for the citizen" (para 14).

106. If, therefore, residents of the UK and elsewhere whose communications have been swept up in PRISM and Tempora are to have any faith in these proceedings, it is incumbent upon the Tribunal to arrange its procedures within the existing legal framework in such a way as to maximise public confidence in the outcome. As the Master of the Rolls observed in *Al Rawi and others v Security Service and others* [2010] EWCA Civ 482 at para 56:

> While considering practical considerations, it is helpful to stand back and consider not merely whether justice is being done, but whether justice is being seen to be done. If the court was to conclude after a hearing, much of which had been in closed session, attended by the defendants, but not the claimants or the public, that for reasons, some of which were to be found in a closed judgment that was available to the defendants, but not the claimants or the public, that the claims should be dismissed, there is a substantial risk that the defendants would not be vindicated and that justice would not be seen to have been done. The outcome would be likely to be a pyrrhic victory for the defendants, whose reputation would be damaged by such a process, but the damage to the reputation of the court would in all probability be even greater.

107. The Claimant therefore asks that the Tribunal hold a public, *inter partes* hearing to determine the following preliminary issues:

(1) What, if any, legal framework governs the receipt of intercepted communications and/or communications data from a foreign intelligence service in respect of communications originating from and/or received in the UK? If such a framework does exist, is it compatible with Article 8?

(2) What, if any, legal framework governs the granting of access of intercepted communications and/or communications data to a foreign intelligence service? If such a framework does exist, is it compatible with Article 8?

(3) Does RIPA, through the definition of "external communication" in section 20 or otherwise, provide sufficient clarity concerning the conditions and circumstances in which UK residents are liable to have their communications intercepted?

(4) Is the power to access "stored communications" under section 1(5)(c) RIPA without an interception warrant compatible with Article 8 ECHR?

Need for Tribunal to conduct effective investigation into allegations

108. The Claimant notes that the Tribunal has the power under section 68(2) to require the relevant Commissioners to "provide the Tribunal with all such assistance (including the Commissioner's opinion as to any issue falling to be determined by the Tribunal) as the Tribunal think fit". In the present case, the Claimant submits that both the Intelligence Services Commissioner and the Interception of Communications Commissioner appear to be well-placed to assist the Tribunal with its investigations. Indeed, it appears that the Interception of Communications Commissioner has already commenced his own investigation into the recent media reports regarding PRISM and Tempora.[26]

[26] Press release from the Interception of Communications Commissioner, *Sir Anthony May's response to the Article Published in the Independent*, 16 July 2013, included the following: "I can confirm that I am currently conducting an investigation into the various recent media reports relating to disclosures about interception attributed to Edward Snowden. This will take some time. I am also, and independently of the recent media reports, undertaking a series of investigations which have a bearing on various aspects of recent media debate. It is not appropriate to give details of this for the moment because, as will be appreciated, the subject matter is sensitive and subject to statutory constraint, and because my statutory role is to report to the Prime Minister. Nor do I intend to report on these topics until the various strands of my investigations are complete. But I shall in due course report on these and related topics to the Prime Minister.

109. Paragraph 8.3 of the Acquisition and Disclosure of Communications Data Code of Practice further provides:

> Should the Commissioner establish that an individual has been adversely affected by any wilful or reckless failure by any person within a relevant public authority exercising or complying with the powers and duties under the Act in relation to the acquisition or disclosure of communications data, he shall, subject to safeguarding national security, inform the affected individual of the existence of the Tribunal and its role. The Commissioner should disclose sufficient information to the affected individual to enable him or her to effectively engage the Tribunal.

There is, however, no corresponding provision under the Interception of Communications Code of Practice. The Claimant submits, moreover, that the threshold identified by para 8.3 is too low: the unlawful acts of a public authority may give rise to a serious breach of an individual's right to private communications, without that breach being the result of a "wilful or reckless" failure.

110. In the circumstances, the Claimant submits that the Tribunal should direct the relevant Commissioners to assist the Tribunal with its investigation of the Claimant's claim.

G. RELIEF

111. For the reasons given above, the Complainant seeks the following relief:

(1) a public and *inter partes* hearing on the preliminary issues;

(2) an open judgment on the preliminary issues;

(3) a declaration that the Respondents acted unlawfully in breach of their statutory duties under RIPA and the HRA, and in violation of the Claimant's rights under Article 8 ECHR.

(4) Any further relief the Tribunal thinks appropriate.

MATTHEW RYDER QC
Matrix Chambers

ERIC METCALFE
Monckton Chambers

JAMES WELCH

Legal Director, Liberty

Case No.IPT/13/77/H

IN THE MATTER OF A COMPLAINT TO

THE INVESTIGATORY POWERS TRIBUNAL

Under the Human Rights Act 1998

BETWEEN:

LIBERTY

(THE NATIONAL COUNCIL

FOR CIVIL LIBERTIES)

Claimant

and

THE SECURITY SERVICE

THE INTELLIGENCE SERVICE

GOVERNMENT COMMUNICATIONS HEADQUARTERS

Respondents

WRITTEN SUBMISSIONS OF LIBERTY

Liberty

Liberty House

26-30 Strutton Ground

London SW1P 2HR