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

B E T W E E N:

PRIVACY INTERNATIONAL
BYTES FOR ALL

Claimants

and

(1) SECRETARY OF STATE FOR THE FOREIGN AND COMMONWEALTH OFFICE
(2) THE SECRETARY OF STATE FOR THE HOME OFFICE
(3) THE SECRET INTELLIGENCE SERVICE
(4) THE SECURITY SERVICE
(5) GOVERNMENT COMMUNICATION HEADQUARTERS
(6) THE ATTORNEY GENERAL

Respondents

SKELETON ARGUMENT SERVED BY PRIVACY INTERNATIONAL AND BYTES FOR ALL

For preliminary issues hearing: 14 July 2014, time estimate 5 days

---

Introduction

1. This skeleton argument is served on behalf of Privacy International ("PI") and Bytes for All ("B4A").

2. This case is about mass surveillance of the population of the UK, and the citizens of most other countries of the world. In essence, the IPT is asked to decide whether HM Government can issue a general warrant for the universal search, seizure, and sophisticated automatic analysis of communications and their sharing with foreign governments. It is also about the Government's ability to obtain virtually all communications of UK residents from the Intelligence Services of other states without requiring any warrant at all, and subject only to a general power to act "*in the interests of national security*."

3. The case has been brought because of the disclosure by Edward Snowden and various newspapers of bulk interception operations in the UK and USA, involving the collection, analysis and use of everyone's communications and the sharing of that data

between the UK and USA and other countries. The scale of the mass surveillance now taking place was unthinkable even a few years ago. It was introduced without public debate or knowledge.

4. The fact that such bulk collection and sharing is even possible reflects rapid technological change. All or most internet and telephone communications, without meaningful limits, are now being collected, stored and analysed by the Security and Intelligence Services, regardless of any individual ground for suspicion. This raises important issues of law and principle.

5. Despite its reassuring public words, when speaking privately GCHQ has repeatedly expressed its pleasure at the light UK oversight regime that has permitted this scale of mass interception. GCHQ describes the UK legal regime as a "*selling point" for the Americans*." GCHQ is "*less constrained by NSA's concerns about compliance*" and dedicated to exploiting "*to the full our unique selling points of … the UK's legal regime*." In a briefing, one of GCHQ's senior legal advisers noted "*we have a light oversight regime compared with the US."* The IPT has "*so far always found in our favour"*. See King para. 144

6. This case is therefore also about the oversight regime for the Security and Intelligence Services, including the IPT itself. The IPT has an important constitutional role. In RIPA Parliament granted broad powers intended to be used in secret. Parliament recognised the real risk that Ministers and the Services might overreach. It thus created the IPT as a judicial bulwark to ensure that neither Ministers, nor the Services, carry out surveillance that is inconsistent with our constitutional principles.

Judicial scrutiny of state surveillance

7. The extent of the surveillance now taking place is novel. But the issues before the IPT are not. It has always been the role of the judges to protect the individual against broad government intrusions into privacy.

8. The concerns expressed by the Claimants in this case are not fine legal problems only apparent after a careful examination of Delphic Strasbourg case law. They are issues

that judges have dealt with for several hundred years and are now addressing again across the common law world.

General warrants and the common law

9. George III opened Parliament on 19 April 1763. In his speech, he praised the Treaty of Paris, ending the Seven Years War but ceding numerous colonies to France. The speech was the work of Lord Bute, the former Prime Minister.

10. John Wilkes penned a savage criticism of the speech. The critique was published four days later in issue 45 of *The North Briton*. The choice of issue 45 was no accident: Bute was popularly associated with the Jacobite rising of 1745 by Bonnie Prince Charlie against George II.

11. George III considered the publication a personal insult and seditious. He ordered that a general warrant be issued to identify the author, publisher, printer and their associates.

12. In the language of Mr Farr, the general warrant was no doubt thought necessary because "*any regime that… only permitted interception in relation to specific persons or premises, would not have allowed adequate levels of intelligence information to be obtained and would not have met the undoubted requirements of intelligence for the protection of national security*" (para. 151).

13. Lord Halifax, the Secretary of State, complied:

> "On 19 April 1763, the King made a speech from the throne… on the 23 April 1763 a certain seditious and scandalous libel or composition… was unlawfully and seditiously composed, printed and published concerning the King and his said speech… That the Earl of Halifax was then… one of His Majesty's principal Secretaries of State; and that information was given to him of the said publication of the aforesaid libel… he thereupon in due manner issued his warrant in writing under his hand and seal… by which warrant the said earl did in His Majesty's name authorise and require them, taking a constable to their assistance, to make strict and diligent search for the said authors, printers and publishers of the aforesaid seditious libel… and them or any of them having found, to apprehend and seize, together with their papers, and to bring in safe custody before the said earl, to be examined

concerning the premises, and to be further dealt with according to law" (*Money v Leach* (1765) 3 Burrow 1742, 97 ER 1075).

14. The King's agents duly arrested Wilkes, and sent him to the Tower. They then crossed London breaking into and searching dozens of premises and arresting almost 50 other people.

15. In a series of decisions, the Courts declared the general warrant void, and awarded compensation to the victims. In *Huckle v Money* (1763) 2 Wilson 205, 95 ER 768 Lord Pratt CJ noted that:

> "To enter a man's house by virtue of a nameless warrant, in order to procure evidence, is worse than the Spanish Inquisition; a law under which no Englishman would wish to live an hour; it was a most daring public attack made upon the liberty of the subject".

16. In *Wilkes v Wood* (1763) Lofft 1, 98 ER 489 the Lord Chief Justice said:

> "The defendants claimed a right, under precedents, to force persons houses, break open escrutores, seize their papers, &c. upon a general warrant, where no inventory is made of the things thus taken away, and where no offenders names are specified in the warrant, and therefore a discretionary power given to messengers to search wherever their suspicions may chance to fall. If such a power is truly invested in a Secretary of State, and he can delegate this power, it certainly may affect the person and property of every man in this kingdom, and is totally subversive of the liberty of the subject."

17. Similarly, in *Entick v Carrington* (1765) 2 Wilson 275 a further general warrant issued by Lord Halifax led to an award of damages. The argument of Treasury Counsel was the familiar refrain:

> "Supposing the practice of granting warrants to search for libels against the State be admitted to be an evil in particular cases, yet to let such libellers escape who endeavour to raise rebellion is a greater evil, and may be compared to the reasoning of Mr Justice Foster in the case of pressing where he says, "that war is a great evil, but it is chosen to avoid a greater. The practice of pressing is one of the mischiefs war brings with it; but it is a maxim in law and good policy too, that all private mischiefs must be borne with patience, for preventing a national calamity," &c."

18. The Lord Chief Justice disagreed:

> "The defendants have no right to avail themselves of the usage of these warrants since the Revolution, and if that would have justified them they have not averred it in their plea, so it could not be put, nor was in issue at the trial; we can safely say there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society; for papers are often the dearest property a man can have."

19. These were not ground breaking decisions. In 1644, Coke condemned general warrants, as did Sir Matthew Hale in 1736. Hale explained that a "*general warrant to search in all suspected places is not good*" and "*not justifiable*" because they gave such discretion to mere Crown servants "*to be in effect the judge*" (History of the Pleas of the Crown, p. 150). The effect of these decisions can be seen today in the modern case law on Article 8 ECHR.

20. The difference between 'internal' and 'external' is not new either. The Revenue Act 1767 was part of a package of measures to deal with the troublesome colonies. Parliament concluded that general writs were essential in such parts and sought to legislate to secure their availability for use outside of the British Islands. Section 10 provided:

> "… it is doubted whether such officers can legally enter houses and other places on land, to search for and seize goods, in the manner directed by the said recited acts: To obviate which doubts for the future, and in order to carry the intention of the said recited acts into effectual execution, be it enacted, and it is hereby enacted by the authority aforesaid, That from and after the said twentieth day of November, one thousand seven hundred and sixty seven, such writs of assistance, to authorise and impower the officer of his Majesty's customs to enter and go into any house, warehouse, shop, cellar, or other place, in the British colonies of plantations of America, to search for and seize prohibited or uncustomed goods, in the manner directed by the said recited acts, shall and may be granted by the said superior or supreme courts of justice having jurisdiction within such colony or plantation respectively."

21. Again, to use the language of Mr Farr, it was no doubt thought that general warrants were needed because the government did not have the "*sufficient control and considerable resources to investigate individuals and organisations*" it had in the British Islands, and it was thus not "*feasible to adopt an interception regime that requires either a particular person, or set of premises, to be identified before interception can take place*" (para. 144).

22. The subsequent events are well known. The American colonial courts continued to refuse to issue general writs, or attempts at enforcement failed. The American Revolution swiftly followed as a result. The Fourth Amendment ultimately prohibited the use of general warrants.

Development of modern communications

23. In the 1700s, if the state wished to read correspondence or private papers, it had to take control of a physical item. In the last century, that ceased to be the case. It took the law, particularly in the UK, a long time to catch up.

24. In Prohibition era America, bootlegging was common. Without judicial approval, federal agents installed telephone wiretaps in the building used by a suspected bootlegger, and in the public telephones in the streets around his home. The bootlegger was convicted with evidence obtained by the wiretaps.

25. By 5-4 the US Supreme Court held that the absence of judicial authorisation did not breach the Fourth Amendment (*Olmstead v United States* (1928) 277 US 438). In US constitutional law, the dissenting opinion of Justice Brandeis has a status equivalent to that of Lord Atkin in *Liversidge v Anderson* [1942] AC 206. Justice Brandeis well understood the nature of modern invasions of privacy:

> "When the Fourth and Fifth Amendments were adopted, "the form that evil had theretofore taken" had been necessarily simple. Force and violence were then the only means known to man by which a Government could directly effect self-incrimination. It could compel the individual to testify -- a compulsion effected, if need be, by torture. It could secure possession of his papers and other articles incident to his private life -- a seizure effected, if need be, by breaking and entry. Protection against such invasion of "the sanctities of a man's home and the privacies of life" was provided in the Fourth and Fifth Amendments by specific language. … But "time works changes, brings into existence new conditions and purposes." Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.
>
> Moreover, "in the application of a constitution, our contemplation cannot be only of what has, been but of what may be." The progress of science in furnishing the Government with means of espionage is not likely to stop with

> wiretapping. Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions. "*That places the liberty of every man in the hands of every petty officer*" was said by James Otis of much lesser intrusions than these. To Lord Camden, a far slighter intrusion [in *Entick v Carrington*] seemed "*subversive of all the comforts of society*." Can it be that the Constitution affords no protection against such invasions of individual security?"

26. In consequence:

> "The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded and all conversations between them upon any subject, and, although proper, confidential and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wiretapping."

27. The laudable motive provides no excuse:

> "… it is also immaterial that the intrusion was in aid of law enforcement. Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well meaning but without understanding."

28. The US Supreme Court quickly confined *Olmstead* to its facts. It formally reversed the decision in *Katz v United States* (1967) 389 US 347. The Court by then understood that modern means of communication were equally deserving of protection as physical papers or correspondence. The medium was irrelevant, as was the absence of physical intrusion:

> "… a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."

29. Nor did it matter that the wiretap was limited, justified and proportionate:

> "It is apparent that the agents in this case acted with restraint. Yet the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer. They were not required, before commencing the search, to present their estimate of probable cause for detached scrutiny by a neutral magistrate. They were not compelled, during the conduct of the search itself, to observe precise limits established in advance by a specific court order. Nor were they directed, after the search had been completed, to notify the authorizing magistrate in detail of all that had been seized."

UK and Convention cases

30. Modern domestic law on surveillance begins with the judgment of Sir Robert Megarry in *Malone v Commissioner of Police for the Metropolis*, referred to in *Malone v UK* (1984) 7 EHRR 14. At that time, telephone tapping was entirely unregulated, occurred in secret, and it was still the official position of HM Government to pretend that MI6 and GCHQ did not exist.

31. Sir Robert Megarry expressed grave concerns about the absence of safeguards or proper judicial control. The Government disagreed. Parliament was told that the population should "*repose their trust in the Ministers concerned to exercise that control responsibly and with a right sense of balance between the value of interception as a means of protecting order and security and the threat which it may present to the liberty of the subject*" [37]. The Strasbourg Court disagreed, holding that a proper statutory basis was required. The result was the Interception of Communications Act 1985, which created the predecessor to the IPT and the system of certificated warrants now found in section 8(4) of RIPA.

32. Also in 1985, Cathy Massiter (a former MI5 officer) disclosed that Patricia Hewitt and Harriet Harman, then senior employees of Liberty, had been subject to Security Service surveillance, and that Liberty itself "*was classified as a communist controlled subversive organisation*" (*Hewitt & Harman v UK* (1989) 14 EHRR 657 at [15]). The Commission held that the absence of any proper or lawful framework for the Security Service was a breach of Article 8. Compensation was paid and the Security Service Act

1989 was introduced. Five years later the existence of GCHQ and MI6 was officially acknowledged by the passing of the Intelligence Services Act 1994.

33. By 1999, it had become clear that general surveillance of telephone calls between the UK and the Republic of Ireland was taking place. Liberty and others made a complaint to the Tribunal set up under the 1985 Act. Nothing is known about the Tribunal's decision, save that it held that there was no contravention of the relevant legislation.

34. In 2001 the new IPT considered a further complaint by Liberty and others on the same factual basis (IPT/01/77). The IPT decided that the Section 8(4) regime under RIPA, together with the Code of Practice was compliant with Article 8 ECHR and the law was sufficiently accessible and foreseeable.

35. Since then, the Strasbourg Court has ruled four times on bulk surveillance and the associated data collection and retention issues. These cases each confirm that any kind of bulk data collection and analysis, especially if automated, poses grave risks and must be very narrowly confined:

    a. First, in *Weber & Saravia v Germany* (2008) 46 EHRR SE5 the Court confirmed the lawfulness of a German "strategic monitoring" system that collected wireless satellite telecommunications (but not wired communications) amounting to up to 10% of calls subject to extremely stringent safeguards.

    b. Secondly, in *Liberty v UK* (2009) 48 EHRR 1 the Strasbourg Court found a further breach of Article 8 by the UK on prescribed by law grounds. The 1985 Act did not provide a clear or foreseeable basis for the bulk interception of communications. The Strasbourg Court noted but did not consider the correctness of IPT/01/77, or its application in the present context.

    c. Thirdly, in *S v UK* (2009) 48 EHRR 50 the Grand Chamber held that the mere collection and retention and DNA fingerprints of innocent people was contrary to Article 8 ECHR. Collecting such information about innocent people failed to strike a fair balance between public and private interest. The UK ran the same arguments as in this case: "*the retention could not be considered*

as having any direct or significant effect on the applicants unless matches in the database were to implicate them in the commission of offences on a future occasion" [121]. Retaining and searching the records of innocent people on the database was necessary "*to increase the size and, therefore, the use of the database in the identification of offenders in the future*" [123]. The innocent had nothing to fear. All these arguments were rejected. The UK had "*overstepped any acceptable margin of appreciation in this regard"* [125] even though the DNA database was undoubtedly a valuable tool for detecting and prosecuting serious criminals. The fact that the state finds data collection and analysis useful for proper purposes marks the start of the analysis, not the end.

d. Finally, in *MK v France* (18 April 2013) the Strasbourg Court held that the French national digital fingerprint database was unlawful. The French court held that "*retaining the fingerprints was in the interests of the investigating authorities, as it provided them with a database comprising as full a set of references as possible. Furthermore, this measure was not prejudicial to the applicant thanks to the confidentiality of the database, which prevented any impact on the applicant's private or social life*" [13]. France argued that bulk collection and automated searching of fingerprints was a good idea because it would protect the innocent by ruling out their involvement in crimes, and prevent identity theft. The Strasbourg Court again disagreed. It noted (contrary to the Respondents' position in this case) that the need for safeguards *"is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes*" [32]. The Court noted that the logic of the arguments put forward by France would justify universal collection and automated processing of everyone's fingerprints: "… *would in practice be tantamount to justifying the storage of information on the whole population of France, which would most definitely be excessive and irrelevant*" [37].

36. Meanwhile, the Grand Chamber of the CJEU has held in C-293/12 *Digital Rights Ireland* that Directive 2006/24/EC requiring the retention of metadata (not but content)

is unlawful. The Directive was incompatible with the right to privacy contained in Articles 7 and 8 of the EU Charter.[1]

37. The Advocate General advised that the Directive should be quashed, due the absence of any sufficient or proper safeguards:

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

38. The Grand Chamber agreed. It accepted that data retention was valuable "*to contribute to the fight against serious crime and thus, ultimately, to public security*" [41]. But having cited the relevant Strasbourg case law, it noted the dangers of collecting and using personal data in bulk:

> "37. It must be stated that the interference caused by Directive 2006/24 with the fundamental rights laid down in Articles 7 and 8 of the Charter is, as the Advocate General has also pointed out, in particular, in paragraphs 77 and 80 of his Opinion, wide-ranging, and it must be considered to be particularly serious. Furthermore, as the Advocate General has pointed out in paragraphs 52 and 72 of his Opinion, the fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."

[1] "Article 7: Respect for private and family life
Everyone has the right to respect for his or her private and family life, home and communications.
Article 8: Protection of personal data
1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority."

39. Further, "*the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony. It therefore applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives… It therefore entails an interference with the fundamental rights of practically the entire European population*" [56].

40. The Grand Chamber held that the Directive was unlawful. It placed particular emphasis on:

    a. The comprehensive nature of the bulk collection of data ('*vast quantity*" [66]), even when there is no evidence that a person might have a link with serious crime [58].

    b. The absence of any exceptions to protect persons whose communications are subject to special protection, such as lawyers and doctors [58].

    c. The absence of any relationship between the data retained and a particular geographical zone, or people likely to be involved in serious crime [59].

    d. "*Above all*", the absence of any prior review by a court or independent administrative body [62].

    e. The absence of any safeguards to ensure that data is retained within the EU.

41. The analysis in each of these decisions is remarkably similar to the old general warrant cases, updated to reflect the types and scale of data collection and monitoring now possible as a result of technological change.

US litigation

42. These issues are also being litigated in the US. At present, there are numerous cases before the US courts about the lawfulness of the NSA's blanket US telephone call metadata collection and related issues:

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

> "… people have a reasonable expectation of privacy that is violated when the Government, without any basis whatsoever to suspect them of any wrongdoing, collects and stores for five years their telephony metadata for purposes of subjecting it to high-tech query and analysis without judicial approval."
>
> "people in 2013 have an entirely different relationship with phones than they did thirty-four years ago."
>
> "records that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic – a vibrant and constantly updating picture of the person's life."

b. On 3 June 2014, another US District Court judge declined, with considerable reluctance, to follow *Kayman* because he considered himself bound by a US Supreme Court decision that call records (as opposed to content or location information) are not sufficiently private to justify constitutional protection[2]:

> "Judge Leon's decision should serve as a template for a Supreme Court opinion. And it might yet. Justice Sotomayor is inclined to reconsider *Smith*, finding it "*ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks*." *See U.S. v. Jones,* 132 U.S. 945, 957 (2012) (Sotomayor, J., concurring). The Fourth Amendment, in her view, should not "*treat secrecy as a prerequisite for privacy*." *Id.*
>
> But *Smith* was not overruled, and it continues – along with the Circuit decisions discussed above – to bind this Court. This authority constrains the Court from joining *Klayman"* (*Smith v Obama*).

c. Finally, on 11 June 2014, the US Court of Appeals for the Eleventh Circuit held that the collection of location information about a person from mobile

[2] It is common ground that this principle does not apply to the Convention case law. It is accepted by the Respondents that the collection of content or metadata both involve an interference under Article 8(1).

phone records was a search requiring prior judicial authority (*Davis v USA*). After reviewing the history and Supreme Court authorities set out above, the Court of Appeals held that "*warrantless gathering of… cell cite location information violated* [Davis's] *reasonable expectation of privacy*". The Court emphasised the dangers to privacy in the use of modern communications devices, requiring the full protection of the law. The first danger is with the aggregation of information to build a mosaic of information that can be logged and analysed. The second danger is that such information is sensitive, private and very revealing. Until the modern age, it would never have been collected, still less would it have been available to public officials:

> "As the circuit and some justices reasoned, the car owner can reasonably expect that although his individual movements may be observed, there will not be a "tiny constable" hiding in his vehicle to maintain a log of his movements…
>
> In contrast, even on a person's first visit to a gynecologist, a psychiatrist, a bookie, or a priest, one may assume that the visit is private if it was not conducted in a public way. One's cell phone, unlike an automobile, can accompany its owner anywhere. Thus, the exposure of the cell site location information can convert what would otherwise be a private event into a public one.
>
> … There is a reasonable privacy interest in being near the home of a lover, or a dispensary of medication, or a place of worship, or a house of ill repute."

Issues (i) – (iii): Access to US PRISM/ "UPSTREAM collection"

Factual background

43. Preliminary issues (i)-(iii) proceed on the basis of the agreed factual premises. The Tribunal does not need to make factual determinations to resolve them. It is, however, not possible to determine, in any meaningful way, whether the alleged activities of the UK's Intelligence Services are "*in accordance with*" or "*prescribed by law*" without some sense of what is meant by the Claimants' communications and/or communications data being "*obtained*" pursuant to the US's "*PRISM*" and "*UPSTREAM*" programmes, and how they may, in turn, be "*obtained*" by the UK Intelligence Services.

The US's PRISM and UPSTREAM collection programs

44. It is now clear that the UK's Intelligence Services can, at least in principle, obtain extensive access to the communications and communication data of UK residents that have been intercepted or obtained by the US National Security Agency ("the NSA"). That access includes access to both the raw data itself (for example being able to directly search and extract bulk intercepted communications which may never be analysed by the NSA) and access to refined data that has been analysed and collated by the NSA.

45. The NSA obtains communications pursuant at least to two broad programs: PRISM and "UPSTREAM collection". Both are authorised by the US's Foreign Intelligence Surveillance Act ("FISA") §1881a. Pursuant to FISA §1881a the NSA can be authorised to gather intelligence on "*persons reasonably believed to be located outside the United States to acquire foreign intelligence information*" provided that the power is not used intentionally to target US citizens reasonably believed to be located outside the US. Subject to this restriction, the NSA can gather "*foreign intelligence*" on anyone located anywhere in the world. As a matter of US law, the NSA can engage in bulk collection of a wide range of communications of UK residents.

46. The information currently available about PRISM is set out in the witness statement of Eric King. In essence PRISM enables the NSA to obtain information from some of the world's largest internet companies, such as Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple. Information obtained is likely to include the emails, web-searches, phone calls, photos, videos made or sent by individuals in the UK who use any of the products of those companies, or who communicate with individuals using, for example, a Gmail account or other products of internet companies based in the US.

47. The information currently available about the NSA's UPSTREAM collection programme is also set out in the witness statement of Eric King at para. 102. UPSTREAM collection involves the direct interception of communications during transmission. It is described, according to NSA presentation slides published in *The Guardian*, as being the "*collection of communications on fiber cables and infrastructure as data flows past*". It is estimated that fibre optic cables carry 90% of the world's

communications and, as another slide states, much of that will "*flow through the US*". That is because the US is the "*world's telecommunications backbone*" and "*a target's phone calls, e-mail or chat will take the cheapest path and not the physically most direct path... [C]ommunications [of individuals outside the US] could easily be flowing into and through the US*". Moreover, many companies, such as Google, Facebook and Twitter, have servers in the US and all messages and searches that use their products will travel through the US. The NSA has publicly accepted that it engages in bulk interception of communications of people outside the US and has stated publicly that "*the US is the principal hub in the world's telecommunication system and FISA is designed to allow the US government to acquire foreign intelligence while protecting the civil liberties and privacy of Americans*" (see Farr Exhibits Tab 9 p 234).

48. By using a combination of overseas access points, intercepting communications as they pass through the US and obtaining information from telecommunication and internet companies, the NSA is able to access a large majority of the world's communications and communication data (King para. 90). That is access to a vast quantity of personal information about individuals across the globe: the contents of their phone calls, emails, texts and other forms of communication, the history of their web-searches, their location when they have made and received calls or sent emails. It will include the communications and communication data of UK residents who use the internet, and it will include communications which, are on any view, entirely "*internal*" to the UK, such as an email between two people in London. That is because a great many of those or emails will flow through the fibre optic cables which the NSA is able to access, or will be stored by a telecommunications company in the US to which the NSA has access.

The UK Intelligence Services obtaining communication material from the US' PRISM and UPSTREAM collection programs

49. Assume two Londoners exchange emails. The email may beintercepted by the NSA as it passes through US cables or be obtained from an internet company. There are three ways the UK Intelligence Services could obtain the email from the NSA:

    (i) the NSA could provide the emails, unsolicited, to the Intelligence Services;

(ii) the Intelligence Services could ask the NSA to intercept or otherwise obtain the contents of the emails or the associated metadata in relation to a named individual or class of individuals located in the UK, and the communication or communication data could be provided at the UK Intelligence Services' request;

(iii) the NSA could give the UK Intelligence Services access to its bulk intercepted material and the Intelligence Services could search, for themselves (whether supervised or unsupervised), for the communications or communication data of named individuals located in the UK or using some other identifier or search term.

50. The evidence suggests that information is obtained in all of these ways. What is known about the level of cooperation between GCHQ and NSA is set out in the witness statement of Eric King at 81. It appears that, at least at times, they operate, for all intents and purposes, as one agency. As one senior member of Britain's intelligence community told *The Guardian*[3] *"[w]hen you get a GCHQ pass it gives you access to the NSA too. You can walk into the NSA and find GCHQ staff holding senior management positions, and vice versa"*, and many intelligence facilities run by NSA and GCHQ are jointly operated. Indeed the intention of the UK and US has since 1946 been that, where possible, communications each obtained would be exchanged. The agreement was made public in 2010. It appears from Charles Farr's statement [25] that it continues to govern the relationship between the UK and US intelligence services. The agreement provides that "*foreign communications*" each obtains will be exchanged and "*such exchange will be unrestricted on all work undertaken except when specifically excluded from the agreement at the request of either party and with the agreement of the other. It is the intention of each party to limit such exceptions to the absolute minimum and to exercise no restrictions other than those reported and mutually agreed upon*" (Farr Exhibit Tab 7 p 141). For material obtained by the US, communications relating to British residents will be "*foreign communication*". According to the agreement it is thus intended that such communications be shared "*unrestricted*" with the UK government. In an essay by an ex-NSA employee marked UNCLASSIFIED and approved for public release by the

[3] http://www.theguardian.com/world/2013/dec/02/turing-snowden-transatlantic-pact-modern-surveillance?CMP=twt_gu

NSA's office of Pre-Publication Review, it was stated that: "*If you are a citizen of the UK, Canada, New Zealand, or Australia, you may also be glad, because everything the NSA collects is by default shared with your government*."[4]

51. It appears that that unrestricted sharing of information applies both to individual pieces of information and the product of bulk interception. It has been reported that the material intercepted by GCHQ under its TEMPORA program is analysed by a team consisting of 250 NSA analysts and 300 GCHQ analysts and that the NSA has full access to the material (King para. 86). An April 2013 NSA document suggests that GCHQ was seeking broad authority to access the NSA's PRISM and UPSTREAM collection data, and indicated that, at least during the Olympics, 100 GCHQ operatives were given unsupervised access to PRISM (King para. 122).

52. For present purposes neither the precise detail of the US's UPSTREAM interception and PRISM programs, nor the manner in which its product is obtained by the UK Intelligence Services, requires determination. To test the issues in dispute between the parties it can be assumed that the US intercepts and stores communications and communications data traveling through fibre optic cables over which it has access, as well as accessing material stored by telecommunications companies in the US. The NSA will therefore be able to access the majority of web-searches, emails and other internet communications sent or undertaken in the UK including those which the sender and recipient are at all times in the UK. It can also be assumed, for the purpose of determining the issues of principle, that the UK Intelligence Service is given unrestricted access to the communications and communications data intercepted or otherwise obtained by the US and, at times, is provided with individual pieces of intelligence information, whether pursuant to a specific request or unsolicited.

Issue (i)

53. Issue (i) is whether the statutory regime set out at paragraphs 36-76 of the Respondents' Open Response is adequate to ensure that any obtaining of communications or communication data of UK residents by the Intelligence Services from the US' PRISM or "UPSTREAM collection" programmes is "*in accordance with the law*" pursuant to ECHR Art 8. For the purposes of the argument the Claimants will

[4] http://lorensr.me/nsa-an-inside-view.html

focus upon intercepted communication rather than communication obtained by the US from telecommunications companies (so as to avoid having to repeat the formulation "*intercepted or otherwise obtained*") but the argument of principle applies equally to both.

54. The statutory regime relied on by the Respondents is the Security Services Act 1989 and the Intelligence Services Act 1994, as read with the Counter-Terrorism Act 2008, the Human Rights Act 1998, the Data Protection Act 1998 and the Official Secrets Act 1989 (Respondents' Open Response [36]-[56]). If the "*in accordance with the law*" test developed in the Strasbourg jurisprudence governing interception of communications (set out in cases such as *Malone v UK* (1985) 7 EHRR 14, *Weber v Germany* (2008) 46 EHRR SE5 and *Liberty v UK* (2009) 48 EHRR 1)), applies to communications and/or communications data obtained by the UK Intelligence Services from the US, it would not come close to being satisfied.

Satisfaction of "in accordance with the law" test in interception cases

55. There is a significant body of Strasbourg jurisprudence on what constitutes interference "*in accordance with the law*" in the context of interception of communications. These will be termed below the "*Strasbourg interception criteria*."

56. As the ECtHR has repeatedly made clear, the phrase "*in accordance with the law*" does not merely require there to be a basis in domestic law for an interference with Art 8 rights "*but also relates to the quality of the law, requiring it to be compatible with the rule of law*" (*Malone* at [67]). In the context of interception of communications by Respondent states, which by its nature happens in secret and where its occurrence may not be revealed to those subjected to it, the "*quality of the law*" must meet certain requirements. Interception must occur pursuant to a legal regime that is sufficiently accessible and "*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 this secret and potentially dangerous interference with the right to respect for private life and correspondence*" (ibid). It must be clear "*what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive*" and the law must indicate "*with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities*" (*Malone* [79]). The requirement that

conduct be "*in accordance with the law*" also applies to the treatment of material after it has been obtained and covers the "*procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material*" (*Liberty v UK* at [69]).

57. In *Weber* the ECtHR summarised its jurisprudence on the requirement that interception, examination and storage of communications occur in circumstances that are sufficiently foreseeable to be regarded as "*in accordance with the law*":

> "93 As to the ... requirement, [of] the law's foreseeability, the Court reiterates that foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly... However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident ... It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated... The domestic 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...
>
> 94 Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must 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 adequate protection against arbitrary interference."

58. The Court continued in Weber by setting out the minimum requirements of a legal regime governing interception with communication for it to be regarded as compatible with Art 8:

> "95 In its case law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed."

59. If, pursuant to a properly issued RIPA 8(1)/(2) warrant, the Intelligence Services lawfully intercept an email, text or Skype call sent by A who is located in London to B who is also located in London, there are a number of safeguards. The RIPA regime requires that in order to issue a warrant the Secretary of State will need to be satisfied that the interception is necessary in the interests of national security or one of the other condition listed in s 5(3). The warrant will need to identify a person or premises (RIPA s 8(1)) and how the communications that are to be intercepted can be identified (s 8(2)). The warrant can only last for a limited time (RIPA s 9). The Code of Practice sets out rules governing interception where the material is subject to legal privilege (paras 3.3-3.8) as well as confidential personal and journalistic material (paras 3.9-3.11). Safeguards for the handling, storage, dissemination and destruction of the material are set out in RIPA s 15 and the Code of Practice Chapter 6. If the email has already been sent and UK authorities wish to obtain it from a provider of telecommunications services, RIPA Part I Chapter II will apply. It governs a request made by UK authorities to obtain the individual's emails and other information once they have been stored by the providers of telecommunication services. If the communication is, incidentally, obtained pursuant to a RIPA s 8(4) "*external warrant*" it will be subject to the "*extra safeguards*" set out in RIPA s 16. Whether those protections suffice, and whether the distinctions between external/internal communications is meaningful, given the nature of modern communication, is set out further below. There will, however, at least be provisions that impose some limits on the searches that can be conducted under s 16(2), and the authorisations that must be obtained if other forms of search are to be undertaken under s 16(3) as well as other safeguards.

60. The same email, text or Skype call may, as many will, pass through the US during its transmission or be subsequently stored on the server of a telecommunications company located in the US. Suppose the email, text or skype call is intercepted as part of a bulk collection by the NSA, and the NSA then allows the Intelligence Services to access and search its database and retrieve the contents and/or metadata of the communication. Neither RIPA nor the Code of Practice apply. If the requirements set out in the Strasbourg interception criteria must be met in relation to the Intelligence Services obtaining the communication, it is clear that they do not come close to being

satisfied. There is no published and sufficient clear domestic legal provision which will indicate to A and B "*the circumstances in which and the conditions on which*" the Intelligence Services are entitled to obtain the communication or communication data that passed between them; they do not know, with sufficient specificity, what category of people are liable to have their communications obtained in this way, the procedures to be followed for examining, using or storing the data or the circumstances in which it will be erased.

61. The Respondents in their Open Response at [81] mischaracterise the Claimants' argument on this point as being that there is "*no relevant legal regime*" that regulates the obtaining of intercept material from US authorities. That has never been the Claimants' position. The Claimants' position in their Grounds was that "*there is no domestic legal regime meeting the requirements of Art 8/10*" (Privacy International Grounds [43]). That remains their position for the reason set out above. The Art 8 "*in accordanace with the law*" requirements are not satisfied by the statutory regimes which provide, for these purposes, no more than that the Intelligence Services can obtain information necessary for discharging their functions of protecting national security (see Security Services Act 1989 s 1(2) and 2(2)(a) and the Intelligence Services Act 1994 1(2) and 2(2)(a)). Nor will they be satisfied by the requirement that the communications will only be kept for as long as considered necessary for the purpose of protecting national security (Data Protection Act 1998). Permitting the Intelligence Services to obtain, retain and process the communications and communications data of anyone in the UK, provided only that they consider it necessary for national security, does not provide adequate protection against arbitrary interference.

62. The absence of legal regime meeting the criteria set out in the Strasbourg intercept cases is also apparent from the consideration of the issue by the Interception of Communications Commissioner, Sir Anthony May, in his 2013 annual report published on 8 April 2014. Sir Anthony May considered the receipt of "*intercept material about British citizens*" by British agencies from their US counterparts [6.8.1]-[6.8.6] [Farr Exhibit Tab 14 p 914]. This issue, as Sir Anthony May noted at [6.8.6], is outside his remit pursuant to RIPA s 57. He nevertheless considered it briefly as it sparked controversy following the Snowden leaks.

63. The only statute that Sir Anthony May referred to as directly applicable was the Intelligence Services Act 1994. It does no more than permit the Secret Intelligence Service to "*obtain … information relating to the actions or intentions of persons outside the British Isles*" (s 1(2) (emphases added)). That is unlikely to apply to the communications of A and B if they are both located in London, and in any event, as set out above, such a general and broad power does not come close to satisfying the Strasbourg interception criteria. Sir Anthony May also considered a further test by which he considered the legality of obtaining intercept material from the US could be measured, namely whether a RIPA-by-analogy test was satisfied. He concluded:

> "information lawfully obtained by interception abroad is not necessarily available by interception to an interception agency here. In many cases it will not be available. If it is to be lawfully provided from abroad, it is sometimes appropriate for the interception agencies to apply explicitly by analogy the RIPA 2000 Part I principles of necessity and proportionality to its receipt here even though RIPA 2000 Part I does not strictly apply, because the interception did not take place in the UK by an UK agency. This is responsibly done in a number of appropriate circumstances by various of the agencies, and I am asked to review the consequent arrangements, although this may not be within my statutory remit".

64. It is evident from Sir Anthony May's observations that the closest he could find to a regime regulating the accessing of information obtained by a foreign intelligence service was an internal and unpublished practice, "*responsibly followed*" by the Intelligence Services, to apply, at least "*in a number of appropriate circumstances*", and "*by analogy*", "*the RIPA 2000 Part 1 principles of necessity and proportionality*". That again plainly does not satisfy the Strasbourg interception criteria. It is no better than the position before *Malone* and *Hewitt & Harman* when the only protections against arbitrary interception were internal policies and procedures. If all that is done is that, at least in some circumstances, the Intelligence Services ask themselves whether they regard the accessing of information as "*necessary and proportionate*", sufficient and accessible safeguards against arbitrary use do not exist. Pursuant to the HRA 1998 any interference with Art 8 rights by a public authority must be "*necessary and proportionate*". That does not, in itself, provide a "*sufficiently clear*" indication to members of the public as to "*the circumstances in which and the conditions on which*" their Art 8 rights may be subject to interference in this context.

65. Sir Anthony May concluded that the Intelligence Services were not receiving from US agencies intercept material that could not lawfully be acquired by intercept within the UK and thereby circumventing domestic regimes. It is not clear, however, and with respect to Sir Anthony May, what is meant by that conclusion. It could mean that in no circumstances would the Intelligence Services obtain a communication between two people located in the UK that had been intercepted by the US unless there was already in place a warrant which satisfied RIPA s 8(1) and (2). If that is a prohibition which the Intelligence Service is required to adhere to it should be published and the parameters of what may and may not be done clearly set out. If that is not what is meant, it is not clear what policy is being adopted to avoid "*circumventing*" RIPA.

66. That is also the answer, if, as appears to be the case, the Respondents' position is that there is no requirement for further legal provision to govern the accessing by the UK Intelligence Services of material intercepted or obtained by another intelligence service. Further provision is not needed, the Respondents' argue, because, pursuant to *Padfield* [1968] AC 997, it would be unlawful to "*deliberately circumvent*" the safeguards in RIPA by asking a foreign intelligence agency to intercept and disclose "*specified communications*" (Respondents' Open Response [58]). No doubt the language used is carefully chosen. It is assumed that the concession apples only to "*deliberate*" circumvention and to the express prior request to obtain "*specified*" communications. As soon as one asks what that means in practice, and what is the scope of the self-imposed prohibition, it is clear that it does not satisfy Art 8. Suppose the US intercepts communications and communications data of residents of the UK, including much of which would be regarded pursuant to RIPA as being "*internal*". Does that mean the Intelligence Services cannot access it at all? Does it mean the Intelligence Services cannot access it unless there was already in place a RIPA s 8(1) or 8(2) warrant which would have permitted the Intelligence Services to intercept it themselves? If not, what is the Intelligence Services' practice? If those questions are answered at all it is only in unpublished and non-accessible documents and certainly one cannot find clear and intelligible limits to the Intelligence Services' powers by applying *Padfield* or assuming that the Intelligence Services will act "*by analogy*" with RIPA.

Do the Strasbourg Interception criteria apply?

67. The principal submission of the Respondents does not, however, appear to be that the legal regime governing the obtaining of communications material from the US satisfies the Strasbourg interception criteria. The Respondents' principal submission is that those criteria, and the "*strict standards*" they have developed (Respondents Open Response at [88]), apply only where the State was itself directly responsible for the interception (ibid [83]-[92]). Instead, they argue that the standards do not apply to the obtaining of communications from a foreign state.

68. The Respondents submit that no material obtained by UK Intelligence Services should be subject to the Strasbourg minimum safeguards for intercept material. That is the case, the Respondents submit, even if the material is intercepted communications between two UK residents, and which would require a warrant satisfying RIPA s 8(1) and 8(2) if the UK Intelligence Services were to intercept it themselves or would be subject to RIPA s 16 if obtained by a s 8(4) warrant. The Claimants' argument is that that is wrong in principle.

69. The parties have identified no ECtHR or domestic authorities that have considered the issue. It needs to be approached as a matter of principle and the parties arguments can be tested by considering three scenarios:

Scenario 1 The UK Intelligences Services intercept emails, texts and calls between A and B who are both located in London as the communications are leaving the UK on transatlantic fibre optic cables. It is accepted by the Respondents that the Intelligences Services can access, read and analyse them only if there is a RIPA s 8(1) and (2) warrant in place, or, if obtained incidentally pursuant to a s 8(4) warrant, is subject to the provisions of s 16;

Scenario 2 The NSA intercepts the same emails, texts and calls between A and B when the transatlantic fibre optic cables arrive in the US as part of its bulk interception programme. The UK Intelligences Services are permitted to search the database of the NSA's bulk interceptions, and they find, read, analyse and store the communications between A and B.

Scenario 3 A and B travel in the US. The FBI covertly videos them or obtains intelligence about them from covert human sources. On viewing the material the FBI considers that it suggests a threat to the UK and sends it to the UK Intelligences Services which analyses and stores the material.

70. The Claimants' position is that the obtaining by the Intelligence Service of the emails, texts and calls should, for the purposes of the "*in accordance with law*" requirement in Art 8, be treated in the same, or approximately the same, way under scenarios (1) and (2). That does not mean that the legal regime governing both must be identical. It means, however, that the "*quality of the law*", in terms of its foreseeability and the level of protection it provides against arbitrary interference, must be of a similar nature. That is because both scenarios concern the legal provision necessary to protect the same right to privacy, i.e. A and B's right when they communicate with one another in the UK not to have the UK Government access, read, analyse, store those communications. The Respondents' position is that it is scenarios (2) and (3) that should be treated in the same way ("*as a matter of principle, there is no good reason*" to treat them differently (Respondents' Open Response [89])). Indeed they go further and suggest that that no "*workable distinction*" can be drawn between them (Farr [29]).

71. From A and B's perspective it is difficult to see any difference between their communications being obtained by the Intelligence Services in scenario (1) as opposed to scenario (2). In both situations what may be profoundly private communication within the UK is obtained by HM Government, analysed, collated with other information, stored and can be used. It has long been recognised by the ECtHR, and subsequently by Parliament in RIPA, that interception of communication poses a particular danger to democratic society and therefore requires particular safeguards. One of the Respondents' arguments is that there is no difference between interception of communication and other forms of surveillance. That is also Mr Farr's view (see witness statement [29]-[30]). That is not a good argument. The ECtHR, as well as Parliament in RIPA, recognises that intercepted communications raise particular and special privacy concerns. In *Uzun v Germany* (2011) 53 EHRR 24 the ECtHR declined to apply the "*minimum safeguards*" which, it explains, have been "*developed by the Court … to avoid abuses … in the context of applications concerning the interception of*

telecommunications" as those "*rather strict standards*" are not applicable to lesser interferences with private life [65]-[66].

72. It is a fundamental, and often-repeated, principle of the European Convention that it is "*intended to guarantee not rights that are theoretical or illusory but rights that are practical and effective*" (for a recent reaffirmation by the Court of Appeal see *G (A Child) v LSC* [2014] EWCA Civ 656 at [97]). If the "*minimum safeguards*" developed by the ECtHR, and reflected in RIPA, in relation to the interception or obtaining of communications, especially "*internal*" communications, are not to become "*theoretical or illusory*", one cannot treat scenario (1) and (2) in an entirely different way in terms of the "*quality of law*" required. It is no less of an interference with privacy, and no less necessary to have a published legal framework satisfying Art 8, under both scenarios. The impact on privacy is the same if the Intelligence Services themselves intercept A and B's communications on fibre optic cables within the UK, and if the NSA intercept the same communications because (as is likely to be the case) they transit the US and are picked up in the US bulk interception programme, and that because the NSA and GCHQ work so closely together, that bulk interception is then made available to the UK Intelligence Services. That is so, in particular, in circumstances in which the US intelligence services are much better resourced than their UK counterparts (with Mr Farr at [23] estimating that the US's intelligence budget is some 18 times greater than the UK's). Presumably that enables the NSA to intercept and store a far greater proportion of the purely internal communications of UK residents than can the UK's own Intelligence Services (as Mr Farr explains at [23] "*the US can provide the UK with intelligence that the UK - with its far more limited resources – could not realistically obtain by itself*").

73. The NSA and GCHQ appear to be conducting, and certainly have the capacity to conduct, what is, in effect, a joint operation to intercept and share material. That, in principle, enables the UK Intelligence Services to obtain the communications and communications data of UK residents. If, as appears to be the case, both the UK and US have bulk interception programs for communications and communication data passing through fibre optic cables over which they have control, and each gives the other access to the product of these programmes, any meaningful distinction between internal communication intercepted by the UK and that intercepted by the US

disappears as far as minimum legal safeguards are concerned. It is impossible to see why, as a matter of principle, the requirement for published and accessible safeguards against abuse and arbitrary interference should be different if it is the US that intercepts the communications and provides them to the UK Intelligence Services, than if the UK Intelligence Services obtains them directly.

74. The Respondents disagree. Their argument is that it is scenarios (2) and (3) that are in principle indistinguishable and should both be treated as the UK Intelligence Services having "*merely obtained information from a foreign state*" (Respondents' Open Response [87]).

75. The evidence provided by Mr Farr in support of the argument sets out in some detail the importance of what he describes as "*the sharing of intelligence with foreign states*" [15]-[26]. He explains that serious and organized criminal and terrorists frequently plan and carry out activities designed to harm UK interests "*whilst they are outside the UK or in association with others who are outside the UK*" [15] and he refers to the global threat that the UK faces [16]-[19]. He concludes at [20] "*given this background, it is highly unlikely that any government will be able to obtain all the intelligence it needs through its own activities. It is therefore vital for the UK Government to be able to obtain intelligence from foreign governments both to improve its understanding of the threats that the UK faces, and to gain the knowledge needed to counter those threats*."

76. It is notable, however, that nowhere does Mr Farr refer to the concerns raised in the Claimants' Grounds or the kinds of "*intelligence sharing*" that is at issue in this case. The concern is with what anyone would regard as an entirely domestic activity (the sending of an email, text or a phone call between two people in the UK, metadata showing an individual's location within the UK, or an internet search by someone in the UK which may reveal an individual's sexuality, politics or health problems). Given the nature of the internet, is very likely to be accessible to foreign intelligence services and in particular those of the US. If it is collected in bulk and the UK is then given access to it, that is no sense <u>foreign</u> intelligence about activities going on <u>outside the UK</u>. It is private communication that occurs entirely within the UK. Nowhere does the Respondent explain why that material needs to be, or should be, obtained without the same protections Parliament has accorded through RIPA.

77. That does not mean that RIPA can simply be transposed so that it applies in precisely the same way in scenario (1) and (2) or that precisely the same form of warrant will be required in both situations. It is not, however, with respect to the Tribunal, for these proceedings to seek to design a lawful statutory scheme. It requires a significant re-think by Parliament as to how a legal regime can operate which permits communications to be intercepted, analysed and stored where necessary to protect national security, while ensuring adequate protection for privacy. The world has moved on in ways that were unimaginable even 14 years ago when RIPA was enacted. Purely domestic communication, for which RIPA provided particular protection, now routinely travels round the world and can be obtained by the UK Intelligence Services, via a foreign agency, without any form of RIPA warrant. It is the Claimants' position that the legal regime which includes no published criteria (beyond it being necessary to protect national security), no requirement for a warrant and no Code of Practice to determine when the Intelligence Services, by working with their US counterparts, are permitted to access, analyse, store the majority of what are, on any analysis, the entirely domestic internet-based communications or web-searches of anyone in this country, does not satisfy the Art 8 "*in accordance with the law*" requirement.

Issue (ii)

78. Issue (ii) is whether, if the Claimants' communications and communications data are obtained by the US pursuant to its PRISM or UPSTREAM collection program, and then obtained, retained, used or disclosed, that interferers with the Claimants' Art 10 rights as well as their Art 8 rights.

79. The ECtHR held in *Weber* that the threat of secret surveillance "*necessarily strikes at the freedom of communication between users of telecommunications services and therefore amounts in itself to an interference with the exercise of the applicant's rights under Art 8, irrespective of any measures actually taken against her*" [144]. The first applicant in *Weber* was a journalist. She argued that given the danger that her telecommunications might be monitored, there was a risk that her journalistic sources might be disclosed or deterred from contacting her. There was therefore an interference with her Art 10 rights. That was accepted by the ECtHR which held that its findings on Art 8 "*must be applied,*

mutatis mutandis, to the ... applicant's rights, in her capacity as a journalist, to freedom of expression as guaranteed by Art 10(1)" [145].

80. The ECtHR has also recognised that in terms of any interference with the right to receive and disseminate information, non-governmental organisations should be treated in the same way as the press. In *Österreichische Vereinigung zur Erhaltung v Austria* (App 39534/07, Judgment 28 November 2013) the ECtHR held at [34]:

> *the Court has held that the gathering of information is an essential preparatory step in journalism and an inherent, protected part of press freedom …. However, the function of creating forums for public debate is not limited to the press. That function may also be exercised by non-governmental organisations, the activities of which are an essential element of informed public debate. The Court has therefore accepted that non-governmental organisations, like the press, may be characterised as social "watchdogs". In that connection their activities warrant similar Convention protection to that afforded to the press.*

81. That applies to Privacy International and B4A. They seek to improve privacy in developing countries, sometimes in weak or emerging democracies of particular relevance to US and UK foreign policy, and where strong privacy safeguards may conflict with the objectives of intelligence agencies. Groups and individuals in repressive regimes, as well as individuals in the UK concerned about their own privacy, and victims, whistleblowers and journalists frequently contact both Privacy International and Bytes for All. They may be dissuaded from doing so, or from communicating freely, for fear that their communications will be accessed by the UK Intelligence Services. Art 10 is therefore engaged.

Issue (iii)

82. Issue (iii) is whether, if there is an interference with the Claimants' Art 10 rights, the statutory regime as set out in paragraphs 36-76 of the Respondents' Open Response to the Claims brought by Liberty and Privacy International satisfy the Art. 10(2) "*prescribed by law*" requirement. The Art 10(2) "*prescribed by law*" requirement mirrors the Art 8(2) "*in accordance with the law*" requirement, and the Claimants submit, for the reasons set out above, that neither is satisfied.

Issues (iv), (vi-vii) Is TEMPORA 'in accordance with the law'?

Issues (viii-x) Prior judicial approval, specific targeting and absence of suspicion

The test

83. The test is set out in the decision of the ECtHR in *Gillan & Quinton v UK* (2010) 50 EHRR 45:

a. First, the activity must have a basis in domestic law that is sufficiently clear and certain. This means that the law must be "*adequately accessible and foreseeable*".

b. Secondly, the measure must be compatible with the rule of law. The Court will consider the quality of the law. The law must provide "*a measure of legal protection against arbitrary interferences by public authorities*". In particular, discretion cannot be "*granted to the executive… in terms of an unfettered power*". The law must indicate "*the scope of any such discretion… and the manner of its exercise*". Safeguards must "*constitute a real curb on the wide powers afforded to the executive so as to offer the individual adequate protection against arbitrary interference*" [77-79].

IPT 01/77

84. The IPT considered this issue in the context of section 8(4) in *IPT 01/77* (decided in December 2004). The case concerned the section 8(4) bulk interception of telephone calls between the UK and the Republic of Ireland. It was not suggested that every telephone call in the UK (or the Republic of Ireland) was being intercepted. Nor was it alleged that any significant quantity of internal communications were being swept up. The surveillance covered a single microwave radio link over the Irish Sea.

85. The operative passage in the Tribunal's decision is as follows:

> "38. It is in those circumstances that the Respondents submit, by reference to the criteria in s 5(3), as exercised with proportionality and the existence of multiple safeguards, that both the question and the answer are the same as in *Christie*. We agree. It is clear from the *Sunday Times* case that foreseeability is

> only expected to a degree that is reasonable in the circumstances, and the circumstances here are those of national security, as discussed in *Klass* and *Leander*. This is not a *Silver* case where the legislation itself was inadequate and the guidelines were unpublished. In this case the legislation is adequate and the guidelines are clear. Foreseeability does not require that a person who telephones abroad knows that his conversation is going to be intercepted because of the existence of a valid s 8(4) warrant. The "why me" test is as inapt in this case as it would have been found to be by the Court of Appeal in its recent decision in… *Gillan*… at paragraph 50 of the judgment of the Court given by Lord Woolf LCJ, in relation to the subject of a valid stop and search order."

86. The passage in *Gillan* [2004] 3 WLR 1144 cited was as follows:

> "… In such a situation the authorisation and confirmation of a random power of search, provided by Parliament subject to the safeguards we have identified, cannot, as a matter of general principle, be said to be an unacceptable intrusion, that is neither necessary nor proportionate (as those terms are used in an ECHR context) into the human rights of those who are searched in the absence of some identified specific threat. The disadvantage of the intrusion and restraint imposed on even a large number of individuals by being stopped and searched cannot possibly match the advantage that accrues from the possibility of a terrorist attack being foiled or deterred by the use of the power."

Views of Sir Anthony May

87. Recently, the current Interception of Communications Commissioner, Sir Anthony May, has commented on the 'prescribed by law' issue. In his 2013 Annual Report, published on 8 April 2014, he cited *IPT 01/77* with approval, and included a summary of the decision in his report. He said:

> "6.5.45. The general tenor of the Rulings is to endorse the structural integrity in law of the section 8(4) procedure including the principle of a filtering process to reduce and make individual selections from generalised interception material.
>
> 6.5.46 In light of this IPT decision, it is, I think pertinent to ask what has changed since 2000 or 2004 so that a statutory procedure which was re-enacted in 2000, and whose integrity was judged to be intact in 2004, may now have become inadequate and outdated."

88. Sir Anthony May concluded that although the "*internet has expanded in volume and sophistication*" and "*investigatory techniques are no doubt more sophisticated than they were*" nothing had changed (para. 6.5.47).

Is Sir Anthony May right?

89. Sir Anthony May's views deserve careful consideration. However, they are wrong in law. It would also perhaps have been preferable if he had consulted outside the security and intelligence services before offering his conclusions:[5]

    a. The decision of the IPT was based on the decision of the Commission in *Christie v UK* and the decision of the Court of Appeal in *Gillan*. But both cases have since been held by the Strasbourg Court to have been wrongly decided:

        i. *Christie* was expressly overruled by the Strasbourg Court in *Liberty v UK* at [63] ("*The Court's approach to the foreseeability requirement in this field* [of general surveillance programmes] *has, therefore, evolved since the Commission considered the United Kingdom's surveillance scheme in… Christie*"). The correct legal test is different from that applied in *IPT 01/77.*

        ii. *Gillan* was reversed in *Gillan v UK*. The Strasbourg Court held that the without suspicion stop and search power used on Mr Gillan was not compliant with Article 8 because the power was so arbitrary as to not be in accordance with the rule of law.

[5] The approach adopted by the Independent Reviewer of Terrorism Legislation is the better one. As the Independent Reviewer notes on his website "*… access to the secret state, though vital, is not enough. I need to be familiar also with the work of scholars, NGOs, lawyers, judges, journalists, politicians and campaigners, to have some idea of how difficult issues are dealt with in other countries, and to hear from people who have been exposed to anti-terrorism powers that to them may seem intrusive or oppressive*." This is done to minimise the risk identified by Megarry J in *Cordell v Second Clanfield Properties* [1969] 2 Ch 9 of reliance on extra-judicial pronouncements by judges ("*The author, no doubt, has the benefit of a broad and comprehensive survey of this chosen subject as a whole, together with a lengthy period of gestation, and intermittent opportunities for reconsideration. But he is exposed to the peril of yielding to preconceptions, and he lacks the advantage of that impact and sharpening of focus which the detailed facts of a particular case bring to the judge. Above all, he has to form his ideas without the aid of the purifying ordeal of skilled argument on the specific facts of a contested case. Argued law is tough law… Today, as of old, by good disputing shall the law be well known*".

b. IPT 01/77 therefore requires reconsideration, applying the law as it now is.

90. This point is made good by the Government's response to *Liberty v UK*:

a. After the decision in *Liberty v UK*, the Respondents took advice from the First Treasury Counsel on what, if any, amendments were needed to the law to ensure that section 8(4) warrants were lawful. On advice, it was said that "*whilst the Home Office believes that the issues raised in the Liberty case have, to a large extent, already been addressed by the implementation of RIPA and the Code, it has decided to make some changes*" (Report of the Interception of Communications Commissioner for 2009, para. 2.12):

> "Following receipt of legal advice it intends making a small number of amendments to the Code chapter 5 (covering RIPA section 8(4) interception warrants) and chapter 6 (safeguards). These deal with how, post-interception, material gathered under warrant comes to be examined, including giving a better indication of the filtering of extraneous material via automated systems. The proposed revised draft Code of Practice was issued by the Home Office for consultation on 12 March 2010".

b. However, the proposed revised code was never introduced, and the proposed changes were never made "*because of timing constraints and the expectation that new legislation would be enacted relating to communications data*" (Farr [162]). The Government therefore:

i. recognised that the analysis in *IPT 01/77* as to the compatibility of Section 8(4) warrants no longer satisfied Article 8 ECHR in light of the decision in *Liberty v UK;*

ii. accepted that changes were needed to the Code to make the legal regime compatible with the rule of law;

iii. consulted on a draft revised Code; but

iv. ultimately did nothing, apparently because it was hoped that Parliament would approve a new scheme, which because of the

privacy concerns it posed, Parliament did not. See Mr Hosain's witness statement.

91. The changes proposed to the Code were substantial. In summary:

    a. Adding a duty to carry out an "*internal review involving scrutiny by more than one official*" before applying for a section 8(4) warrant (para. 5.2).

    b. A requirement to use "*automated systems where technically possible… to process and filter the volumes of material that are gathered under section 8(4) warrants*" whilst permitting access to a limited number of authorised staff to check whether bulk data falls within the certificated categories or to ensure the efficacy of the system (para. 6.5).

    c. A duty to create a record before reading, looking at or listening to material setting out why access is necessary and proportionate. The system must require reference to specific selection factors, prevent access unless the record has been created and limit access to a defined period of time (para. 6.6).

    d. Periodic audits (para. 6.7).

92. Having decided that changes to the operative rules (set out in the Code) were necessary in order to comply with *Liberty v UK*, but not having made the changes, it is difficult to see how the section 8(4) scheme is prescribed by law.

93. In any event, the changes in the draft revised Code of Practice do not come close to complying with the modern Strasbourg case law:

    a. The Strasbourg court has provided guidance on the 'prescribed by law' standard in *Liberty v UK*, *Weber & Saravia v Germany*, *S v UK* and *MK v France*. Three important principles from those decisions are:

i. universal collection and analysis of everyone's data is far more likely to be an arbitrary interference with the rule of law than targeted collection by area, or person;

ii. the use of powerful automated storage, search and retrieval systems makes interception, collection and retention of data more not less intrusive; and

iii. a potentially valuable power in combating serious crime or terrorism (such as a general warrant, or a DNA or fingerprint database, or a section 8(4) warrant) may be arbitrary and incompatible with the rule of law.

b. A scheme such as TEMPORA has inadequate safeguards as to be prescribed by law:

i. The distinction between 'internal' and 'external' communications is ambiguous, based on hitherto secret guidance about 'platform services', and has no practical meaning in the context of a section 8(4) warrant covering large numbers of fibre-optic cables. This is dealt with below under issue (v).

ii. There is no prior judicial oversight of a section 8(4) warrant. Given the extraordinary potential scope of such a warrant, this is necessary to ensure that the surveillance involved is compatible with the rule of law. For example, if an analyst makes a decision to target a particular foreign person for intrusive surveillance, providing that the searches are within the scope of a certificate (which may simply say 'terrorism'), his communications can be collected without any need to obtain approval from the Secretary of State, still less any judicial oversight.

iii. There is no requirement for individual targeting. A search covers *everyone's* communications, whether or not there is any basis to

suspect each individual of any wrongdoing. When entire fibre optic cables are being intercepted, surveillance is not restricted to a particular country or area or group, but to the communications of the population of the British islands and the world as a whole. Furthermore, searches in practice will cover both British residents and those abroad (see issue (v) below).

iv. The scheme is discriminatory. See issue (xii) below.

94. These points can be tested by reference to the German "strategic monitoring" scheme in *Weber & Saravia* (which was held to be lawful) and the Data Retention Directive in *Digital Rights Ireland* (which was not):

a. In *Weber & Saravia* there were far stronger procedural safeguards, and the degree and scope of interference was far less:

i. The independent G10 Commission (including a legally qualified President) had to consent in advance to proposed monitoring monthly. There was therefore independent detailed and continuous scrutiny of the precise surveillance measures used. The Commission had the power to order that individuals subject to monitoring be notified [25]. In contrast, RIPA prohibits a person from knowing he or she has been subject to a section 8(4) warrant.

ii. The exact purposes for which interception was permitted were specified in the G10 Act and thus public [27]. In contrast, the content of certificates under section 8(4) are always secret, even if they are generally worded and disclosure of their content would itself not pose a real risk to national security.[6]

[6] On 3 June 2014, *The Register* reported that "Miliband's first 2009 warrant for TEMPORA authorised GCHQ to collect information about the "political intentions of foreign powers", terrorism, proliferation, mercenaries and private military companies, and serious financial fraud".

iii. The categories under the G10 Act were very tightly defined (an armed attack on Germany, the commission of a terrorist attack in Germany, international arms trafficking, illegal importation of drugs into Germany, counterfeiting (but only when committed abroad) or money laundering (but only when it threatened the monetary stability of Germany). It is notable that the German Federal Courts themselves restricted the legislation [29]. In contrast, a section 8(4) certificate can cover any purpose within the far wider rubric of national security, serious crime or economic protection.

iv. Only wireless communications can be intercepted, which comprised only 10% of communications (although fixed line communications could be intercepted for the sole purpose of preventing a potential armed attack on Germany). In practice, interception could only cover some satellite communications because interception only took place in Germany and modern satellites focused their "downlink" on very narrow areas [31]. The scheme was therefore one of truly strategic monitoring, to protect the existence of the nation, rather than the "*collect it all*" approach of TEMPORA.

v. Searches were conducted using catchwords. Each catchword had to be suitable for investigating the dangers in the monitoring order and catchwords had to be listed in the order and thus subject to oversight and supervision [32]. In contrast, there is no equivalent requirement for Secretary of State (still less judicial) approval of search terms used under RIPA.

vi. There were stringent requirements on how information could be used. It could only be employed for the purpose of preventing, investigating and prosecuting specified, extremely serious, criminal offences [33-44]. Transmission or further use had to be approved by a staff member with the qualifications to hold judicial office. In contrast, section 8(4) information may be used for any of the much more broadly defined functions of the Security and Intelligence Services, as

well as being transferred abroad. There is no requirement for legal oversight.

vii. All data had to be reviewed to decide whether it should be destroyed every six months. Destruction had to be supervised by a person with the qualifications to hold judicial office [45-50].

viii. Persons subject to monitoring had to be notified as soon as possible. The German Courts struck down the exception to the notification duty if the data were destroyed within three months of collection [50-54]. In contrast, under RIPA a person is never told that they have been subject to a section 8(4) warrant, even once the monitoring has come to an end, so in practice challenge is difficult if not impossible.

ix. The Strasbourg Court gave particular emphasis to the public statement of the exact offences for which strategic monitoring was permitted [96], the substantial limits imposed by only intercepting wireless communications, the stringent requirements imposed by the legislation (and the German courts) on the use of information, and the publicly disclosed destruction procedure and the prior authorisation requirement by an independent Commission [115]. None of these safeguards exist in RIPA.

b. In *Digital Rights Ireland*, the scheme was unlawful because everyone's data were being collected in bulk and could be subjected to revealing automated analysis. There were no exceptions for geographical area, or persons not likely to be involved in serious crime. Nor was there any prior review by a judicial officer, or safeguards to ensure data are retained within the EU. The similarities to TEMPORA are striking, save that TEMPORA is far more intrusive because content as well as metadata is collected and subjected to automated analysis.

95. Finally, the UK oversight regime is not a sufficient safeguard:

a. Neither the ISC nor the Commissioner appear to have been aware of or investigated the true scale and scope of mass interception operations by GCHQ until revealed by a whistleblower.

b. For example, the Commissioner is only now conducting a "*further detailed investigation into the actual application of individual selection criteria from stored selected material initially derived from section 8(4) interception*" (2013 Report, para. 6.6.8). To date, the Commissioner had had this "*fully explained and then demonstrated to* [him]" but had not seen any detailed material and could not form any judgment. Whilst this inquiry is welcome, it is long after the event and could and should have taken place many years ago when mass interception programmes were developed.

c. There is no requirement for prior approval of section 8(4) warrants (cf. the G10 Commission), and no detailed examination of keywords or search terms (cf. the G10 Commission) and full investigation has only taken place *after* disclosure to the public.

d. GCHQ's private view of the light touch nature of the UK oversight regime is fair and accurate. This is not a criticism of individual Commissioners, or of their integrity, but a structural problem about what can realistically be done by a single Commissioner with no technical expertise and few staff who cannot discuss their work with anyone other than staff of the Security and Intelligence Services.

Issue (v) External communications

96. RIPA draws a fundamental distinction between internal and external communications. In contrast to Section 8(1) warrants, Section 8(4) warrants do not require the warrant to specify a particular person or set of premises to be targeted. Instead, an entire communications link can be targeted. Blanket interception and searching is permissible for material within the scope of a (secret) certificate issued by the Secretary of State. But a section 8(4) warrant must be primarily targeted at external not internal communications.

97. There are two problems with this distinction:

a. First, the distinction is ambiguous and uncertain in its scope and effect. The law is not sufficiently clear to comply with Article 8 ECHR.

b. Secondly, as a result of technological change, the distinction between internal and external communications is quickly becoming meaningless. This is because internal communications sent over a link containing external communications can still be swept up and analysed. Internal and external communications look the same, and cannot easily be differentiated. Such collection of internal communications is no longer truly minor or incidental, but is a fundamental feature of the modern internet. The distinction between internal and external is therefore no longer fit as an effective means of giving any protection against what is in effect a general warrant. It leads to arbitrary and unjustifiable results and is not therefore prescribed by law.

98. As the Code of Practice explains, external communications "*do not include communications both sent and received in the British islands, even if they pass outside the British Islands en route*". So a phone call from Jersey to London, routed via a telephone cable in France is an internal communication. Similarly, an email sent and received in London is an internal communication, even if routed via a server in California. As much is common ground (Farr [130]).

99. But it has now become clear that GCHQ applies a gloss if a communication involves a "*web-based platform*". Mr Farr says that where a message is placed on a "*platform*" which provides access to a number of people "*with access to the relevant Twitter account or Facebook page*", GCHQ treat the communication as being "*not* [between] *any particular person who eventually reads the post or tweet, whose exact identity the person posting or tweeting cannot possibly know at the time the message is sent*" but with "*the platform itself, because the platform is both the repository for the message, and the means by which it is broadcast…*" (Farr [136]). Mr Farr explains that this means that a person posting on Facebook makes an external communication, because he or she is posting to a "platform" rather than sending an email.

100. This concept of a "platform" appears nowhere in RIPA, or the Code of Practice, and until Mr Farr's statement was served, had never been publicly mentioned.

101. As Dr Brown notes and Mr King explains, this analysis makes little sense, and leads to results that are at best unclear and at worst arbitrary. Mr King gives several worked examples, but here is another. Assume ten London students are arranging a night out:

    a. In 1990, they would have all phoned each other and left messages on answerphones to arrange a time. It is very unlikely that these communications ever left the British Islands (or even the M25). But even if they did, they are undoubtedly internal communications.

    b. In 2000, they would have made the arrangement by mobile phone text message or an email to which they were all copied. These are undoubtedly internal communications, even if the route taken in transmission left the British Islands.

    c. In 2014, the friends will probably not email at all. They will send a group message using Google Plus, or post a message to their Facebook wall. The friends will each be able to log in to Google or Facebook and see the message. The effect is the same – a communication has been made within a group. The message will be visible only to the selected group of friends. Or even if it is theoretically discoverable by the public, it is extremely unlikely that anyone else would see or read it. Further, as Mr King explains, by default posts on Facebook are not shared with the world, but only with people expressly accepted as 'friends'.

102. Despite this, Mr Farr says that making a post on Facebook involves using a "platform" which makes the communication external. This is a distinction without a difference, made without public knowledge, and removes the protections given to internal communications when using modern communication tools. It is also so arbitrary and unclear that it is very difficult to tell whether a communication is internal or not. This

type of uncertain gloss on statutory provisions, applied without public knowledge, is not compatible with the prescribed by law requirement.

103. Further, the distinction between internal and external no longer offers internal communications any meaningful protection. This is because a substantial proportion of 'internal' communications is now in fact routed outside the British Islands on fibre optic cables. Mr King gives examples such as the switch from mobile text messages (formerly transmitted without leaving the British Islands) to instant messaging via the internet, where a server will be used outside of the UK and the information will transit by fibre optic cable.

104. The world has dramatically changed from the position considered in *Liberty v UK* which concerned the collection of simple telephone calls between the UK and the Republic of Ireland. There, it was unlikely that many internal communications would be incidentally collected. Telephone calls between two Londoners would be unlikely to be routed via a microwave telephone link to Dublin. But Skype calls between two Londoners may well be routed via California and will therefore be collected by TEMPORA. Mr Farr accepts as much ([153]).

105. When fibre optic cables are tapped under section 8(4), <u>all</u> communications on them will be intercepted, even if they are, on analysis, "internal" communications within the meaning of RIPA. It is not practically possible to tell internal and external communications apart: they all look the same. Further, all such communications may be subjected to automated filtering and scanning for items of interest, even where "internal" (see Farr [139]-[141]). Such information can then be read, looked at or listened to so long as it has been selected using search terms not referable to an individual known to be in the UK. And if a person of interest in the UK is discovered, the Secretary of State can issue a certificate under section 16(3) of RIPA permitting further searches of the bulk collected material to identify all of a particular individual's communications.

106. Therefore, once (a) there is bulk interception of fibre optic cables; and (b) most communications travel on fibre optic cables; and (c) most communications leave the British Islands at some point, the important protection given to internal

communications ceases in practice to apply. The safeguards for internal communications are in the modern world illusory. They have been substantially superseded by technology. As a result the internal/external distinction no longer offers any meaningful protection against a general warrant not based on actual suspicion against an identified person or premises. This is incompatible with the quality of law requirement.

Issue (xii) Discrimination

107. Electronic surveillance is subject to substantial restrictions under EU law. These restrictions are in place to ensure that individuals and companies in other EU countries are not less favourably treated as a result of UK surveillance practices.

108. Article 5(1) of Directive 2002/58/EC requires EU Member States to "*prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data… except when legally authorised to do so in accordance with Article 15(1)".*

109. Article 15 provides that Member States may adopt legislative measures to permit interception and surveillance where such restriction "*constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security… defence, public security, and the prevention, investigation, detection and prosecution of criminal offences… All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union*."

110. Article 6 of the TEU provides for recognition of the Charter of Fundamental Rights of the EU and that "*fundamental rights, as guaranteed by the European Convention… shall constitute general principles of the Union's law*". These rights include a prohibition on discrimination.

111. RIPA is indirectly discriminatory on grounds of nationality and national origin because of the distinction between internal and external communications, and the special protections granted to people in the UK under section 16 RIPA. A British person is more likely to be present in the British Islands and *vice versa*. A section 8(4)

warrant is therefore likely to have a disparate adverse impact on non-British nationals. See *Orphanos v QMC* [1985] 1 AC 761. It does not matter that some British people will not benefit from section 16 (because they are not in the British Islands) and some non-Britons will (because they are in the British Islands). See Case C-542/09 *Commission v Netherlands* at [38].

112. The discrimination must therefore be justified. No proper justification has been advanced. The basic point is that in *A v SSHD (No. 1)* [2005] 2 AC 68 (the Belmarsh case) that there is no good reason to treat foreigners differently when terrorism and serious crime is a risk both inside the UK and elsewhere. Both nationals and non-nationals may pose threats to UK national security or may commit serious crimes. Some people would no doubt think that bulk section 8(4) surveillance over all internal communications in the UK would help to detect serious criminals. But it is not permitted here because of the justified constitutional objection to general warrants.

113. RIPA is objectionable for the same reasons as the Revenue Act 1767 was: it targets foreigners, reserving protections for those in the UK. The discriminatory effect will fall overwhelmingly on foreign nationals, who are more likely to be engaging in external communications.

114. Mr Farr's answer is that it is harder to investigate terrorism and crime abroad. No doubt that is true to an extent, in some countries. But that cannot provide any answer for the less favourable treatment of countries where the UK has criminal and intelligence sharing relationships pursuant to the EU common foreign and security policy or other arrangements.

Issue (xiii) 'NCND'

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

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

b. However, the NCND principle is no more than a policy. It is not a rule of law. It has a number of relevant exceptions, and is only to be applied by the Tribunal in an appropriate case. The judicial function of the Tribunal requires it to hold a fair hearing, which includes the rejection of an unjustified attempt to rely on the NCND principle. As the Court of Appeal recently put it in *Mohamed Ahmed Mohamed & CF v SSHD* [2014] EWCA Civ 559:

> "Lurking just below the surface of a case such as this is the governmental policy of "neither confirm nor deny" (NCND), to which reference is made. I do not doubt that there are circumstances in which the courts should respect it. However, it is not a legal principle. Indeed, it is a departure from procedural norms relating to pleading and disclosure. It requires justification similar to the position in relation to public interest immunity (of which it is a form of subset). It is not simply a matter of a governmental party to litigation hoisting the NCND flag and the court automatically saluting it."

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

> "33. There are some well-established circumstances in which the [Security] Service does acknowledge that information has been collected and is still held. Sometimes, the information may be released. These circumstances, as Mr Burnett QC [for the SSHD] put it in his oral submissions to us, can be grouped together as cases where the person concerned already knows "conclusively" that there is information held upon him. Another situation which can arise is where the Service itself decides that the acknowledgement should be made, and even that the information should be published, because that is seen as assisting the proper performance of its statutory functions, or as otherwise being in the public interest. This too becomes a case of "official confirmation" that the information is held. These and similar cases, Mr Burnett QC submits, are "well recognised exceptions" to the policy of answering requests with some variant of the formula NCND. They are "dictated by common sense".

34. This group of cases (which is not closed) includes –

(a) Members or former members of agencies who know that data are held.

(b) Individuals who are subject to removal from the United Kingdom on grounds of national security who have become conclusively aware of Security Service interest in them.

(c) Those involved in criminal proceedings who have conclusively become aware of Security Service interest in them.

(d) Others in whom Security Service interest has been publicly confirmed in [Court or other] proceedings."

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

> "Mr Kovats was properly handicapped in dealing with the issue because of the longstanding NCND policy of the British Government. The reason for the policy is explained in the witness statement of Mr Martin Sterling, a senior policy adviser in the Cabinet Office: it would be prejudicial to the effective administration of public affairs to do so. Confirming the accuracy of information within a leaked document would compound any prejudice already caused and would reward persons involved in the leaking. Even a denial of accuracy would, by inference, lead to an unwarranted assumption that an undenied leak was accurate. Hence, subject to exceptional circumstances, the policy must apply universally to be effective."

e. The Court rejected the NCND argument at [28]:

> "We make clear that if the only objection to the admission in evidence of the document were the NCND policy, we would have permitted it to be admitted, for the following reasons, which lay behind our initial ruling on the point. First, it is far from clear that the documents of other governments are covered by the policy. All that Mr Sterling states is that he "cannot see any reason for the NCND principle not

applying in these circumstances". Secondly, as Mr Sterling accepts, the policy admits of exceptions. Thirdly, it does not, as such, bind the court. Fourthly, in the circumstances with which we have to deal, the interests of justice would override the policy: the document has been in the public domain for many months, even if it got there as a result of an unlawful act. If it were necessary for us to take it into account evidentially to determine the true purpose of declaring the [Marine Protected Area], we would not regard the NCND policy as a sufficient reason for refusing to do so. To refuse to do so could, in principle, permit Her Majesty's Government (HM Government) to conceal an improper and unlawful motive for an executive act which is claimed to have had an adverse impact upon the rights of a significant number of individuals of Chagossian origin or descent."

The Court of Appeal agreed [2014] EWCA Civ 708 at [73].

f. There are therefore many circumstances in which NCND policy is not justified or appropriate. The materials obtained by Edward Snowden and now published worldwide by various media outlets are a paradigm example of an absurd claim to NCND:

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

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

iii. Similarly, the Secretary to the D-Notice Committee (Air Vice Marshal Vallance) reported to the 7 November 2013 meeting "*the dominant aspect of this reporting period was the publication by The Guardian, and latterly by The Independent, of information from the classified documents*

stolen by the NSA fugitive Edward Snowden". The Secretary referred to the "*highly sensitive information about GCHQ*" that had been published, and *The Guardian's* agreement "*not to publish certain highly sensitive details*". During this period, the Intelligence Services had "*continued to ask for more advisories to be sent out*" but the Secretary was skeptical about this. The Secretary then referred again to "*the publication … of selected parts of the highly sensitive intelligence information stolen by Edward Snowden*". There is no suggestion in these public minutes that it was sensible or necessary to maintain a 'NCND' response. Indeed, the minutes are entirely inconsistent with 'NCND' because they do not even attempt to maintain the pretense that the documents are anything other than accurate and genuine. To the contrary, the concern was understandably to prevent the publication of certain highly sensitive operational details.

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

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

v. Reliance on NCND in these circumstances is a misuse of the NCND policy and is not lawful. It does not protect national security because there comes a point where any harm to national security has already been done by the original disclosure. At the very least, as the Court of Appeal made clear in *Mohamed & CF*, it is not sufficient for the Respondents simply to assert NCND and make general statements about its appropriateness. It is necessary for the Respondents to justify non-disclosure in the particular context of this case.

Issue (xiv) Disclosure

116. Rule 6(5) prohibits the Tribunal from ordering disclosure. In the *Procedural Ruling* of 23 January 2003, the IPT held that this provision was *intra vires* [176-181]. Accordingly, the IPT decided that *even if it was satisfied that no harm to national security would result*, it had no power to direct disclosure.

117. In *Kennedy v UK*, the Strasbourg Court took a more careful position, noting that "*in the circumstances*" restrictions on disclosure were justified [187]. In that case, revealing whether or not closed material even existed would have confirmed whether or not Mr Kennedy was subject to surveillance.

118. The present case is very different. The Respondents admit that PRISM exists and is used by the UK security and intelligence services, that section 8(4) warrants are used, and the existence of UPSTREAM collection. It is also admitted that there is substantial closed material available. If the Tribunal conclude that there is no risk to national security in disclosure of particular information or materials, why should it not have the power to direct disclosure or take other appropriate steps to ensure a fairer hearing?

119. In this respect, the *Procedural Ruling* should be reconsidered in light of the last decade of experience of experience of closed litigation in the ordinary courts and in SIAC.

120. There, a fairer approach has been found, without creating any additional risk to national security. The Court will consider whether to permit closed material to be withheld with the assistance of a Special Advocate. It will also consider whether to direct a gist be served (CPR 82.14(7))[7]. Disclosure will only be ordered if there would be no harm to national security.

121. But if disclosure is directed, the government does not have to comply. But if it does not comply, the Court may direct "*that the* [government] *is not to rely on such points in [its] case, or that the* [government] *makes such concessions or takes such other steps as the court may direct*" (CPR 82.14(9)). In short, where the Court concludes that the

[7] There are similar provisions in the SIAC procedure rules.

government is making an unfounded claim to secrecy, it will invite, but not insist, on disclosure. But the Court will consider putting the government to its election – give fair disclosure of what the Court has concluded is innocuous material or be debarred from relying on it, or be required to concede the point the material is relevant to. This approach ensures that there is no harmful disclosure, and a fairer trial.

122. The IPT should adopt the same approach. It is not necessary to declare any part of the Rules invalid to do so. If the IPT considers that any withheld material can safely be disclosed, it can invite the Respondent to consent under Rule 6(3). If the Respondent refuses to consent, the Tribunal should exercise its general power to determine its own procedure under section 68(1) of RIPA to make a direction to ensure fairness.

Issue (xv) Special Advocate

123. The Respondents claim that the IPT has no jurisdiction to appoint a Special Advocate. This is a surprising position given that the Respondents are recorded in the *Procedural Ruling* as expressly accepting that the IPT has the power to appoint a Special Advocate [155].

124. In a case such as this, if the Tribunal considers that it is ultimately necessary to have a closed hearing (no good or lawful basis has yet been identified), a Special Advocate will be an essential procedural safeguard. The appointment of Counsel to the Tribunal is not sufficient. There ought to be an advocate advancing the Claimants' position in respect of the material they are not permitted to see, and checking to see if there are additional arguments or grounds that should be advanced based on closed material. In contrast to an *amicus*, the Claimants can select their own Special Advocate (from a panel appointed by the Attorney General), meet with a Special Advocate on a privileged basis before he or she sees any closed material, can give him or her instructions, and continue to send privileged information, advice and instructions throughout the case. Further, the Special Advocate can call witnesses. Given the context, complexity and importance of the instant case and the likely complexity of the technical material the IPT may see in closed it is very difficult to see any good reason why a Special Advocate should not be appointed here (and no reasons are put forward by the Respondents).

DAN SQUIRES

BEN JAFFEY

BHATT MURPHY

12 June 2014