IN THE INVESTIGATORY POWERS TRIBUNAL
BETWEEN:

PRIVACY INTERNATIONAL

Claimant

and

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

Defendants

STATEMENT OF GROUNDS

INTRODUCTION

1. Privacy International was founded in 1990. It is a leading UK charity working on the right to privacy at an international level. It focuses, in particular, on tackling the unlawful use of surveillance. It is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Council of Europe, the European Parliament, the Organisation of Economic Co-operation and Development, and the United Nations.

2. The Secretary of State for the Foreign and Commonwealth Office is the minister responsible for oversight of the Secret Intelligence Service and for the Government Communication Headquarters ("*GCHQ*"). The Secretary of State for the Home Office is the minister responsible for the Security Service.

3. Privacy International is seeking to challenge two matters: first, the soliciting and/or receipt of private information about those located in the UK from US authorities (Ground 1) and secondly, the interception of vast quantities of electronic data on fibre

optic cables leaving the UK and the sharing of that data with US authorities (Ground 2).

4. As to Ground 1, given the current global nature of electronic communications, the emails, phone-calls and internet browsing information of an individual located in the UK will very often pass through the US during their transmission. Much of that information will also be stored, after transmission, on the servers of global internet companies located in the US such as Google, Facebook or Yahoo. That will be so even if the individual, and the party with whom they are communicating, are both located in the UK and have no connection to the US. Recent reports suggest that under the powers contained in the US' Foreign Intelligence Surveillance Act ("FISA") §1881a, US authorities have been intercepting the communications of non-US nationals located outside the US as they pass through fibre cables and electronic infrastructures in the US, and have also been obtaining stored information about such individuals held by US based internet and telecommunication companies. Reports also suggest that such information has been shared with UK authorities.

5. If UK authorities intercept the phone calls, emails, web-browsing and other communications of individuals located in the UK, or require the disclosure of that information when it is stored by telecommunication or internet companies, the authorities must comply with the legal regime set out in Regulation of Investigatory Powers Act 2000 ("*RIPA*"). That does not apply if UK authorities solicit or otherwise receive such information from their US counterparts and that is so even if the communications in question were sent and received in the UK. There is no legal regime which is contains sufficiently clear and detailed rules so as to give individuals in the UK an adequate indication of the circumstances in which, and the conditions on which this may occur and their private information obtained by US authorities will be solicited, received, stored, shared, or used by UK authorities. The contents of an individual's phone calls and emails and the web-sites they visit can be information of an obviously and highly private nature. If UK authorities are to be permitted to access such information in relation to those located in the UK in secret and without their knowledge or consent, the European Convention of Human Rights Articles 8 and 10 requires there to be a legal regime in place which contains sufficient safeguards against abuse of power and arbitrary use. There is no such regime.

6. As to Ground 2, the collection, search and storage of all communications data passing through very large numbers of fibre optic cables on a continuous basis comprises blanket surveillance. Such surveillance cannot be justified as a proportionate response to a legitimate aim. Bulk interception of communications and bulk inspection of such data is a disproportionate interference with the rights guaranteed by Article 8 ECHR, and it is not being undertaken pursuant to a legal regime containing sufficient safeguards to render it "*in accordance with the law*". Further, and in any event, such surveillance has a disproportionate impact on non-UK nationals, who are unjustifiably less favourably treated than UK nationals. Such differences of treatment are unjustifiable breaches of EU law and the ECHR.

GROUND 1

Factual background and relevant legal powers

7. On 6 June 2013 The Guardian and The Washington Post revealed the existence of an extensive external intelligence-gathering programme operated by the US National Security Agency ("*NSA*") and the close involvement of UK authorities in the programme. The scope of the programme is extraordinary, giving the NSA access to the emails, communications, documents, videos and web histories of vast numbers of non-US persons located outside the US including those resident in the UK.

8. The existence of the programme was first revealed in the press after former NSA system administrator, Edward Snowden, leaked a 41-slide presentation regarding the US government's surveillance capabilities. The US Director of National Intelligence James R. Clapper has confirmed the existence of the surveillance programme described in the leaked slides,[1] and it has been stated by the US government that it is authorised under FISA section 1881a.

US powers to obtain information on non-US persons outside the US

9. FISA section 1881a is entitled "*Procedures for targeting certain persons outside the United States other than United States persons*". Section 1881(a) ss (a) provides:

> *the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.*

Section 1881a ss (b) sets out "*limitation*" to the authorisation granted in ss (a). It provides:

> *An acquisition authorized under subsection (a) –*
>
> *(1) may not intentionally target any person known at the time of acquisition to be located in the United States;*
>
> *(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;*

1 http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/869-dni-statement-on-activities-authorized-under-section-702-of-fisa

(3) may not intentionally target a United States person reasonably believed to be located outside the United States;

(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and

(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.

10. An authorisation pursuant to FISA section 1881(a) permits "*foreign intelligence information*" to be obtained both by directly intercepting communications during transmission and by making a request to an electronic service provider that stores the information to make it available to the authorities.

11. The definition of "*foreign intelligence information*" which can be gathered pursuant to FISA s 1881(a) is set out in s 1801. It is very broad. Pursuant to section 1801(e) "*foreign intelligence information*" includes "*information with respect to a foreign power or foreign territory that relates to … the conduct of the foreign affairs of the United States*." The term "*foreign power*" is defined in section 1801(a) to include not only foreign governments or entities directed or controlled by foreign governments, but also pursuant to section 1801(a)(5) "*a foreign-based political organization, not substantially composed of United States persons*." Foreign-intelligence information thus covers information with respect to any foreign-based political organisation or government that relates to the foreign affairs of the US. It would thus, for example, include the contents of private and lawful discussions by those who are members of, or are communicating with, political organizations or governments that in any way relates to US foreign policy. The US has a different regime governing the interception of communications and obtaining private information where the target is a US citizen or is located in the US. Such individuals are accorded a significantly greater level of protection, including through the Fourth Amendment to the Constitution of the United States.

The information gathering programme

12. The leaked slides indicate that there are two aspects of the NSA's information gathering programme - one is entitled "*Prism*" and the other described as "*upstream collection*". Essentially "*Prism*" enables the NSA to obtain information stored by

telecommunication companies or online service providers. "*Upstream collection*" is the direct interception of communications around the world by the NSA during their transmission, in particular as they pass through fibre cables and electronic infrastructures in the US.

13. Prism is described by the NSA as being "*one of the most valuable, unique and productive accesses*" it has to monitor communications.[2] According to the leaked slides, through Prism, the NSA is able to obtain information from the servers of "*Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple*." At this time, the released slides and subsequent reporting have left open the question of how exactly the NSA accesses this information, whether it is obtained directly from the companies' servers or by requiring the companies to hand over the information that they store. What is, however, clear is that, via Prism, the NSA has access to the personal data of a very large number of individuals around the world including those resident in the UK.

14. That is because internet and telecommunication companies store enormous quantities of personal information. For example, Google, through its "*gmail*" service, provides the most widely used web-based email system with an estimated 425 million active users worldwide in June 2012. Google is able to store all of the emails sent to or from a gmail account, and even if users delete the emails they can remain stored on Google's servers. Google's search engine is also the most widely used in the world and it was estimated in 2012 that it processed over 5 billion search requests per day. Google by default collects and stores the data on what searches users conduct, what advertising they respond to, what videos they watch and a myriad of other interactions users have with a Google website.

15. It is not only the content of user activities that internet companies retain. For instance, with regard to a communication, user-records can include, but are not limited to, the location from which a communication originated, the device that sent the communication, the IP address of the sender, the time at which it was sent, the recipient of the communication and his/her device and IP address, the size or length of the communication. Email services such as Gmail will also retain a user's list of contacts, and drafts as well as all messages sent and received. Google Docs/Drive is a

2 http://www.guardian.co.uk/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism

service to store and edit in real time text documents, spreadsheets and presentations, which increasingly is becoming standard in many industries. They too will be stored by internet companies.

16. Much of the information companies, such as Google, Yahoo, Facebook, Microsoft hold will relate to users located outside the US. The companies are among the world's largest providers of internet and communication services, and their users are spread across the globe. According to the leaked slides Prism thus gives access to non-US individuals' "*email, chat- video, voice, videos, photos, stored data, VoIP, file transfers, video conferencing, notification of target activity – logins, online social networking details*." If the NSA can access such information those companies hold about their users, it can obtain the personal data of numerous individuals living outside the US including UK nationals living in the UK. The NSA can obtain their emails, web-browsing history and other private information, irrespective of whether they have ever visited the US or communicated with anyone in the US.

17. The second method of data gathering is described as "*upstream collection*". It is, in essence, the interception of communications during their transmission. This too, according to the leaked slides, is conducted under FISA section 1881a and is described as the "*collection of communications on fiber cables and infrastructure as data flows past*." This description is superimposed over a map of the world that contains brown lines that track the routes of the world's major undersea fibre-optic cables. These cables carry 99% of the world's communications much of which flows through the US. As another slide states: "*much of the world's communications flow through the US*." It continues: "*a target's phone calls, e-mail or chat will take the cheapest path and not the physically most direct path... Your target's communications could easily be flowing into and through the US*".

18. It thus appears that phone calls, emails and other forms of communication are intercepted directly, and the contents recorded, by US agencies if the electronic data passes via cables and servers located in the U.S. Again that permits a vast amount of personal data to be intercepted and stored. As the slide explains, electronic communication does not pass round the globe by the most direct route but the cheapest. Not only is an email sent from the UK to France just as likely to travel

through cables and infrastructure in the US as to take a more physically direct path, but the same is true of emails within a country. An email between two people located in London may well travel through the US. As the leaked slides suggest, the US is the "*world's telecommunications backbone*". The fibre optic infrastructure going into and out of the US has the capacity to facilitate around 90% of the world's electronic communications. Numerous emails, phone calls, internet chat, and other information that is communicated electronically by individuals located in the UK, thus pass through the US and can be intercepted by the NSA.

The UK's access to the US material

19. Shortly after revealing the existence of the US' FISA programme, The Guardian reported that the US is sharing the information it obtains with UK authorities. It has been reported that GCHQ has had access to the Prism system since at least June 2010, and has generated 197 intelligence reports from the system in 2012. It is not known what the contents are of those reports, whether they relate to emails, phone calls or other matters. Nor is there any reason to believe that access by GCHQ is restricted only to Prism-related information, and it is assumed that it extends to all material acquired under section 1881a including material that is directly intercepted from fibre cables.

20. The likelihood that such sharing of information is occurring is supported by recent reports which suggest that, in comparable circumstances, when the UK obtains intercept material, it makes it available to its US counterparts. Recent revelations regarding activities of the UK intelligence agencies confirm that the interception of undersea cables by the UK has become routine. As indicated below in relation to Ground 2, The Guardian reported on 21 June 2013 that GCHQ captures content flowing through undersea cables that land in the UK and is sharing the information with the US. Reports indicate that the material intercepted by GCHQ is examined by a team consisting of 250 NSA analysts and 300 GCHQ analysts suggesting it is essentially a joint project. It is assumed that, similarly, where the NSA intercepts communications of those located outside the USA, the communications can be shared with the UK and analysed jointly by GCHQ/NSA.

21. Through their access to the US programme, including Prism, UK authorities are able to obtain private information about UK citizens, or those otherwise resident in this

country, without having to comply with any of the requirements of the Regulation of Investigatory Powers Act 2000 ("*RIPA*") described below. What is not known, as there appears to be no clear legal regime governing it, is what is done with the information, to whom it is provided and how long it is stored. The mechanisms by which UK government agencies gain access to such information are also opaque. It is not known whether the UK requests information from the US about specific targets or whether it has direct access to the information gathered by the NSA. Even those with responsibility for oversight of UK intelligence agencies are apparently unclear on the point. Sir Malcolm Rifkind MP, current chair of the UK Security and Intelligence Committee, and previously responsible for overseeing GCHQ as foreign secretary between 1995 and 1997, told the Today programme on BBC Radio 4 on 10 June 2013 that "*[o]ne of the big questions that is being asked is if British intelligence agencies want to seek to know the content of emails can they get round the normal law in the UK by simply asking an American agency to provide that information?*"[3]

Privacy International as a potential target for surveillance

22. Privacy International is concerned that its information and communications, as well as those of its partners and supporters, could be obtained by the US under its FISA section 1881a programme and shared with UK authorities, or that such information has already been obtained and shared.

23. FISA section 1881a gives US authorities the capability to access communications provided they are "*targeting... persons reasonably believed to be located outside the United States to acquire foreign intelligence information*." Privacy International, being headquartered in London, is made up of persons located outside of the US. Privacy International also generates a significant amount of "*foreign intelligence information*".

24. As set out above, FISA 1881a defines foreign intelligence information as any information with respect of a "*foreign power*" which relates to US "*foreign affairs*." A "*foreign power*" is not only a foreign government or government-controlled entity, but also any "*foreign-based political organisation*". Privacy International would satisfy that description. It promotes the right to privacy by raising awareness, conducting research, and providing educational materials. It also monitors and reports on surveillance

3 http://www.guardian.co.uk/world/2013/jun/10/gchq-broke-law-nsa-intelliegence

methods and tactics employed against individuals or groups, working at national and international levels toward the provision of strong and effective privacy protections. From time to time Privacy International also undertakes campaigning and other political activities, which involve trying to secure support for, or oppose, a change in the law or in the policy or decisions of governments, and Privacy International supports networks of research organisations and campaign groups across the world with similar goals and objectives. Privacy International also corresponds, in private, with other political organisations and with governments and politicians in the UK and around the world. These bodies and individuals, as well as Privacy International itself, would fall within the definition of a "*foreign power*" pursuant to FISA s 1801.

25. As part of its activities, Privacy International often comments on the foreign affairs of the US not least now that revelations about the US' foreign surveillance programme are emerging. It has also communicated with politicians about privacy issues relevant to US foreign policy. As a result, Privacy International generates private communications and internal organisational discussions which relate to US foreign affairs and would fall within the FISA s 1881a definition of "*foreign intelligence information*". These private communications, transmitted via, or captured on, the many U.S.-based internet services that Privacy International (and many other foreign organizations) routinely use, therefore, make it vulnerable to interception by U.S. intelligence agencies under FISA section 1881a. Members and employees of Privacy International also routinely send emails and make phone calls which could be intercepted as they pass through the US.

Grounds of challenge

The applicable domestic legal regime and summary of claim

26. The First Defendant addressed Parliament on 10 June 2013 following the press revelations about the Prism programme. He refused to confirm or deny the existence of the programme (even though its operation has been confirmed by US authorities) nor to indicate whether information had been provided to the UK. He stated only that UK agencies comply with UK law in dealing with information obtained from overseas. He referred in this regard, in particular, to RIPA.

27. RIPA regulates the interception of communications, the acquisition of communication data and surveillance in the UK. Part I Chapter I covers the interception of communication during its transmission. Such interception requires a warrant issued by the Secretary of State pursuant to RIPA s 5. Section 5 sets out the conditions for the granting of a warrant, including that it is necessary on grounds of national security, or for the purpose of preventing or detecting serious crime or other listed bases (section 5(3)). RIPA Part I Chapter II covers the acquisition and disclosure of "*communication data*", namely data held by a person providing a telecommunication service (section 21(4)).

28. RIPA distinguishes between "*internal*" and "*external*" surveillance. Where the communication is internal (i.e. neither sent nor received outside the British Islands, see RIPA s 20), a warrant to permit lawful interception must describe one person as the "*interception subject*" (s 8(1)(a)) or identify a "*single set of premises*" for which the interception is to take place (s 8(1)(b)). The warrant must set out "*the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications that may be or are to be intercepted*" (s 8(2)). Where the communication is "*external*", that is either sent or received outside the British Islands, RIPA s 8(1) and 8(2) do not apply. There is no need to identify any particular person who is to be subject of the interception or a particular address that will be targeted.

29. However none of these provisions, whether concerning internal or external interception, nor the "*Interception of Communications: Code of Practice*" made pursuant to RIPA s 71 ("the Code of Practice"), will apply if telephone, email or other communications are intercepted by US authorities, or otherwise provided to those authorities, and then passed to UK authorities. That would not require a warrant from the Secretary of State pursuant to RIPA nor otherwise be covered by the Act. That would be the case even if the UK authorities solicited the interception of the material as well as where they were its passive recipients. Similarly, the storage, onward transmission or destruction of such information is not covered by RIPA or the Code of Practice. Nor are there any other publicly accessible, clear and detailed rules (whether in statutes or some other form) that set out the circumstances in which, and the conditions on which, UK public authorities are permitted to solicit the interception of

communications of UK residents by foreign authorities or to receive, store and transmit their contents.

European Convention of Human Rights provisions

30. Article 8 of the Convention provides:

> *1. Right to respect for private and family life. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

Article 10 provides:

> *1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.*
>
> *2 The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.*

Interference with Art 8 and/or 10

31. Telephone conversations and emails fall within the definition of "*private life*" and "*correspondence*" protected by Art 8 (see *Malone v UK* (1985) 7 EHRR 14 [64], *Weber v Germany* (2008) 46 EHRR SE5 at [77] and *Kennedy v UK* (2011) 52 EHRR 4 at [118]). The same is true of an individuals' web history which may reveal highly personal material about their sexuality or political beliefs.

32. In order to establish an interference pursuant to Art 8, it is not necessary for Privacy International to prove that its communications or private information has been accessed, stored or transmitted by UK authorities. It is sufficient that they fall within the group of individuals or organisations who may be subject to such measures.

33. In *Weber* a journalist and one of her contacts in Uruguay sought to challenge the German legislative framework which permitted the monitoring of international telephone calls. The applicants were not able to establish that their calls had been monitored but were nevertheless permitted to challenge the applicable legislative regime. As the European Court of Human Rights ("*the ECHR*") held in *Weber*:

> *78 The Court ... notes that the applicants ... were unable to demonstrate that the impugned measures had actually been applied to them. It reiterates, however, its findings in comparable cases to the effect that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Art.8 , irrespective of any measures actually taken against them...*
>
> *79 Consequently, the impugned provisions ... in so far as they authorise the interception of telecommunications, interfere with the applicants' right to respect for private life and correspondence. Furthermore, the Court ... takes the view that the transmission of data to and their use by other authorities, which enlarges the group of persons with knowledge of the personal data intercepted and can lead to investigations being instituted against the persons concerned, constitutes a further separate interference with the applicants' rights under Art.8... Moreover, the impugned provisions interfere with these rights in so far as they provide for the destruction of the data obtained and for the refusal to notify the persons concerned of surveillance measures taken in that this may serve to conceal monitoring measures interfering with the applicants' rights under Art.8 which have been carried out by the authorities.*

34. If, as in *Weber*, an individual is permitted to challenge the legal regime governing surveillance without proving that they were the victim of surveillance, the same must be true, *a fortiori*, where there is evidence that surveillance may be occurring but where there is no detailed legal regime. In those circumstances, where there is no statutory scheme, Code of Practice or published policy indicating who can be targeted and in what circumstances, it is even more difficult for an individual to know whether they have been subject to surveillance. Providing there is a *prima facie* case that an individual falls within the category of those who may have been targeted, that will suffice to challenge the lack of a governing legal regime.

35. For the reasons set out above, Privacy International and its members, employees and supporters, are those whose information may be obtained under FISA §1881a and provided by the NSA to UK authorities. It may be that UK authorities have already, or will in the future, solicit the interception of their communications by US authorities or otherwise seek private material from the US. It may also be that UK authorities will store or transmit such information. There is thus a potential interference with Privacy International's Art 8 rights and that of its members, employees and supporters. That is sufficient for Privacy International to establish an interference within the meaning of Art 8(1).

36. The ECHR further 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]. It continued: "*this finding 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]. There was a danger, the court held, that the first applicant's telecommunications might be monitored and her journalistic sources might be disclosed or deterred from contacting her. There was therefore an interference with her Art 10 rights. The same applies to Privacy International. Privacy International works on capacity building on issues of privacy in developing countries, sometimes in places with weak democracies which are of particular interest to U.S. and UK foreign policy, and where strong privacy safeguards may conflict with the objectives of intelligence agencies. Groups and individuals in repressive regimes, individuals in the UK concerned about their own privacy, as well as victims, whistleblowers and journalists frequently contact Privacy International. They may be dissuaded from doing so, or from communicating freely, for fear that their communications will be monitored.

Justification for interference

37. In order for the interference pursuant to Art 8 and 10 to be justified it must be "*in accordance with the law*" or "*prescribed by law*", must pursue one or more of the legitimate aims set out in Art 8(2)/10(2) and must be "*necessary in a democratic society*."

38. There is a significant body of jurisprudence of the ECHR on what constitutes interference "*prescribed by law*" in the context of secret surveillance and information gathering. It has been held that the legal regime governing interception of communication must be 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*." (*Malone* [67]). 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 *"prescribed by 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* (2009) 48 EHRR 1 at [69]).

39. In *Weber* the ECHR summarised its jurisprudence on the requirement that interception, examination and storage 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.*

40. The Court continued in *Weber* by setting out the minimum requirements of a legal regime governing secret surveillance and interference with communication for it to be regarded as lawful:

> *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.*

41. In *Weber* itself the ECHR held that the German regime governing interception of communications was of sufficient detail and specificity and was sufficiently accessible to render any interference with Art 8/10 rights in accordance with the law. There was a clear statutory provision that set out the categories of people liable to have their communications intercepted, the duration of any interception, the limits and precautions concerning transmission of material, the circumstances in which material would be retained or destroyed and provisions by which individuals would be notified that their telecommunications had been intercepted (when that could be done without jeopardising the purpose of monitoring). Similarly, the ECHR held in *Kennedy* that where interception of internal communication occurred in the UK pursuant to RIPA and the Code of Practice, the governing legal framework was sufficiently clear and accessible and contained sufficient safeguards against arbitrary use or abuse of power that it, too, was "*in accordance with the law*" for the purposes of Art 8.

42. The operation of the UK's domestic regime can be illustrated if one takes, for example, an individual living in London who sends an email or makes a skype call to someone located elsewhere in the UK. If UK authorities are to lawfully intercept the email or phone call during its transmission, they will require a warrant issued by the Secretary of State pursuant to RIPA s 5. 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 the person or premises as the interception subject (RIPA s 8(1)) and 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.

43. The position is entirely different if the same information is obtained from a foreign source. If the UK authorities ask the US authorities to intercept the individual's emails or calls as they pass through US fibre cables or communications infrastructure, no published legal structure applies indicating the circumstances in which, and conditions on which, that can occur. That will be so even if both the person sending and the person receiving the email or call are located in the UK but it happens to pass through the US. Similarly if the UK requests US authorities to obtain such information from a US based internet company, RIPA will not apply. Simply put, there is no domestic legal regime meeting the requirements of Art 8/10 which will set out the circumstances in which UK authorities can obtain, store and transfer UK residents private communication and other information that are intercepted by US authorities, nor which will govern the circumstances in which the UK can request the interception. The same applies to obtaining private information such as emails, web-histories etc held by internet and other telecommunication companies. Nor is there a legal regime that indicates, once such communications are provided to UK authorities, the procedure for examining, using or storing the communication, the conditions for transferring it to third parties and the circumstances in which it will be destroyed which satisfy Arts 8 and 10.

44. It is also not clear (partly because of the lack of an accessible legal regime) that the collection, receipt, storage and transmission of information will pursue a legitimate aim and be necessary in a democratic society. Pursuant to RIPA, the necessity of interception, as well as the requisite procedural safeguards, are, in part, ensured by the provision in RIPA s 5(3) that interception requires a warrant issued by the Secretary of State who must be satisfied that the warrant is necessary on grounds of national

security, preventing or detecting serious crime etc. Pursuant to FISA section 1881a, the NSA can obtain information with respect to a lawful political organisation (if it is located outside the US and does not involve the intentional targeting of US citizens), provided only that the information obtained is in some way related to the conduct of US foreign affairs. There is no requirement that obtaining the information is necessary to protect US, let alone UK, national security interests or to prevent serious crime. The communication can relate to legitimate political activities of those who seek to discuss, criticise or influence US foreign policy. The interceptions and collection of such communications not only cannot be said to be "*necessary in a democratic society*", but the threat of such monitoring chills lawful communication about political matters that are essential to the proper functioning of a democratic society.

45. With communication being increasingly global, and vast amounts of personal data being transferred and stored around the world, there is an obvious gap in legal protection to ensure respect for private life. The regimes in both the US and the UK governing the interception, obtaining, and storing of material deal differently with foreign and domestic interception and information gathering (in the UK the difference depends on whether communication is regarded as "*internal*" or "*external*" and in the US on whether or not the person targeted is a non-US citizen located outside the US). Those differences between foreign and domestic interception and information gathering regimes lead to an absence of legal protection when information is shared between countries. UK authorities can intercept communications sent or received by individuals located in the US (and which will be regarded as "*external*" for the purposes of RIPA), which happen to pass through UK fibre cables, and hand them over to US authorities, thus avoiding the US rules governing interception of those located within the country. The NSA can intercept an email under FISA section 1881a which is sent between two individuals in London because it happens to travel through the US as it will be regarded as "*foreign intelligence material*" as far as the US authorities are concerned, and it can then be handed over to the UK authorities without their having to comply with any of the requirements governing interception set out in RIPA and the Code of Practice. The same is true of private information about UK residents stored by internet companies in the US.

46. The absence of a sufficiently clear legal regime protecting the privacy of individuals in the UK to deal with those situations and to provide sufficient protection against abuse of power and arbitrary use is a breach of ECHR Art 8/10.

GROUND 2

47. Privacy International also complains of a further breach of:

    a. Articles 8 and 14 ECHR;

    b. RIPA 2000; and

    c. Article 12 TFEU.

Factual background

48. Privacy International complains about the intelligence operation known as *Tempora* reported in the *Guardian* newspaper on 21 June 2013. Under this operation, GCHQ has intercepted more than 200 fibre optic cables landing in the United Kingdom. Extracted data is stored for at least 3 days for content, and 30 days for metadata and is automatically searched according to search terms. Intercepted traffic includes internet usage and telephone calls. It is reported that GCHQ has set over 40,000 search terms and the US National Security Agency has set over 31,000 search terms which are used to determine which data should be extracted.GCHQ is reported to collect more metadata than the NSA, and to collect vast quantities of data. Under this programme, there is therefore bulk interception, storage and search of internet traffic of all users of intercepted fibre optic cables.

49. *Tempora* was purportedly authorised under certificated warrants issued pursuant to section 8(4) of RIPA 2000. Such certificated warrants do not have to name or describe either one person or a single set of premises as the subject of the interception.

50. Pursuant to *Tempora* <u>all</u> data on the intercepted fibre optic cables is intercepted, whether internal or external, and extracted data is subject to storage and search.

51. The certificated warrants described above have been in place for several years, and are renewed on a rolling basis by the Secretary of State. The vast majority of data intercepted concerns persons over whom there is no basis whatsoever for suspicion of terrorism or serious crime. Nevertheless, all such data is intercepted, searched and stored.

52. There is no requirement of judicial authorisation or approval of warrants or certificates.

53. The effect of *Tempora* is that all communications using fibre optic cables are subject to the risk of interception, search and storage. In practical terms, all users of telephones and the internet in the UK, Europe and worldwide are subject to the risk of interception.

Ground of challenge

54. Privacy International is a victim for the purposes of section 7 of the Human Rights Act 1998 for the reasons set out above under Ground 1. It falls within the group of individuals or organisations which may be subject to interception of its communications for the reasons set out above.

55. The requirements for justification of the interference are set out above. *Tempora* is in breach of Article 8 ECHR because:

    a. The operation is not prescribed by law. RIPA does not provide sufficiently specific or clear authorisation for such wide-ranging and universal interception of communications, nor any sufficient or proper safeguards against misuse that are known and available to the public.

    b. The operation is disproportionate. The collection, search and storage of all communications data passing through very large numbers of fibre optic cables on a continuous basis comprises blanket surveillance. Such surveillance cannot be justified as a proportionate response to a legitimate aim. Bulk interception of communications and bulk inspection of such data is a disproportionate interference with the rights guaranteed by Article 8.

    c. In addition, the following specific elements of the operation are disproportionate and unjustified:
        i. The scale, selection and content of the search terms applied.
        ii. The permission given to the NSA to select search terms.
        iii. The granting of access to such data to US officials.
        iv. The absence of judicial control over the grant of certificated warrants.

v. The absence of the requirement for a warrant targeting specific individuals or premises.
vi. The search and storage of bulk data over individuals where there is no reason to suspect involvement of those individuals in terrorism or serious crime.
vii. Rolling renewal of authorisations.

56. For the same reasons, the operation and the grant of the warrants is in breach of section 5(2) of RIPA in that it is disproportionate to what is sought to be achieved by the interception.

57. Further, the operation is in breach of Article 12(1) TFEU. The *Tempora* operation has a disparate adverse impact on EU citizens who are not nationals of the United Kingdom. This is because a certification under section 8(4) of RIPA 2000 can only be granted in respect of the interception of external communications, which are more likely to be made by non-UK citizens. Union citizens who are not UK citizens are far more likely to have their communications intercepted, searched and retained. Both UK citizens and non-UK citizens pose risks to national security. Accordingly, such differences in treatment are not justifiable or lawful. A systematic scheme of processing of personal data primarily directed at non-UK nationals cannot be justified under EU law. See *Case C-524/06 Huber v Germany* [2008] ECR I-9705 at [69-81].

58. Article 14 ECHR read with Article 8 leads to the same conclusion. The *Tempora* operation involves unjustified discrimination against non-UK nationals. See *A v SSHD (No. 1)* [2005] 2 AC 68.

59. Privacy International seeks a public hearing of its complaint. The existence and scope of the *Tempora* operation is now in the public domain. The ordinary policy of 'neither confirm nor deny' has no lawful or proper basis in such circumstances. See *R (Bancoult) v SSFCA* [2013] EWHC 1502 (Admin).

CONCLUSION

60. These grounds accompany the forms T1 and T2 filed by Privacy International. They set out, in summary terms, the Grounds relied upon. Privacy International will make detailed submissions and serve evidence in due course, once the basis on which it s alleged that the operations are proportionate and lawful has been disclosed

61. Privacy International seeks the following orders:

(i) A declaration that the Secretary of State for the Foreign Office and/or the Secretary of State for the Home office have unlawfully failed to ensure that there is in place a regime which complies with Article 8 and 10 ECHR governing the soliciting, receiving, storing and transmitting by UK authorities of private communications of individuals located in the UK which have been obtained by US authorities.

(ii) A declaration that the soliciting, receipt, storage and transmission of such information by the Security Service, the Secret Intelligence Service and/or GCHQ is unlawful.

(iii) An order that the Security Service, the Secret Intelligence Service and/or GCHQ will not solicit, receive, store or transmit such information unless and until such activities are governed by a legal regime which satisfies ECHR Art 8 and 10 and will destroy any material unlawfully obtained.

(iv) A declaration that the *Tempora* operation under which there is blanket interception, search and storage of data passing through fibre optic cables is unlawful and contrary to Article 8 ECHR, Article 14 ECHR, RIPA 2000 and Article 12 TFEU and an order requiring the destruction of any unlawfully obtained material.

(v) An injunction restraining further unlawful conduct.

Dinah Rose QC
Ben Jaffey
Blackstone Chambers

Dan Squires
Matrix Chambers

8 July 2013