EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

Communicated on 24 November 2015

FIRST SECTION

Application no. 24960/15
10 HUMAN RIGHTS ORGANISATIONS and Others
against the United Kingdom
lodged on 20 May 2015

STATEMENT OF FACTS

The applicants are ten human rights organisations whose details are set out in the Appendix.

A. The circumstances of the case

The facts of the case, as submitted by the applicants, may be summarised as follows.

1. The background facts

The applicants communicate on a regular basis with a range of groups and individuals, both nationally and internationally, as part of their human rights activities. Their contacts include other non-governmental organisations, politicians, government officials, journalists, lawyers, victims of human rights abuses and whistle-blowers. The applicants' staff members communicate using a variety of means including email, text messages, phone calls, video calls, social media and instant messaging. The information contained in their communications frequently includes material which is sensitive, confidential and, in some cases, legally privileged.

Because of the nature of their activities, the applicants believe that it is very likely that the content of their private communications and their communications data have been obtained by the United Kingdom intelligence services via interception powers exercised pursuant to the Regulation of Investigatory Powers Act 2000 ("RIPA"), under the domestic interception and collection programme, Tempora, or by way of the Prism or Upstream programmes operated by the United States National Security Agency ("NSA"). Further details of these programmes are set out below.

2. The three surveillance programmes

In 2013 Mr Edward Snowden, a former systems administrator with the NSA, leaked information revealing mass surveillance programmes operated by the NSA.

According to the leaked documents, the Prism programme allows access to the content of communications (including emails, chats, video, images, documents, links and other information) and communications data (information permitting the identification and location of internet users) in respect of communications which pass through large US companies, including Microsoft, Apple, Yahoo, Google, Facebook, PalTalk, AOL, Skype and YouTube. Since Global internet data take a mixture of the cheapest and fastest routes rather than the most direct route, a substantial amount of global data passes through the servers of US companies. The leaked documents show that the United Kingdom Government Communications Headquarters ("GCHQ") has had access to Prism since July 2010 and has used it to generate intelligence reports.

The Upstream programme allows the collection of content and communications data from fibre-optic cables and infrastructure owned by US communications service providers. This programme has broad access to global data, in particular of non-US citizens, which can then be collected, stored and searched using keywords.

GCHQ's operates its own surveillance programme, Tempora. This programme allows GCHQ to access content and communications data passing through fibre optic cables running from the United Kingdom to North America and then use "selector terms" (such as phone numbers and email addresses) to filter the data. The Tempora program is authorised by a section 8(4) warrant under the Regulation of Investigatory Powers Act 2000 ("RIPA" – see "Relevant domestic law and practice", below). According to the applicants, the United States Government have access to the information collected by Tempora.

3. The domestic proceedings

(a) The lodging of the complaints before the Investigatory Powers Tribunal

Between June and December 2013, each of the ten applicants lodged a complaint before the Investigatory Powers Tribunal ("IPT"). They alleged that the intelligence services, the Home Secretary and the Foreign Secretary had acted in violation of Articles 8, 10, and 14 by: (i) accessing or otherwise receiving intercepted communications and communications data from the US Government under the Prism and Upstream programmes ("the Prism issue"); and (ii) intercepting, inspecting and retaining their communications and their communications data under the Tempora programme ("the section 8(4) issue"). The applicants sought disclosure of all relevant material relied on by the intelligence services in the context of their interception activities and, in particular, all policies and guidance.

On 14 February 2014 the IPT ordered that the ten cases be joined. It subsequently appointed counsel to the tribunal.

In their response to the applicants' claims, the Government adopted a "neither confirm nor deny" approach, that is to say, they declined to confirm or deny whether the applicants' communications had actually been

intercepted. It was therefore agreed that the IPT would determine the legal issues on the basis of assumed facts, namely that the NSA had obtained the applicants' communications and communications data via Prism or Upstream and had passed them to GCHQ, where they had been retained, stored, analysed and shared; and that the applicants' communications and communications data had been intercepted by GCHQ under the Tempora programme and had been retained, stored, analysed and shared. The question was whether, on these assumed facts, interception, retention, storage and sharing of data was in accordance with the law under Articles 8 and 10, taken alone and together with Article 14.

The IPT held a five-day, public hearing from 14-18 July 2014. The Government requested an additional closed hearing in order to enable the IPT to consider the GCHQ's unpublished internal arrangements – so-called "below the waterline" – for processing data. The applicants objected, arguing that the holding of a closed hearing was not justified and that the failure to disclose the arrangements to them was unfair. The request for a closed hearing was granted pursuant to Rule 9 of the IPT's Rules of Procedure (see "Relevant domestic law and practice", below) and on 10 September a closed hearing took place. The applicants were neither present nor represented. In the closed hearing, the IPT examined the internal arrangements regulating the conduct and practice of the intelligence services. It found that it was entitled to look "below the waterline" to consider the adequacy of the applicable safeguards and whether any further information could or should be disclosed to the public in order to comply with the requirements of Articles 8 and 10.

On 9 October 2014 the IPT notified the applicants that it was of the view that there was closed material which could be disclosed. It explained that it had invited the Government to disclose the material and that the Government had agreed to do so. The material was accordingly provided to the applicants in a note ("the 9 October disclosure") and the parties were invited to make submissions to the IPT on the disclosed material.

The applicants sought information on the context and source of the disclosure but the IPT declined to provide further details. The applicants made written submissions on the disclosure.

The respondents subsequently further amended and amplified the disclosed material. Following final disclosures made on 12 November 2014, the 9 October disclosure provided as follows:

> "The US Government has publicly acknowledged that the Prism system and Upstream programme ... permit the acquisition of communications to, from, or about specific tasked selectors associated with non-US persons who are reasonably believed to be located outside the United States in order to acquire foreign intelligence information. To the extent that the Intelligence Services are permitted by the US Government to make requests for material obtained under the Prism system (and/or ... pursuant to the Upstream programme), those requests may only be made for unanalysed intercepted communications (and associated communications data) acquired in this way.
>
> 1. A request may only be made by the Intelligence Services to the government of a country or territory outside the United Kingdom for unanalysed intercepted communications (and associated communications data), otherwise than in accordance with an international mutual legal assistance agreement, if either:

a. a relevant interception warrant under [RIPA] has already been issued by the Secretary of State, the assistance of the foreign government is necessary to obtain the communications at issue because they cannot be obtained under the relevant RIPA interception warrant and it is necessary and proportionate for the Intelligence Services to obtain those communications; or

b. making the request for the communications at issue in the absence of a relevant RIPA interception warrant does not amount to a deliberate circumvention of RIPA or otherwise contravene the principle established in *Padfield v. Minister of Agriculture, Fisheries and Food* [1968] AC 997 [that a public body is required to exercise its discretionary powers to promote (and not to circumvent) the policy and the objects of the legislation which created those powers] (for example, because it is not technically feasible to obtain the communications via RIPA interception), and it is necessary and proportionate for the Intelligence Services to obtain those communications. In these circumstances, the question whether the request should be made would be considered and decided upon by the Secretary of State personally. Any such request would only be made in exceptional circumstance, and has not occurred as at the date of this statement.

...

2. Where the Intelligence Services receive intercepted communications content or communications data from the government of a country or territory outside the United Kingdom, irrespective whether it is/they are solicited or unsolicited, whether the content is analysed or unanalysed, or whether or not the communications data are associated with the content of communications, the communications content and data are, pursuant to internal "arrangements", subject to the same internal rules and safeguards as the same categories of content or data, when they are obtained directly by the Intelligence Services as a result of interception under RIPA.

3. Those of the Intelligence Services that receive unanalysed intercepted material and related communications data from interception under a s.8(4) warrant have internal 'arrangements' that require a record to be created, explaining why access to the unanalysed intercepted material is required, before an authorised person is able to access such material pursuant to s.16 of RIPA.

4. The internal 'arrangements' of those of the Intelligence Services that receive unanalysed intercepted material and related communications data from interception under a s.8(4) warrant specify (or require to be determined, on a system-by-system basis) maximum retention periods for different categories of such data which reflect the nature and intrusiveness of the particular data at issue. The periods so specified (or determined) are normally no longer than 2 years, and in certain cases are significantly shorter (intelligence reports that draw on such data are treated as a separate category, and are retained for longer). Data may only be retained for longer than the applicable maximum retention period where prior authorisation has been obtained from a senior official within the particular Intelligence Service at issue on the basis that continued retention of the particular data at issue has been assessed to be necessary and proportionate (if the continued retention of any such data is thereafter assessed no longer to meet the tests of necessity and proportionality, such data are deleted). As far as possible, all retention periods are implemented by a process of automated deletion which is triggered once the applicable maximum retention period has been reached for the data at issue. The maximum retention periods are overseen by, and agreed with the Commissioner. As regards related communications data in particular, Sir Anthony May made a recommendation to those of the Intelligence Services that receive unanalysed intercepted material and related communications data from interception under a s8(4) warrant, and the interim Commissioner (Sir Paul Kennedy) has recently expressed himself to be content with the implementation of that recommendation.

5. The Intelligence Services' internal 'arrangements' under SSA [the Security Services Act 1989], ISA [the Intelligence Services Act 1994] and ss.15-16 of RIPA are periodically reviewed to ensure that they remain up-to-date and effective. Further, the Intelligence Services are henceforth content to consider, during the course of such periodic reviews, whether more of those internal arrangements might safely and

usefully be put into the public domain (for example, by way of inclusion in a relevant statutory Code of Practice)."

(b) The IPT's first judgment of 5 December 2014

The IPT issued its first judgment on 5 December 2014. The judgment addressed the current arrangements in place (i.e. as of 5 December 2014) for intercepting and sharing data and made extensive reference throughout to this Court's case-law, and in particular the cases of *Weber and Saravia v. Germany* (dec.), no. 54934/00, ECHR 2006-XI; *Liberty v. the United Kingdom*, no. 58243/00, 1 July 2008; and *Kennedy v. the United Kingdom*, no. 26839/05, 18 May 2010.

The tribunal identified two parts to the claim: the Prism issue and the section 8(4) issue (see the description of the complaints lodged, above). It began by underlining the importance of setting the complaints into context, explaining:

"6. ... The actions of the Respondents... are all taken, or assumed to be taken, in the interests of national security, and at a time when ... the threat to the United Kingdom from international terrorism is 'Substantial', indicating that an attack is a strong possibility; this has been recently upgraded to 'Severe', meaning that an attack is highly likely. The Claimants accept that Convention jurisprudence recognises the need for states to defend themselves and to introduce measures in support of national security, and that the concept, familiar within the confines of Article 8, of accessibility and foreseeability, of laws, rules and arrangements established by democracies in that regard may be approached differently from those situations where national security is not an issue ..."

The IPT accepted that the Prism issue engaged Article 8 and that there would need to be compliance by the authorities involved in processing the data with requirements imposed by that Article, particularly in relation to storage, sharing, retention and destruction. In its view, in order for the interference to be considered "in accordance with the law", there could not be unfettered discretion for executive action, the nature of the rules had to be clear and the ambit of the rules had to be in the public domain so far as possible (citing *Bykov v. Russia* [GC], no. 4378/02, §§ 76 and 78, 10 March 2009). The tribunal considered it plain that in the field of national security, much less was required to be put in the public domain and the degree of foreseeability required by Article 8 had to be reduced, because otherwise the whole purpose of the steps taken to protect national security would be at risk (citing *Leander v. Sweden*, 26 March 1987, § 51, Series A no. 116).

The IPT continued:

"41. We consider that what is required is a sufficient signposting of the rules or arrangements insofar as they are not disclosed ... We are satisfied that in the field of intelligence sharing it is not to be expected that rules need to be contained in statute (**Weber**) or even in a code (as was required by virtue of the Court's conclusion in **Liberty v UK**). It is in our judgment sufficient that:

i) Appropriate rules or arrangements exist and are publicly known and confirmed to exist, with their content sufficiently signposted, such as to give an adequate indication of it (as per **Malone** ... [*v. the United Kingdom*, 2 August 1984, Series A no. 82]).

ii) They are subject to proper oversight."

As to the existence of rules or arrangements, the IPT noted that arrangements were provided for in the statutory framework set out in the Security Services Act 1994 ("the SSA") and the Intelligence Services Act

1994 ("the ISA" – see "Relevant domestic law and practice", below). It further referred to a witness statement where the Director-General of the Office for Security and Counter Terrorism ("OSCT") at the Home Office had explained that the statutory framework set out in those Acts was underpinned by detailed internal guidance, including arrangements, in respect of which staff received mandatory training; and that the full details of the arrangements were confidential since they could not be safely published without undermining the interests of national security. The tribunal acknowledged that the arrangements were not made known in their detail to the public and that, to that extent, were not accessible. It further accepted that, unlike the Code of Practice published under RIPA, not even a summary of what they contained had been disclosed. However, the IPT considered it significant that the arrangements were subject to oversight and investigation by the Intelligence and Security Committee of Parliament and the independent Interception of Communications Commissioner.

In so far as the claimants challenged the tribunal's decision to look "below the waterline" when assessing the adequacy of the safeguards, the IPT considered itself entitled to look at the internal arrangements in order to be satisfied that there were adequate safeguards and that what was described "above the waterline" was accurate and gave a sufficiently clear signposting as to what was "below the waterline" without disclosing the detail of it.

The IPT did not accept that the holding of a closed hearing, as it had been carried out in the applicants' case, was unfair. In the IPT's view, it accorded with the statutory procedure, gave the fullest and most transparent opportunity for hearing full arguments *inter partes* on hypothetical and actual facts with as much as possible heard in public, and protected the public interest and national security. The tribunal was satisfied that the 9 October disclosure (as subsequently amended) provided a clear and accurate summary of that part of the evidence given in the closed hearing which could and should be disclosed and that the rest of the evidence given in closed hearing was too sensitive for disclosure without risk to national security or to the "neither confirm nor deny" principle.

In relation to the receipt of intercept material from Prism and Upstream, the IPT held that the internal arrangements were adequate for ensuring compliance with the statutory framework and with Articles 8 and 10 of the Convention. The tribunal was further satisfied that the arrangements were sufficiently signposted in the statutory framework, the statements of the Intelligence and Security Committee and the Interception of Communications Commissioner and the 9 October disclosure. They were also subject to appropriate oversight. It concluded that the scope of discretion conferred on the respondents to receive and handle the material, and the manner of its exercise were accordingly accessible with sufficient clarity to give the individual adequate protection against arbitrary interference. There was therefore was no breach of Articles 8 or 10.

As regards the section 8(4) issue, the IPT reviewed the applicable legal framework in RIPA, including the sections 15 and 16 safeguards requiring the putting in place of appropriate arrangements for collecting and processing the data (see "Relevant domestic law and practice", below), and the supporting Code of Practice. It referred again to the witness statement of the Director General, in which he had explained that while full details of the

sections 15 and 16 arrangements could not be made public, they were made available to the Interception of Communications Commissioner who was required to keep them under review, each intercepting agency was required to keep a record of the arrangements in questions; and any breach of the arrangements had to be reported to the Commissioner.

The IPT formulated four questions to be decided in order to determine whether the section 8(4) regime was compatible with Articles 8 of the Convention:

> "(1) Is the difficulty of determining the difference between *external* and *internal* communications ... such as to cause the s.8(4) regime not to be *in accordance with law* contrary to Article 8(2)?
>
> (2) Insofar as s.16 of RIPA is required as a safeguard in order to render the interference with Article 8 *in accordance with law*, is it a sufficient one?
>
> (3) Is the regime, whether with or without s.16, sufficiently compliant with the **Weber** requirements, insofar as such is necessary in order to be *in accordance with law*?
>
> (4) Is s.16(2) indirectly discriminatory contrary to Article 14 of the Convention, and, if so, can it be justified?"

In relation to the first question, the IPT found that the differences in view as to the definition of "external communications" did not render the section 8(4) regime incompatible with Article 8 § 2. The tribunal explained that the difficulty in distinguishing between "internal" and "external" communications had existed since the enactment of RIPA and that both types of communications, if intercepted under a section 8(4) warrant, were in any case to be considered for examination by reference to section 16 RIPA.

In respect of the second question, the IPT held that the section 16 RIPA safeguards were sufficient. It explained that although the section provided greater protection in certain respects for communications content, rather than data, and while it was true that the *Weber* requirements also extended to communications data, the difference in treatment was justified and proportionate because that data were used to identify individuals whose intercepted material was protected by section 16 (that is, because of physical presence in the British Islands).

Turning to the third question, the IPT concluded that the section 8(4) regime was sufficiently compliant with the *Weber* requirements and was in any event "in accordance with the law". The failure to target communications at interception level was acceptable and inevitable. There was no requirement for search words to be included in an application for a warrant or in the warrant itself, or for the warrant to be judicially authorised. The tribunal was further of the view that it was not necessary that the precise details of all the safeguards should be published or contained in legislation. The undisclosed, administrative arrangements could be taken into account provided that the scope of the discretion and the manner of its exercise were disclosed. The IPT was satisfied that, as a result of what it had heard at the closed hearings and the 9 October disclosure as amended, there was no large databank of communications data being built up and that there were adequate arrangements in respect of duration of retention of data and its destruction. As with the Prism issue, the tribunal considered that the section 8(4) arrangements were sufficiently signposted in statute, in the

Code of Practice, in the Interception of Communications Commissioner's reports and, now, in its own judgment.

As regards the fourth and final question, the IPT did not make any finding as to whether there was in fact indirect discrimination on grounds of national origin as a result of the different regimes applicable to individuals located in the British Islands and those located outside. It considered that any indirect discrimination was sufficiently justified on the grounds that it was harder to investigate terrorism and crime threats from abroad and that to require a certificate under section 16(3) RIPA (see "Relevant domestic law and practice", below), which exceptionally allows access to material concerning persons within the British Islands intercepted under a section 8(4) warrant on a case-by-case basis, would radically undermine the efficacy of the section 8(4) regime.

Finally, the IPT noted that there was no separate argument in relation to Article 10, over and above that arising in respect of Article 8, save that there might be a special argument relating to Article 10 with respect to the need for judicial pre-authorisation of a warrant (referring to *Sanoma Uitgevers B.V. v. the Netherlands* [GC], no. 38224/03, 14 September 2010). In relation to this, the tribunal emphasised that the applicants' case did not concern targeted surveillance of journalists or non-governmental organisations. In the context of untargeted monitoring via a section 8(4) warrant, it was "clearly impossible" to anticipate a judicial pre-authorisation prior to the warrant limited to what might turn out to impact upon Article 10. Although the tribunal accepted that an issue might arise in the event that, in the course of examination of the contents, some question of journalistic confidence arose, it observed that there were additional safeguards in the Code of Practice in relation to treatment of such material.

Following the publication of the judgment, the parties were invited to make submissions on whether, prior to the judgment, the legal regime in place in respect of the Prism issue complied with Articles 8 and 10 and on the proportionality and lawfulness of any alleged interception of their communications. The tribunal did not permit further submissions on the proportionality of the section 8(4) regime as a whole.

(c) The IPT's second judgment of 6 February 2015

In its second judgment of 6 February 2015, the IPT considered whether, prior to its December 2014 judgment, the Prism or Upstream arrangements breached Article 8 or 10.

It agreed that it was only by reference to the 9 October disclosure as amended that it was satisfied the current regime was "in accordance with the law". The tribunal was of the view that without the disclosures made, there would not have been adequate signposting, as was required under Articles 8 and 10. It therefore made a declaration that prior to the disclosures made:

> "23. ... [T]he regime 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 pursuant to Prism and/or ... Upstream, contravened Articles 8 or 10 ECHR, but now complies."

(d) The IPT's third judgment of 22 June 2015 as amended by its 1 July 2015 letter

The third judgment of the IPT, published on 22 June 2015, determined whether the applicants' communications obtained under Prism or Upstream had been solicited, received, stored or transmitted by the United Kingdom authorities in contravention of Articles 8 or 10 of the Convention; and whether the applicants' communications had been intercepted, viewed, stored or transmitted by the United Kingdom authorities so as to amount to unlawful conduct or in contravention of Articles 8 or 10.

The tribunal made no determination in favour of eight of the ten applicants. In line with its usual practice where it did not find in favour of the claimant, it did not confirm whether or not their communications had been intercepted. The IPT made determinations in favour of two organisations. The identity of one of the organisations was wrongly noted in the judgment and the error was corrected by the IPT's letter of 1 July 2015.

In respect of Amnesty International, the IPT found that email communications had been lawfully and proportionately intercepted and accessed pursuant to section 8(4) RIPA but that the time-limit for retention permitted under the internal policies of GCHQ had been overlooked and the material had therefore been retained for longer than permitted. However, the IPT was satisfied that the material had not been accessed after the expiry of the relevant retention time-limit and that the breach could be characterised as a technical one. It amounted nonetheless to a breach of Article 8 and GCHQ was ordered to destroy any of the communications which had been retained for longer than the relevant period and to deliver one hard copy of the documents within seven days to the Interception of Communications Commissioner to retain for five years in case they were needed for any further legal proceedings. GCHQ was also ordered to provide a closed report within fourteen days confirming the destruction of the documents. No award of compensation was made.

In respect of the Legal Resources Centre, the IPT found that communications from an email address associated with the applicant had been intercepted and selected for examination under a section 8(4) warrant. Although it was satisfied the interception was lawful and proportionate and that selection for examination was proportionate, the IPT found that the internal procedure for selection was, in error, not followed. There had therefore been a breach of the Legal Resources Centre's Article 8 rights. However, the IPT was satisfied that no use was made of the material and that no record had been retained so the applicant had not suffered material detriment, damage or prejudice. Its determination therefore constituted just satisfaction and no compensation was awarded.

B. Relevant domestic and international law

1. The operation of the intelligence services

There are three intelligence services in the United Kingdom: the security service ("MI5"), the secret intelligence service ("MI6") and GCHQ.

Section 1 of the Security Services Act 1994 ("SSA") provides a statutory basis for the operation of MI5. The functions of MI5 are the protection of

national security and, in particular, its protection against threats from espionage, terrorism and sabotage, from the activities of agents of foreign powers and from actions intended to overthrow or undermine parliamentary democracy by political, industrial or violent means; to safeguard the economic well-being of the United Kingdom against threats posed by the actions or intentions of persons outside the British Islands; and to act in support of the activities of police forces, the National Crime Agency and other law enforcement agencies in the prevention and detection of serious crime.

Pursuant to section 2 of the SSA, the operations of MI5 are under the control of the Director-General, who is appointed by the Secretary of State. It is the duty of the Director-General to ensure that there are arrangements for securing that no information is obtained by MI5 except so far as necessary for the proper discharge of its functions or disclosed by it except so far as necessary for that purpose or for the purpose of the prevention or detection of serious crime or for the purpose of any criminal proceedings.

Section 1 of the Intelligence Services Act 1994 ("ISA") provides a statutory basis for the operation of MI6. The functions of MI6 are to obtain and provide information relating to the actions or intentions of persons outside the British Islands; and to perform other tasks relating to the actions or intentions of such persons. MI6 can only exercise its functions in the interests of national security, with particular reference to the State's defence and foreign policies, in the interests of the economic well-being of the United Kingdom or in support of the prevention or detection of serious crime.

Section 2 of ISA provides for the control of the operations of MI6 by a Chief of Service, to be appointed by the Secretary of State. The Chief's duties include ensuring that there are arrangements for securing that no information is obtained by MI6 except so far as necessary for the proper discharge of its functions, and that no information is disclosed by it except so far as necessary for that purpose, in the interests of national security, for the purposes of the prevention or detection of serious crime or for the purpose of any criminal proceedings.

Section 3 of ISA sets out the authority for the operation of GCHQ. One of the functions of GCHQ is to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material. Again, this function is exercisable only in the interests of national security, with particular reference to the State's defence and foreign policies, in the interests of the economic well-being of the United Kingdom in relation to the actions or intentions of persons outside the British Islands or in support of the prevention or detection of serious crime.

Section 4 provides that GCHQ's operations are under the control of a Director, who is appointed by the Secretary of State. It is the duty of the Director to ensure that there are arrangements for securing that no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary.

Section 19 of the Counter-Terrorism Act 2008 allows the disclosure of information to any of the intelligence services for the purpose of the exercise of any of its functions. It provides that the information an intelligence service obtains in connection with its functions may be used by that service in connection with any of its other functions. Information obtained by MI5 and MI6 may be disclosed by them for the purpose of the proper discharge of their functions, in the interests of national security, for the purpose of the prevention or detection of serious crime or for the purpose of any criminal proceedings". Information obtained by GCHQ may be disclosed by it for the purpose of the proper discharge of its functions or for the purpose of any criminal proceedings.

2. The interception of communications

The Regulation of Investigatory Powers Act 2000 ("RIPA") came into force on 15 December 2000. The explanatory memorandum described the main purpose of the Act as being to ensure that the relevant investigatory powers were used in accordance with human rights.

Section 1(1) of RIPA makes it an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of a public postal service or a public telecommunication system.

Section 8(4) and (5) allows the Secretary of State to issue a warrant for "the interception of external communications in the course of their transmission by means of a telecommunication system". At the time of issuing such a warrant, he must also issue a certificate setting out a description of the intercepted material which he considers it necessary to be examined, and stating that the warrant is necessary, *inter alia*, in the interests of national security, for the purpose of preventing or detecting serious crime or for the purpose of safeguarding the economic well-being of the United Kingdom and that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

RIPA sets out a number of general safeguards in section 15. Pursuant to Section 15(1), it is the duty of the Secretary of State to ensure, in relation to all interception warrants, that such arrangements are in force as he considers necessary for securing that the requirements of subsections (2) and (3) are satisfied in relation to the intercepted material and any related communications data; and, in the case of warrants in relation to which there are section 8(4) certificates, that the requirements of section 16 are also satisfied.

Section 15(2) provides:

> "The requirements of this subsection are satisfied in relation to the intercepted material and any related communications data if each of the following–
>
> (a) the number of persons to whom any of the material or data is disclosed or otherwise made available,
>
> (b) the extent to which any of the material or data is disclosed or otherwise made available,
>
> (c) the extent to which any of the material or data is copied, and
>
> (d) the number of copies that are made,
>
> is limited to the minimum that is necessary for the authorised purposes."

Section 15(3) provides:

> "The requirements of this subsection are satisfied in relation to the intercepted material and any related communications data if each copy made of any of the material or data (if not destroyed earlier) is destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes."

Pursuant to section 15(4), something is necessary for the authorised purposes if, and only if, it continues to be, or is likely to become, necessary as mentioned in section 5(3) of the Act; it is necessary for facilitating the carrying out of any of the interception functions of the Secretary of State; it is necessary for facilitating the carrying out of any functions of the Interception of Communications Commissioner or of the Tribunal; it is necessary to ensure that a person conducting a criminal prosecution has the information he needs to determine what is required of him by his duty to secure the fairness of the prosecution; or it is necessary for the performance of any duty imposed on any person under public records legislation.

Section 15(5) requires the arrangements in place to secure compliance with section 15(2) to include such arrangements as the Secretary of State considers necessary for securing that every copy of the material or data that is made is stored, for so long as it is retained, in a secure manner.

Pursuant to section 15(6), the arrangements to which section 15(1) refers are not required to secure that the requirements of section 15(2) and (3) are satisfied in so far as they relate to any of the intercepted material or related communications data, or any copy of any such material or data, possession of which has been surrendered to any authorities of a country or territory outside the United Kingdom. However, such arrangements are required to secure, in the case of every such warrant, that possession of the intercepted material and data and of copies of the material or data is surrendered to authorities of a country or territory outside the United Kingdom only if the requirements of section 15(7) are satisfied. Section 15(7) provides:

> "The requirements of this subsection are satisfied in the case of a warrant if it appears to the Secretary of State–
>
> (a) that requirements corresponding to those of subsections (2) and (3) will apply, to such extent (if any) as the Secretary of State thinks fit, in relation to any of the intercepted material or related communications data possession of which, or of any copy of which, is surrendered to the authorities in question; and
>
> (b) that restrictions are in force which would prevent, to such extent (if any) as the Secretary of State thinks fit, the doing of anything in, for the purposes of or in connection with any proceedings outside the United Kingdom which would result in such a disclosure as, by virtue of section 17, could not be made in the United Kingdom."

Section 16 sets out additional safeguards in relation to interception of "external" communications under section 8(4) warrants. Section 16(1) explains that the requirements of section 16, for the purposes of section 15, are that the intercepted material is read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant to the extent only that it has been certified as material the examination of which is necessary as mentioned in section 5(3)(a), (b) or (c) of the Act; and falls within section 16(2).

Section 16(2) provides:

"Subject to subsections (3) and (4), intercepted material falls within this subsection so far only as it is selected to be read, looked at or listened to otherwise than according to a factor which–

(a) is referable to an individual who is known to be for the time being in the British Islands; and

(b) has as its purpose, or one of its purposes, the identification of material contained in communications sent by him, or intended for him."

Pursuant to section 16(3), intercepted material falls within section 16(2), even if it is selected by reference to one of the factors mentioned that subsection, if it is certified by the Secretary of State for the purposes of section 8(4) that the examination of material selected according to factors referable to the individual in question is necessary as mentioned in subsection 5(3)(a), (b) or (c) of the Act; and the material relates only to communications sent during a period specified in the certificate that is no longer than the permitted maximum.

The "permitted maximum" is defined in section 16(3A) as follows:

"(a) in the case of material the examination of which is certified for the purposes of section 8(4) as necessary in the interests of national security, six months; and

(b) in any other case, three months."

Pursuant to section 16(4), intercepted material also falls within section 16(2), even if it is selected by reference to one of the factors mentioned that subsection, if the person to whom the warrant is addressed believes, on reasonable grounds, that the circumstances are such that the material would fall within that subsection; or the conditions set out in section 16(5) are satisfied in relation to the selection of the material.

Section 16(5) provides:

"Those conditions are satisfied in relation to the selection of intercepted material if –

(a) it has appeared to the person to whom the warrant is addressed that there has been such a relevant change of circumstances as, but for subsection (4)(b), would prevent the intercepted material from falling within subsection (2);

(b) since it first so appeared, a written authorisation to read, look at or listen to the material has been given by a senior official; and

(c) the selection is made before the end of the permitted period."

Pursuant to section 16(5A), the "permitted period" means:

"(a) in the case of material the examination of which is certified for the purposes of section 8(4) as necessary in the interests of national security, the period ending with the end of the fifth working day after it first appeared as mentioned in subsection (5)(a) to the person to whom the warrant is addressed; and

(b) in any other case, the period ending with the end of the first working day after it first so appeared to that person."

Section 16(6) explains that a "relevant change of circumstances" means that it appears that either the individual in question has entered the British Islands; or that a belief by the person to whom the warrant is addressed in the individual's presence outside the British Islands was in fact mistaken.

Part IV of RIPA provides for the appointment of an Interception of Communications Commissioner and an Intelligence Services Commissioner, charged with supervising the activities of the intelligence services.

Section 65 of RIPA establishes the Investigatory Powers Tribunal, which has jurisdiction to determine claims related to the conduct of the intelligence services, including proceedings under the Human Rights Act 1998.

Section 71 of RIPA requires the Secretary of State to issue Codes of Practice relating to the exercise and performance of the powers and duties under the Act.

3. Data sharing

A British-US Communication Intelligence Agreement of 5 March 1946 governs the arrangements between the British and United States authorities in relation to the exchange of intelligence information relating to "foreign" communications, defined by reference to countries other than the United States, the United Kingdom and the Commonwealth. Pursuant to the agreement, the parties undertook to exchange the products of a number of interception operations relating to foreign communications

The Acquisition and Disclosure of Communications Data: Code of Practice, issued under section 71 RIPA, provides, in relation to the provision of data to foreign agencies:

> "**Acquisition of communication data on behalf of overseas authorities**
>
> 7.11 Whilst the majority of public authorities which obtain communications data under the Act have no need to disclose that data to any authority outside the United Kingdom, there can be occasions when it is necessary, appropriate and lawful to do so in matters of international co-operation.
>
> 7.12 There are two methods by which communications data, whether obtained under the Act or not, can be acquired and disclosed to overseas public authorities:
>
> Judicial co-operation
>
> Non-judicial co-operation
>
> Neither method compels United Kingdom public authorities to disclose data to overseas authorities. Data can only be disclosed when a United Kingdom public authority is satisfied that it is in the public interest to do so and all relevant conditions imposed by domestic legislation have been fulfilled.
>
> ...
>
> **Non-judicial co-operation**
>
> 7.15 Public authorities in the United Kingdom can receive direct requests for assistance from their counterparts in other countries. These can include requests for the acquisition and disclosure of communications data for the purpose of preventing or detecting crime. On receipt of such a request the United Kingdom public authority may consider seeking the acquisition or disclosure of the requested data under the provisions of Chapter II of Part I of the Act.
>
> 7.16 The United Kingdom public authority must be satisfied that the request complies with United Kingdom obligations under human rights legislation. The necessity and proportionality of each case must be considered before the authority processes the authorisation or notice.
>
> **Disclosure of communications data to overseas authorities**
>
> 7.17 Where a United Kingdom public authority is considering the acquisition of communications data on behalf of an overseas authority and transferring the data to that authority it must consider whether the data will be adequately protected outside the United Kingdom and what safeguards may be needed to ensure that. Such safeguards might include attaching conditions to the processing, storage and destruction of the data.

...

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

4. IPT practice and procedure

The IPT was established under section 65(1) RIPA to hear allegations by citizens of wrongful interference with their communications as a result of conduct covered by RIPA. Members of the tribunal must hold or have held high judicial office or be a qualified lawyer of at least ten years' standing. Any person may bring a claim before the IPT and, save for vexatious or frivolous applications, the IPT must determine all claims brought before it (sections 67(1), (4) and (5) RIPA).

Section 65(2) provides that the IPT is the only appropriate forum in relation to proceedings for acts incompatible with Convention rights which are proceedings against any of the intelligence services; and complaints by persons who allege to have been subject to the investigatory powers of RIPA. It has jurisdiction to investigate any complaint that a person's communications have been intercepted and, where interception has occurred, to examine the authority for such interception. Sections 67(2) and 67(3)(c) provide that the IPT is to apply the principles applicable by a court on an application for judicial review.

Under section 67(8) RIPA, there is no appeal from a decision of the IPT "except to such extent as the Secretary of State may by order otherwise provide". No order has been passed by the Secretary of State.

Section 68(2) provides that the IPT has the power to require a relevant Commissioner to provide it with all such assistance as it thinks fit. Section 68(6) and (7) requires those involved in the authorisation and execution of an interception warrant to disclose or provide to the IPT all documents and information it may require.

Section 68(4) deals with reasons for the IPT's decisions and provides that where the tribunal determines any complaint brought before it, it will give notice to the complainant which will be confined, as the case may be, to either a statement that they have made a determination in his favour; or a statement that no determination has been made in his favour.

The IPT has the power to award compensation and to make such other orders as it thinks fit, including orders quashing or cancelling any section 8(1) warrant and orders requiring the destruction of any records obtained under a section 8(1) warrant (section 67(7) RIPA). In the event that a claim before the IPT is successful, the IPT is generally required to make a report to the Prime Minister (section 68(5)).

Section 68(1) provides that the tribunal is entitled to determine its own procedure. Section 69(1) provides that the Secretary of State may also make procedural rules. Under section 69(2) such rules may, *inter alia*, prescribe the form and manner in which proceedings are to be brought before the

tribunal; prescribe the forms of hearing or consideration to be adopted by the tribunal in relation to particular proceedings; prescribe the practice and procedure to be followed in the hearing; and require information about any decision made by the tribunal in relation to any proceedings to be provided to the person who brought the proceedings. Pursuant to section 69(6), in making the rules the Secretary of State must have regard to the need to ensure that matters are properly heard and considered by the tribunal and the need to ensure that information is not disclosed contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of the United Kingdom or the continued discharge of the functions of any of the intelligence services.

The Secretary of State has adopted rules to govern the procedure before the IPT in the form of the Investigatory Powers Tribunal Rules 2000 ("the Rules"). The Rules cover various aspects of the procedure before the IPT.

As regards disclosure of information, Rule 6 provides that the tribunal will carry out its functions in such a way as to secure that information is not disclosed contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, the economic well-being of the United Kingdom or the continued discharge of the functions of any of the intelligence services. In principle, the tribunal is not permitted to disclose: the fact that it has held an oral hearing under rule 9(4); any information disclosed to the tribunal in the course of that hearing or the identity of any witness at that hearing; any information otherwise disclosed to the tribunal by any person involved in the authorisation or execution of interception warrants; or any information provided by a Commissioner; the fact that any information has been disclosed or provided. However, the tribunal may disclose such information with the consent of the person required to attend the hearing, the person who disclosed the information, the Commissioner or the person whose consent was required for disclosure of the information, as the case may be. The tribunal may also disclose such information as part of the information provided to the complainant under rule 13(2), subject to the restrictions contained in rule 13(4) and (5).

Rule 9 deals with the forms of hearings and consideration of the complaint. It provides that the tribunal shall be under no duty to hold oral hearings, but may do so in accordance with Rule 9 (and not otherwise). The tribunal may hold, at any stage of their consideration, oral hearings at which the complainant may make representations, give evidence and call witnesses. It may also hold separate oral hearings which the person whose conduct is the subject of the complaint, the public authority against which the proceedings are brought, or any other person involved in the authorisation or execution of an interception warrant may be required to attend. Rule 9 also provides that the tribunal's proceedings, including any oral hearings, are to be conducted in private.

The taking of evidence is addressed in Rule 11. It allows the tribunal to receive evidence in any form, even where it would not be admissible in a court of law. It may require a witness to give evidence on oath, but no person can be compelled to give evidence at an oral hearing under Rule 9(3).

Finally, Rule 13 provides guidance on notification to the complainant of the IPT's findings:

"(1) In addition to any statement under section 68(4) of the Act, the Tribunal shall provide information to the complainant in accordance with this rule.

(2) Where they make a determination in favour of the complainant, the Tribunal shall provide him with a summary of that determination including any findings of fact.

...

(4) The duty to provide information under this rule is in all cases subject to the general duty imposed on the Tribunal by rule 6(1).

(5) No information may be provided under this rule whose disclosure would be restricted under rule 6(2) unless the person whose consent would be needed for disclosure under that rule has been given the opportunity to make representations to the Tribunal."

In its joint ruling on preliminary issues of law in a case involving a complaint by British-Irish Rights Watch, the IPT clarified a number of aspects of its procedure. The IPT sat, for the first time, in public. As regards its procedures and the importance of the cases before it, it noted:

"10. The challenge to rule 9(6) [requiring oral hearings to be held in private] and to most of the other rules governing the basic procedures of the Tribunal have made this the most significant case ever to come before the Tribunal. The Tribunal are left in no doubt that their rulings on the legal issues formulated by the parties have potentially important consequences for dealing with and determining these and future proceedings and complaints. Counsel and those instructing them were encouraged to argue all the issues in detail, in writing as well as at the oral hearings held over a period of three days in July and August 2002. At the end of September 2002 the written submissions were completed when the parties provided, at the request of the Tribunal, final comments on how the Rules ought, if permissible and appropriate, to be revised and applied by the Tribunal, in the event of a ruling that one or more of the Rules are incompatible with Convention rights and/or ultra vires."

The IPT concluded that the hearing of the preliminary issues in the case should have been conducted in public, that the reasons for the legal rulings should be made public and that in all other respects the Rules were valid and binding on the tribunal and compatible with Articles 6, 8 and 10 of the Convention.

Specifically on the applicability of Article 6 § 1 to the proceedings before it, the IPT found:

"85. The conclusion of the Tribunal is that Article 6 applies to a person's claims under section 65(2)(a) and to his complaints under section 65(2)(b) of RIPA, as each of them involves 'the determination of his civil rights' by the Tribunal within the meaning of Article 6(1)."

As to the proper construction of Rule 9 regarding oral hearings, the IPT considered that the rule made clear that oral hearings could be held at the its discretion. If a hearing was held, it had to be held in accordance with Rule 9. The absence from the Rules of an absolute right to either an *inter partes* oral hearing, or, failing that, to a separate oral hearing in every case was within the rule-making power in section 69(1) RIPA and was compatible with the Convention rights under Article 6, 8 and 10. The tribunal explained that oral hearings involving evidence or a consideration of the substantive merits of a claim or complaint ran the risk of breaching the "neither confirm nor deny" policy or other aspects of national security and the public interest. It was necessary to provide safeguards against that and the conferring of a discretion to decide when there should be oral

hearings and what form they should take was a proportionate response to the need for safeguards.

Regarding Rule 9(6) which stipulates that oral hearings must be held in private, the IPT found the language to be clear and unqualified. The tribunal had no discretion in the matter. It concluded that the very fact that the rule was of an absolute blanket nature was fatal to its validity and concluded that the very width of the rule, preventing any hearing of the proceedings in public, went beyond what was authorised by section 69 of RIPA. In consequence, it found Rule 9(6) to be *ultra vires* section 69 and not binding on the tribunal.

Regarding other departures from the normal rules of adversarial procedure as regards the taking of evidence and disclosure in Rule 6, the IPT concluded that these departures from the adversarial model were within the power conferred on the Secretary of State and compatible with Convention rights in Articles 8 and 10, taking account of the exceptions for the public interest and national security in Articles 8(2) and 10(2), in particular the effective operation of the legitimate policy of "neither confirm nor deny" in relation to the use of investigatory powers. It noted that disclosure of information was not an absolute right where there were competing interests, such as national security considerations.

Finally, as regards the absence of reasons following a decision that the complaint is unsuccessful, the IPT concluded that section 68(4) and rule 13 were valid and binding and that the distinction between information given to the successful complainants and that given to unsuccessful complainants (where the "neither confirm nor deny" policy had to be preserved) was necessary and justifiable.

COMPLAINTS

The applicants argue that the legal framework governing the interception of communications content and data is incompatible with Articles 8 and 10 of the Convention. They allege in particular that they are very likely to have been the subjects of surveillance by the United Kingdom intelligence services, which may have been in receipt of foreign intercept material relating to their electronic communications. In their view, such surveillance amounts to an interference with their rights under Articles 8 and 10 of the Convention which is not "in accordance with the law". In relation to the receipt of foreign intercept material obtained under Prism and Upstream, the applicants contend that the applicable legal framework is excessively broad and gives inadequate indication as to the relevant arrangements in place to ensure lawful processing of data by the intelligence services. As regards interception of communications by GCHQ under the Tempora programme, the applicants submit that the legal framework does not provide the minimum statutory safeguards outlined by the Court in case-law, notably *Weber and Saravia*, cited above, §§ 92-95. In particular, the applicants contend that the safeguards set out in sections 15 and 16 RIPA are inadequate and ineffective. They further contend that the interference which results from the Tempora programme is not "necessary in a democratic

society" as communications are intercepted and retained without any reasonable suspicion and there is no judicial oversight or authorisation for interception.

The applicants also complain under Article 6 that the proceedings before the IPT violated their right to a fair hearing. They contend that the IPT wrongly held closed hearings, failed to ensure that they were effectively represented in these hearings and failed to order the disclosure of documents. They also allege that the IPT failed to hear preliminary arguments on whether the Government's "neither confirm nor deny" policy was justified. Further, they complain that the IPT placed significant reliance on secret arrangements "below the waterline" which were not disclosed to them.

Finally, the applicants contend, relying on Article 14, taken together with Articles 8 and 10, that the section 8(4) RIPA framework is indirectly discriminatory on grounds of nationality and national origin since section 16 RIPA grants additional safeguards to people known to be in the British Islands but denies them to those abroad. The majority of the applicants are based outside the British Islands and complain they are disproportionately likely to have their private communications intercepted and accessed.

QUESTIONS TO THE PARTIES

1. Can the applicants claim to be "victims", within the meaning of Article 34 of the Convention, of violations of their rights under Articles 8 and 10?

2. Are the acts of the United Kingdom intelligence services in relation to:

(a) the soliciting, receipt, search, analysis, dissemination, storage and destruction of interception data in respect of "external communications", in particular with regard to their impact on non-governmental organisations and their confidential information and communications;

(b) the soliciting, receipt, search, analysis, dissemination, storage and destruction of interception data by the United Kingdom in respect of "communications data", in particular with regard to their impact on non-governmental organisations and their confidential information and communications;

"in accordance with the law" and "necessary in a democratic society" within the meaning of Article 8 of the Convention, with reference to the principles set out in, among other authorities, *Weber and Saravia v. Germany* (dec.), no. 54934/00, ECHR 2006-XI; *Liberty and Others v. the United Kingdom*, no. 58243/00, 1 July 2008; and *Iordachi and Others v. Moldova*, no. 25198/02, 10 February 2009?

3. Are the acts of the United Kingdom intelligence services in relation to:

(a) the soliciting, receipt, search, analysis, dissemination, storage and destruction of interception data in respect of "external communications", in particular with regard to their impact on non-governmental organisations and their confidential information and communications;

(b) the soliciting, receipt, search, analysis, dissemination, storage and destruction of interception data by the United Kingdom in respect of "communications data", in particular with regard to their impact on non-governmental organisations and their confidential information and communications;

"prescribed by law", and "necessary in a democratic society" in the pursuit of a legitimate aim, within the meaning of Article 10 of the Convention reference to the principles set out in, among other authorities, *Nordisk Film & TV A/S v Denmark*, no. 40485/02, 8 December 2005; *Financial Times Ltd and Others v the United Kingdom*, no 821/03, 15 December 2009; *Telegraaf Media Nederland Landelijke Media B.V. and*

Others v the Netherlands, no. 39315/06, 22 November 2012; and *Nagla v. Latvia*, no. 73469/10, 16 July 2013?

4. Did the proceedings before the Investigatory Powers Tribunal involve the determination of "civil rights and obligations" within the meaning of Article 6 § 1 (*Klass and Others v. Germany,* 6 September 1978, § 75, Series A no.28)?

5. If so, were the restrictions in the IPT proceedings, taken as a whole, disproportionate or did they impair the very essence of the applicants' right to a fair trial (see *Kennedy v. the United Kingdom*, no. 26839/05, § 186, 18 May 2010)?

6. Has there been a violation of Article 14, taken together with Article 8 and/or Article 10, on account of the fact that the safeguards set out in section 16 of the Regulation of Investigatory Powers Act 2000 grants additional safeguards to people known to be in the British Islands?

APPENDIX

1. Amnesty International Limited ("Amnesty International") is an international human rights organisation based in London. It is represented before the Court by Mr N. Williams, its legal counsel.
2. Bytes for All ("B4A") is a human rights organisation based in Islamabad, Pakistan. It is represented before the Court by Mr M. Scott of Bhatt Murphy Solicitors, a firm of solicitors based in London.
3. The National Council for Civil Liberties ("Liberty") is a human rights organisation based in London. It is represented before the Court by Mr J. Welsh, its legal director.
4. Privacy International charity which focuses on the right to privacy at an international level and is based in London. It is represented before the Court by Mr M. Scott of Bhatt Murphy Solicitors, a firm of solicitors based in London.
5. The American Civil Liberties Union ("ACLU") is a human rights organisation with headquarters in New York. It is represented before the Court by Mr J. Welsh, legal director of Liberty.
6. The Canadian Civil Liberties Association ("CCLA") is a human rights organisation based in Toronto. It is represented before the Court by Mr J. Welsh, legal director of Liberty.
7. The Egyptian Initiative for Personal Rights ("EIPR") is a human rights organisation based in Cairo. It is represented before the Court by Mr J. Welsh, legal director of Liberty.
8. The Hungarian Civil Liberties Union ("HCLU"), also known as *Társaság a Szabadságjogokért* ("TASZ"), is a human rights organisation based in Budapest. It is represented before the Court by Mr J. Welsh, legal director of Liberty.
9. The Irish Council for Civil Liberties ("ICCL") also known as *An Chomhairle um Chearta Daonna*, is a human rights organisation based in Dublin. It is represented before the Court by Mr J. Welsh, legal director of Liberty.
10. The Legal Resources Centre ("LRC") is a human rights organisation based in Johannesburg, South Africa. It is represented before the Court by Mr J. Welsh, legal director of Liberty.