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

Communicated on 9 January 2014

FOURTH SECTION

Application no. 58170/13
BIG BROTHER WATCH and others
against the United Kingdom
lodged on 4 September 2013

STATEMENT OF FACTS

A. The circumstances of the case

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

1. The applicants

Big Brother Watch (the first applicant) is a limited company based in London which operates as a campaign group to conduct research into, and challenge policies which threaten privacy, freedoms and civil liberties, and to expose the scale of surveillance by the State. Its staff members regularly liaise and work in partnership with similar organisations in other countries, communicating by email and Skype. As a vocal critic of excessive surveillance, and a commentator on sensitive topics relating to national security, the first applicant believes that its staff and directors may have been the subject of surveillance by or on behalf of the United Kingdom Government. Moreover, it has contact with internet freedom campaigners and those who wish to complain to regulators around the world, so it is conscious that some of those with whom it is in contact may also fall under surveillance.

English PEN (the second applicant) is a registered charity, based in London but with 145 affiliated centres in over 100 countries. It promotes freedom to write and read, and campaigns around the world on freedom of expression, and equal access to the media and works closely with individual writers at risk and in prison. Most of its internal and external communications are by email and by Skype. Since many of those for and whom with English PEN campaigns express views on governments which may be controversial, English PEN believes that it, and those with whom it

communicates, may be the subject of United Kingdom Government surveillance, or may be the subject of surveillance by other countries' security services which may pass such information to the United Kingdom security services (and vice-versa).

Open Rights Group (the third applicant) is a limited company, based in London, which operates as a campaign organisation, defending freedom of expression, innovation, creativity and consumer rights on the internet. It regularly liaises and works in partnership with other organisations in other countries. It is a member organisation of European Digital Rights, a network of 35 privacy and civil rights organisations founded in June 2002, with offices in 21 different countries in Europe. Most of its internal and external communications are by email and Skype. For similar reasons to those expressed by the first and second applicants, it believes that its electronic communications and activities may be subject to foreign intercept conveyed to United Kingdom authorities, or intercept activity by United Kingdom authorities.

Dr Constanze Kurz (the fourth applicant) is an expert on surveillance techniques, based in Berlin, where she works at the University of Applied Sciences. From 2010 to 2013, she was a member of the Internet and Digital Society Commission of Inquiry of the German Bundestag. She is also spokeswoman of the German "Computer Chaos Club" (CCC), which campaigns to highlight weaknesses in computer networks which risk endangering the interests of the public, occasionally through direct action. Dr Kurz has been outspoken in relation to the recent disclosures regarding United Kingdom internet surveillance activities, which continue to be a subject of significant concern in the German media. She fears that she may well have been the subject of surveillance either directly by the United Kingdom or by foreign security services who may have passed that data to the United Kingdom security services, not only because of her activities as a freedom of expression campaigner and hacking activist, but also because these security services may wish to learn from her and persons with whom she communicates, habitually in encrypted communications.

2. The surveillance programmes complained about

The applicants concern was triggered by media coverage following the leak of information by Edward Snowden, a former systems administrator with the United States National Security Agency (NSA). According to media reports, the NSA has in place a programme, known as PRISM, which allows it to access a wide range of internet communication content (such as emails, chat, video, images, documents, links and other files) and metadata (information permitting the identification and location of internet users), from United States corporations, including some of the largest internet service providers such as Microsoft, Google, Yahoo, Apple, Facebook, YouTube and Skype. Since global internet data takes the cheapest, rather than the most direct route, a substantial amount of global data passes through the servers of these American companies, including possibly emails sent by the applicants in London and Berlin to their international contacts. The applicants submit that the NSA also operates a second interception programme known as UPSTREAM, which provides access to nearly all the traffic passing through fibre optic cables owned by United States

communication service providers such as AT&T and Verizon. Together, these programmes provide very broad access to the communications content and metadata of non-United States persons, to whom the provisions of the Fourth Amendment (the United States Constitutional privacy guarantee), and allow for this material to be collected, stored and searched using keywords. According to the documents leaked by Edward Snowden, the United Kingdom Government Communications Head Quarters (GCHQ) has had access to PRISM material since at least June 2010 and has used it to generate intelligence reports (197 reports in 2012).

In addition, the disclosures based on Edward Snowden's leaked documentation have included details about a United Kingdom surveillance programme called TEMPORA. According to the applicants, TEMPORA is a means by which GCHQ can access electronic traffic passing along fibre-optic cables running between the United Kingdom and North America. The data collected include both internet and telephone communications. GCHQ is able to access not only metadata but also the content of emails, Facebook entries and website histories. The TEMPORA programme is authorised by certificates issued under section 8(4) of the Regulation of Investigatory Powers Act 2000 (RIPA: see below). The applicants allege that United States agencies have been given extensive access to TEMPORA information.

B. Relevant domestic law

Section 1 of the Intelligence Services Act 1994 ("ISA") (see Annex 4) provides a statutory basis for the operation of the United Kingdom's Secret Intelligence Service:

> "**1. The Secret Intelligence Service**.
>
> (1) There shall continue to be a Secret Intelligence Service (in this Act referred to as 'the Intelligence Service') under the authority of the Secretary of State; and, subject to subsection (2) below, its functions shall be –
>
> (a) to obtain and provide information relating to the actions or intentions of persons outside the British Islands; and
>
> (b) to perform other tasks relating to the actions or intentions of such persons.
>
> (2) The functions of the Intelligence Service shall be exercisable only –
>
> (a) in the interests of national security, with particular reference to the defence and foreign policies of Her Majesty's Government in the United Kingdom; or
>
> (b) in the interests of the economic well-being of the United Kingdom; or
>
> (c) in support of the prevention or detection of serious crime."

Section 2 of ISA provides for the control of the operations of the Intelligence Service by a Chief of Service, to be appointed by the Secretary of State. Under section 2(2)(a), the Chief's duties include ensuring:

> "that there are arrangements for securing that no information is obtained by the Intelligence Service except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary –
>
> (i) for that purpose;
>
> (ii) in the interests of national security;

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

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

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

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

(1) the shall continue to be a Government Communications Headquarters under the authority of the Secretary of State; and, subject to subsection (2) below, its functions shall be –

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

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

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

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

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

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, she must also issue a certificate setting out a description of the intercepted material which she 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:

"**15. General safeguards**

(1) Subject to subsection (6), it shall be 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 –

(a) that the requirements of subsections (2) and (3) are satisfied in relation to the intercepted material and any related communications data; and

(b) in the case of warrants in relation to which there are section 8(4) certificates, that the requirements of section 16 are also satisfied.

(2) 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.

(3) 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.

(4) For the purposes of this section something is necessary for the authorised purposes if, and only if –

(a) it continues to be, or is likely to become, necessary as mentioned in section 5(3);

(b) it is necessary for facilitating the carrying out of any of the functions under this Chapter of the Secretary of State;

(c) it is necessary for facilitating the carrying out of any functions in relation to this Part of the Interception of Communications Commissioner or of the Tribunal;

(d) 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

(e) it is necessary for the performance of any duty imposed on any person by the Public Records Act 1958 or the Public Records Act (Northern Ireland) 1923.

(5) The arrangements for the time being in force under this section for securing that the requirements of subsection (2) are satisfied in relation to the intercepted material or any related communications data must 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.

(6) Arrangements in relation to interception warrants which are made for the purposes of subsection (1) –

(a) shall not be required to secure that the requirements of subsections (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; but

(b) shall be 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 subsection (7) are satisfied.

(7) 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.

(8) In this section 'copy', in relation to intercepted material or related communications data, means any of the following (whether or not in documentary form) –

(a) any copy, extract or summary of the material or data which identifies itself as the product of an interception, and

(b) any record referring to an interception which is a record of the identities of the persons to or by whom the intercepted material was sent, or to whom the communications data relates,

and 'copied' shall be construed accordingly."

Section 16 sets out additional safeguards in relation to interception of "external" communications under certificated warrants:

"**16. Extra safeguards in the case of certificated warrants**.

(1) For the purposes of section 15 the requirements of this section, in the case of a warrant in relation to which there is a section 8(4) certificate, 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 –

(a) has been certified as material the examination of which is necessary as mentioned in section 5(3)(a), (b) or (c); and

(b) falls within subsection (2).

(2) 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.

(3) Intercepted material falls within subsection (2), notwithstanding that it is selected by reference to any such factor as is mentioned in paragraph (a) and (b) of that subsection, if –

(a) 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); and

(b) the material relates only to communications sent during a period specified in the certificate that is no longer than the permitted maximum.

(3A) In subsection (3)(b) 'the permitted maximum' 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, six months; and

(b) in any other case, three months.

F2(4) Intercepted material also falls within subsection (2), notwithstanding that it is selected by reference to any such factor as is mentioned in paragraph (a) and (b) of that subsection, if –

(a) 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

(b) the conditions set out in subsection (5) below are satisfied in relation to the selection of the material.

(5) 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.

(5A) In subsection (5)(c) '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.

(6)References in this section to its appearing that there has been a relevant change of circumstances are references to its appearing either –

(a) that the individual in question has entered the British Islands; or

(b) 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 provides for a Tribunal, 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. One such Code issued under section 71 of RIPA, the "Acquisition and Disclosure of Communications Data: Code of Practice", 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."

COMPLAINTS

The applicants allege that they are likely to have been the subject of generic surveillance by GCHQ and/or that the United Kingdom security services may have been in receipt of foreign intercept material relating to their electronic communications, such as to give rise to interferences with their rights under Article 8 of the Convention. They contend that these interferences are not "in accordance with the law", for the following reasons.

In the applicants' submission, there is no basis in domestic law for the receipt of information from foreign intelligence agencies. In addition, there is an absence of legislative control and safeguards in relation to the circumstances in which the United Kingdom intelligence services can request foreign intelligence agencies to intercept communications and/or to give the United Kingdom access to stored data that has been obtained by interception, and the extent to which the United Kingdom intelligence services can use, analyse, disseminate and store data solicited and/or received from foreign intelligence agencies and the process by which such data must be destroyed.

In relation to the interception of communications directly by GCHQ, the applicants submit that the statutory regime applying to external communications warrants does not comply with the minimum standards outlined by the Court in its case-law, in particular *Weber and Saravia v. Germany* (dec.), no. 54934/00, §§ 92-95, ECHR 2006-XI. They contend that section 8(4) of RIPA permits the blanket strategic monitoring of communications where at least one party is outside the British Isles, under broadly defined warrants, which are continuously renewed so as to form a "rolling programme". Although the Secretary of State is required to issue a

certificate limiting the extent to which the intercepted material can be examined, the legislation also permits such certificates to be framed in very broad terms, for example, "in the interests of national security". The applicants claim, in particular, that the concept of "national security" in this context is vague and unforeseeable in scope. They consider that the safeguards set out in sections 15 and 16 of RIPA are of limited scope, particularly in the light of the broad definition of national security employed. They further contend that domestic law does not provide for effective independent authorisation and oversight.

The applicants further contend that the generic interception of external communications by GCHQ, merely on the basis that such communications have been transmitted by transatlantic fibre-optic cables, is an inherently disproportionate interference with the private lives of thousands, perhaps millions, of people.

QUESTIONS TO THE PARTIES

1. Can the applicants claim to be victims of violations of their rights under Article 8?

2. Have the applicants done all that is required of them to exhaust domestic remedies? In particular, (a) had the applicants raised their Convention complaints before the Investigatory Powers Tribunal, could the Tribunal have made a declaration of incompatibility under section 4 of the Human Rights Act 1998; and, if so, (b) has the practice of giving effect to the national courts' declarations of incompatibility by amendment of legislation become sufficiently certain that the remedy under Section 4 of the Human Rights Act 1998 should be regarded by the Court as an effective remedy which should be exhausted before bringing a complaint of this type before the Court (see *Burden v. the United Kingdom* [GC], no. 13378/05, §§ 43-44, ECHR 2008)?

3. In the event that the application is not inadmissible on grounds of non-exhaustion of domestic remedies, 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 obtained by the intelligence services of other States; and/or

(b) their own interception, search, analysis, dissemination, storage and destruction of data relating to "external" communications (where at least one party is outside the British Isles);

"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 *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?