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

Press Release
issued by the Registrar of the Court

ECHR 299 (2018)
13.09.2018

Some aspects of UK surveillance regimes violate Convention

The case of Big Brother Watch and Others v. the United Kingdom (applications nos. 58170/13, 62322/14 and 24960/15) concerned complaints by journalists and rights organisations about three different surveillance regimes: (1) the bulk interception of communications; (2) intelligence sharing with foreign governments; and (3) the obtaining of communications data from communications service providers.

Both the bulk interception regime and the regime for obtaining communications data from communications service providers have a statutory basis in the Regulation of Investigatory Powers Act 2000. The Investigatory Powers Act 2016, when it comes fully into force, will make significant changes to both regimes. In considering the applicants' complaints, the Court had regard to the law in force at the date of its examination. As the provisions of the IPA which will amend the regimes for the bulk interception of communications and the obtaining of communications data from communications service providers were not in force at that time, the Court did not consider them in its assessment.

In today's **Chamber** judgment[1] the European Court of Human Rights held, **by five votes to two**, that:

the bulk interception regime **violated Article 8 of the European Convention on Human Rights (right to respect for private and family life/communications)** as there was insufficient oversight both of the selection of Internet bearers for interception and the filtering, search and selection of intercepted communications for examination, and the safeguards governing the selection of "related communications data" for examination were inadequate.

In reaching this conclusion, the Court found that the operation of a bulk interception regime did not in and of itself violate the Convention, but noted that such a regime had to respect criteria set down in its case-law.

The Court also held, **by six votes to one**, that:

the regime for obtaining communications data from communications service providers **violated Article 8** as it was not in accordance with the law; and

that both the bulk interception regime and the regime for obtaining communications data from communications service providers **violated Article 10 of the Convention** as there were insufficient safeguards in respect of confidential journalistic material.

It further found that the regime for sharing intelligence with foreign governments **did not violate either Article 8 or Article 10.**

The Court **unanimously** rejected complaints made by the third set of applicants under **Article 6 (right to a fair trial),** about the domestic procedure for challenging secret surveillance measures, and under **Article 14 (prohibition of discrimination).**

For an FAQ on the judgment please click here.

1. Under Articles 43 and 44 of the Convention, this Chamber judgment is not final. During the three-month period following its delivery, any party may request that the case be referred to the Grand Chamber of the Court. If such a request is made, a panel of five judges considers whether the case deserves further examination. In that event, the Grand Chamber will hear the case and deliver a final judgment. If the referral request is refused, the Chamber judgment will become final on that day.
Once a judgment becomes final, it is transmitted to the Committee of Ministers of the Council of Europe for supervision of its execution. Further information about the execution process can be found here: www.coe.int/t/dghl/monitoring/execution.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Principal facts

The three joined applications are *Big Brother Watch and Others v. the United Kingdom* (no. 58170/13); *Bureau of Investigative Journalism and Alice Ross v. the United Kingdom* (no. 62322/14); and *10 Human Rights Organisations and Others v. the United Kingdom* (no. 24960/15). The 16 applicants are organisations and individuals who are either journalists or are active in campaigning on civil liberties issues.

The applications were lodged after Edward Snowden, a former US National Security Agency (NSA) contractor, revealed the existence of surveillance and intelligence sharing programmes operated by the intelligence services of the United States and the United Kingdom.

The applicants believed that the nature of their activities meant that their electronic communications and/or communications data were likely to have been intercepted or obtained by the UK intelligence services.

Complaints, procedure and composition of the Court

Relying on Article 8 (right to respect for private and family life and correspondence), the applicants complained about the regimes for the bulk interception of communications, intelligence sharing and for the acquisition of data from communications service providers.

The second and third applications also raised complaints under Article 10 (freedom of expression) related to their work, respectively, as journalists and non-governmental organisations.

The third application relied in addition on Article 6 (right to a fair trial), in relation to the domestic procedure for challenging surveillance measures, and on Article 14 (prohibition of discrimination), combined with Articles 8 and 10, alleging the regime for the bulk interception of communications discriminated against people outside the United Kingdom, whose communications were more likely to be intercepted and, if intercepted, selected for examination.

The applications were lodged on 4 September 2013, 11 September 2014 and 20 May 2015 respectively. They were communicated to the Government on 9 January 2014, 5 January 2015 and 24 November 2015, together with questions from the Court. Various third parties were allowed to intervene in the proceedings and a public hearing was held in November 2017.

Judgment was given by a Chamber of seven judges, composed as follows:

Linos-Alexandre **Sicilianos** (Greece), *President*,
Kristina **Pardalos** (San Marino),
Aleš **Pejchal** (the Czech Republic),
Ksenija **Turković** (Croatia),
Armen **Harutyunyan** (Armenia),
Pauliine **Koskelo** (Finland),
Tim **Eicke** (the United Kingdom),

and also Abel **Campos**, *Section Registrar.*

Decision of the Court

Admissibility

The Court first considered whether the first and second set of applicants had exhausted domestic remedies, part of the process of admissibility, as they had not raised their complaints with the Investigatory Powers Tribunal, a special body charged with examining allegations of wrongful interference with communications by the security services.

It found that while the IPT has shown itself to be an effective remedy which applicants had to use, at the time these two sets of applicants lodged their applications with this Court there existed special circumstances absolving them from that requirement and they could not be faulted for relying on the Court's 2010 judgment in *Kennedy v. the United Kingdom* as authority for the proposition that the IPT was not an effective remedy for a complaint about the general Convention compliance of a surveillance regime.

Article 8

Interception process under section 8(4) of RIPA

The Court noted that the bulk interception of communications was regulated by section 8(4) of the Regulation of Investigatory Powers Act (RIPA) 2000.

Operating a bulk interception scheme was not *per se* in violation of the Convention and Governments had wide discretion ("a wide margin of appreciation") in deciding what kind of surveillance scheme was necessary to protect national security. However, the operation of such systems had to meet six basic requirements, as set out in *Weber and Saravia v. Germany*. The Court rejected a request by the applicants to update the *Weber* requirements, which they had said was necessary owing to advances in technology.

The Court then noted that there were four stages of an operation under section 8(4): the interception of communications being transmitted across selected Internet bearers; the using of selectors to filter and discard – in near real time – those intercepted communications that had little or no intelligence value; the application of searches to the remaining intercepted communications; and the examination of some or all of the retained material by an analyst.

While the Court was satisfied that the intelligence services of the United Kingdom take their Convention obligations seriously and are not abusing their powers, it found that there was inadequate independent oversight of the selection and search processes involved in the operation, in particular when it came to selecting the Internet bearers for interception and choosing the selectors and search criteria used to filter and select intercepted communications for examination. Furthermore, there were no real safeguards applicable to the selection of related communications data for examination, even though this data could reveal a great deal about a person's habits and contacts.

Such failings meant section 8(4) did not meet the "quality of law" requirement of the Convention and could not keep any interference to that which was "necessary in a democratic society". There had therefore been a violation of Article 8 of the Convention.

Acquisition of data from communications service providers under Chapter II of RIPA

The Court noted that the second set of applicants had complained that Chapter II of RIPA allowed a wide range of public bodies to request access to communications data from communications companies in various ill-defined circumstances.

It first rejected a Government argument that the applicants' application was inadmissible, finding that as investigative journalists their communications could have been targeted by the procedures in question. It then went on to focus on the Convention concept that any interference with rights had to be "in accordance with the law".

It noted that European Union law required that any regime allowing access to data held by communications service providers had to be limited to the purpose of combating "serious crime", and that access be subject to prior review by a court or independent administrative body. As the EU legal order is integrated into that of the UK and has primacy where there is a conflict with domestic law, the Government had conceded in a recent domestic case that a very similar scheme introduced by the Investigatory Powers Act 2016 was incompatible with fundamental rights in EU law because it

did not include these safeguards. Following this concession, the High Court ordered the Government to amend the relevant provisions of the Act. The Court therefore found that as the Chapter II regime also lacked these safeguards, it was not in accordance with domestic law as interpreted by the domestic authorities in light of EU law. As such, there had been a violation of Article 8.

Intelligence sharing procedures

The Court found that the procedure for requesting either the interception or the conveyance of intercept material from foreign intelligence agencies was set out with sufficient clarity in the domestic law and relevant code of practice. In particular, material from foreign agencies could only be searched if all the requirements for searching material obtained by the UK security services were fulfilled. The Court further observed that there was no evidence of any significant shortcomings in the application and operation of the regime, or indeed evidence of any abuse.

The intelligence sharing regime therefore did not violate Article 8.

Article 10

The Court declared complaints by the third set of applicants under this provision to be inadmissible but found a violation of the rights of the second set of applicants, who had complained that the bulk surveillance regimes under section 8(4) and Chapter II of RIPA did not provide sufficient protection for journalistic sources or confidential journalistic material.

In respect of the bulk interception regime, the Court expressed particular concern about the absence of any published safeguards relating both to the circumstances in which confidential journalistic material could be selected intentionally for examination, and to the protection of confidentiality where it had been selected, either intentionally or otherwise, for examination. In view of the potential chilling effect that any perceived interference with the confidentiality of journalists' communications and, in particular, their sources might have on the freedom of the press, the Court found that the bulk interception regime was also in violation of Article 10.

When it came to requests for data from communications service providers under Chapter II, the Court noted that the relevant safeguards only applied when the purpose of such a request was to uncover the identity of a journalist's source. They did not apply in every case where there was a request for a journalist's communications data, or where collateral intrusion was likely. In addition, there were no special provisions restricting access to the purpose of combating "serious crime". As a consequence, the Court also found a violation of Article 10 in respect of the Chapter II regime.

Article 6

The third set of applicants complained that the IPT lacked independence and impartiality. However, the Court noted that the IPT had extensive power to consider complaints concerning wrongful interference with communications, and those extensive powers had been employed in the applicants' case to ensure the fairness of the proceedings. Most notably, the IPT had access to open and closed material and it had appointed Counsel to the Tribunal to make submissions on behalf of the applicants in the closed proceedings. Furthermore, the Court accepted that in order to ensure the efficacy of the secret surveillance regime, which was an important tool in the fight against terrorism and serious crime, the restrictions on the applicants' procedural rights had been both necessary and proportionate and had not impaired the essence of their Article 6 rights.

Overall, the applicants' complaint was manifestly ill-founded and had to be rejected.

Other Articles

The third set of applicants complained under Article 14, in conjunction with Articles 8 and 10, that those outside the United Kingdom were disproportionately likely to have their communications intercepted as the law only provided additional safeguards to people known to be in Britain.

The Court rejected this complaint as manifestly ill-founded. The applicants had not substantiated their argument that people outside the UK were more likely to have their communications intercepted. In addition, any possible difference in treatment was not due to nationality but to geographic location, and was justified.

Just satisfaction (Article 41)

The applicants did not claim any award in respect of pecuniary or non-pecuniary damage and the Court saw no reason to make one. However, it made partial awards in respect of the costs and expenses claimed by the applicants in the first and second of the joined cases. The applicants in the third joined case made no claim for costs and expenses.

Separate opinions

Judges Pardalos and Eicke expressed a joint partly dissenting and partly concurring opinion, and Judge Koskelo, joined by Judge Turković, expressed a partly concurring, partly dissenting opinion. These opinions are annexed to the judgment.

The judgment is available only in English.

Press contacts
echrpress@echr.coe.int | tel.: +33 3 90 21 42 08

Patrick Lannin (tel: + 33 3 90 21 44 18)
Tracey Turner-Tretz (tel: + 33 3 88 41 35 30)
Denis Lambert (tel: + 33 3 90 21 41 09)
Inci Ertekin (tel: + 33 3 90 21 55 30)
Somi Nikol (tel: + 33 3 90 21 64 25)