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

Press Release
issued by the Registrar of the Court

ECHR 165 (2021)
25:05/2021

UK surveillance regime: some aspects contrary to the Convention

In today's **Grand Chamber** judgment[1] in the case of Big Brother Watch and Others v. the United Kingdom (application nos. 58170/13, 62322/14 and 24969/15) the European Court of Human Rights held:

unanimously, that there had been a **violation of Article 8 of the European Convention (right to respect for private and family life/communications)** in respect of the bulk intercept regime;

unanimously that there had been a **violation of Article 8** in respect of the regime for obtaining communications data from communication service providers;

by 12 votes to 5, that there had been **no violation of Article 8** in respect of the United Kingdom's regime for requesting intercepted material from foreign Governments and intelligence agencies;

unanimously, that there had been **a violation of Article 10 (freedom of expression)**, concerning both the bulk interception regime and the regime for obtaining communications data from communication service providers; and

by 12 votes to 5, that there had been **no violation of Article 10** in respect of the regime for requesting intercepted material from foreign Governments and intelligence agencies.

The case concerned complaints by journalists and human-rights organisations in regard to three different surveillance regimes: (1) the bulk interception of communications; (2) the receipt of intercept material from foreign governments and intelligence agencies; (3) the obtaining of communications data from communication service providers.

At the relevant time, the regime for bulk interception and obtaining communications data from communication service providers had a statutory basis in the Regulation of Investigatory Powers Act 2000. This has since been replaced by the Investigatory Powers Act 2016. The findings of the Grand Chamber relate solely to the provisions of the 2000 Act, which had been the legal framework in force at the time the events complained of had taken place.

The Court considered that, owing to the multitude of threats States face in modern society, operating a bulk interception regime did not in and of itself violate the Convention. However, such a regime had to be subject to "end-to-end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation were being defined; and that the operation should be subject to supervision and independent *ex post facto* review.

Having regard to the bulk interception regime operated in the UK, the Court identified the following deficiencies: bulk interception had been authorised by the Secretary of State, and not by a body independent of the executive; categories of search terms defining the kinds of communications that would become liable for examination had not been included in the application for a warrant; and search terms linked to an individual (that is to say specific identifiers such as an email address) had not been subject to prior internal authorisation.

1. Grand Chamber judgments are final (Article 44 of the Convention).
All final judgments are transmitted to the Committee of Ministers of the Council of Europe for supervision of their execution. Further information about the execution process can be found here: www.coe.int/t/dghl/monitoring/execution.

The Court also found that the bulk interception regime had breached Article 10, as it had not contained sufficient protections for confidential journalistic material.

The regime for obtaining communications data from communication service providers was also found to have violated Articles 8 and 10 as it had not been in accordance with the law.

However, the Court held that the regime by which the UK could request intelligence from foreign governments and/or intelligence agencies had had sufficient safeguards in place to protect against abuse and to ensure that UK authorities had not used such requests as a means of circumventing their duties under domestic law and the Convention.

Principal facts

The applicants are organisations and individuals that campaign on issues relating to civil liberties and the rights of journalists.

The three applications (which have since been joined) 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 by the UK intelligence services or obtained by them from either communications service providers or foreign intelligence agencies such as the NSA.

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, for the receipt of intelligence from foreign governments and/or intelligence agencies and for the acquisition of data from communications service providers. Some of the applicants also raised complaints under Article 10 (freedom of expression) related to their work as journalists and news organisations.

The three *Big Brother Watch and Others* applications were lodged with the European Court of Human Rights on 4 September 2013, 11 September 2014 and 20 May 2015. In a judgment dated 13 September 2018, the Chamber found that the bulk intercept regime had violated **Article 8 of the European Convention on Human Rights (right to respect for private and family life/communications) and Article 10 (freedom of expression). It also found that the regime for obtaining data from communications service providers had violated Articles 8 and 10; but it considered the regime for obtaining intercept material from foreign governments and/or intelligence agencies to have been Convention compliant.** On 12 December 2018 the applicants requested that the case be referred to the Grand Chamber under Article 43 (referral to the Grand Chamber); on 4 February 2019 the panel of the Grand Chamber accepted that request. A hearing was held on 10 July 2019.
In the first case, leave to intervene as third parties was granted to Human Rights Watch, Access Now, Dutch Against Plasterk, Center For Democracy & Technology, European Network of National Human Rights Institutions and the Equality and Human Rights Commission, the Helsinki Foundation For Human Rights, the International Commission of Jurists, Open Society Justice Initiative, The Law Society of England and Wales and Project Moore. In the second case, leave to intervene was granted to the Center For Democracy & Technology, the Helsinki Foundation For Human Rights, the International Commission of Jurists, the National Union of Journalists and the Media Lawyers' Association. In the third case, leave to intervene was granted to Article 19, the Electronic Privacy Information Center and to the Equality and Human Rights Commission.

Judgment was given by the Grand Chamber of 17 judges, composed as follows:

Robert **Spano** (Iceland), *President*,
Jon Fridrik **Kjølbro** (Denmark),
Angelika **Nußberger** (Germany),
Paul **Lemmens** (Belgium),
Yonko **Grozev** (Bulgaria),
Vincent A. **De Gaetano** (Malta),
Paulo **Pinto de Albuquerque** (Portugal),
Faris **Vehabović** (Bosnia and Herzegovina),
Iulia Antoanella **Motoc** (Romania),
Carlo **Ranzoni** (Liechtenstein),
Mārtiņš **Mits** (Latvia),
Gabriele **Kucsko-Stadlmayer** (Austria),
Marko **Bošnjak** (Slovenia),
Tim **Eicke** (the United Kingdom),
Darian **Pavli** (Albania),
Erik **Wennerström** (Sweden),
Saadet **Yüksel** (Turkey),

and also Søren **Prebensen**, *Deputy Grand Chamber Registrar.*

Decision of the Court

Article 8

Regime for bulk interception

The Court examined the regime for bulk interception of communications as governed by section 8(4) of the Regulation of Investigatory Powers Act (RIPA) 2000.

Owing to the proliferation of threats that States faced from networks of international actors, who used the Internet for communication and who often avoided detection through the use of sophisticated technology, the Court considered that they had a wide discretion ("margin of appreciation") in deciding what kind of surveillance scheme was necessary to protect national security. The decision to operate a bulk interception regime did not therefore in and of itself violate Article 8.

The Court nevertheless considered that, in view of the changing nature of modern communications technology, its ordinary approach towards targeted surveillance regimes needed to be adapted to reflect the specific features of a bulk interception regime with which there was both an inherent risk of abuse and a legitimate need for secrecy. In particular, such a regime had to be subject to "end to end safeguards", meaning that, at the domestic level, an assessment should be made at each stage of the process of the necessity and proportionality of the measures being taken; that bulk interception should be subject to independent authorisation at the outset, when the object and scope of the operation were being defined; and that the operation should be subject to supervision and independent *ex post facto* review. The Court therefore identified several key criteria which needed to be clearly defined in domestic law before such a regime could be said to be compliant with Convention standards.

Applying these newly elaborated criteria to the United Kingdom's bulk interception regime, the Court concluded that the UK regime had suffered from three defects, namely: the absence of independent authorisation for bulk interception warrants; the failure to include the categories of search terms ("selectors") in the application for a warrant; and the failure to ensure that search

terms linked to an individual (that is to say specific identifiers such as an email address) were subject to prior internal authorisation.

In reaching this conclusion, the Court acknowledged the valuable oversight and robust judicial remedy provided by the (then) Interception of Communications Commissioner, an official charged with providing independent oversight of intelligence service activities, and the Investigatory Powers Tribunal, a judicial body set up to hear allegations from citizens that their communications had been wrongfully interfered with. However, those safeguards had not been enough to offset the shortcomings in the regime.

These shortcomings meant that the bulk interception regime had been incapable of keeping the "interference" with citizens' private life rights to what had been "necessary in a democratic society". There had accordingly been a violation of Article 8 of the Convention.

Receipt of intelligence from foreign governments and/or intelligence agencies

The Court concluded that UK law had set out clear, detailed rules governing when intelligence services had been authorised to request intercept material from foreign intelligence agencies and how, once received, the material requested should be examined, used and stored. It also had regard to the role played by the Interception of Communications Commissioner and the Investigatory Powers Tribunal. The Court was therefore satisfied that the regime for requesting and receiving intelligence had been subject to adequate supervision and that an effective *ex post facto* review of activities conducted under this regime had been available.

In these circumstances, sufficient safeguards had been in place to protect against abuse and to ensure that UK authorities had not used requests for intercept material from foreign intelligence partners as a means of circumventing their duties under domestic law and the Convention.

There had, accordingly, been no violation of Article 8 in respect of the regime for the receipt of intelligence from foreign intelligence services.

Acquisition of data from communications service providers

The court noted that the applicants in the second of the joined cases had complained that the regime for the acquisition of communications data under Chapter II of RIPA had been incompatible with their rights under Article 8 of the Convention.

The Court agreed with the Chamber's findings, which the government had not contested, that there had been a violation of Article 8 of the Convention on account of the fact that the operation of the regime had not been "in accordance with the law".

Article 10

The Court reiterated that the protection of a journalist's sources was one of the cornerstones of the freedom of the press. Undermining this protection would have a detrimental impact on the vital public-watchdog role of the press and its ability to provide accurate and reliable information.

The Court was therefore concerned that UK law governing the bulk interception of communications had contained no requirement that the use of selectors or search terms known to be connected to a journalist be authorised by a judge or other independent and impartial decision-making body. Moreover, when it had become apparent that a communication which had not been selected for examination through the deliberate use of a selector or search term known to be connected to a journalist had nevertheless contained confidential journalistic material, there had been no

safeguards to ensure that it could only continue to be stored and examined by an analyst if authorised by a judge or another independent decision-making body.

As a result of those weaknesses there had also been a breach of Article 10 of the Convention.

When it came to requests for data from communications service providers under Chapter II, the Court agreed with the Chamber that the relevant regime had also been in breach of Article 10 of the Convention because it had "not [been] in accordance with the law". However, it found that the regime for receiving intercept material from foreign governments and/or communications service providers did not breach Article 10 of the Convention.

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. It nevertheless made awards to the applicants in the joined cases in respect of costs and expenses incurred as part of their proceedings before the Grand Chamber amounting to 91,000 euros.

Separate opinions

Judges Lemmens, Vehabović, and Bošnjak expressed a joint partly concurring opinion. Judge Pinto de Albuquerque expressed a partly concurring and partly dissenting opinion. Judges Lemmens, Vehabović, Ranzoni and Bošnjak expressed a joint partly dissenting opinion. These opinions are annexed to the judgment.

The judgment is available in English and French.

Press contacts
During the current public-health crisis, journalists can continue to contact the Press Unit via echrpress@echr.coe.int.

Neil Connolly
Tracey Turner-Tretz
Denis Lambert
Inci Ertekin