Q&A on the judgment *Big Brother Watch and Others v. United Kingdom*[1]

This document is a tool for the press, issued in the context of notification of the above judgment. It does not bind the Court.

Is this the first time the European Court of Human Rights has dealt with provisions on secret surveillance?

The European Court of Human Rights has dealt with such issues in many cases going back at least as far as 1978 (Klass v Germany). These cases have included the interception of communications, the obtaining of communications data, the tracking of individuals via GPS and the recording of conversations

Does the case of Big Brother Watch and Others break new ground in the Court's case-law?

The case looks at three different types of surveillance: the bulk interception of communications; intelligence sharing; and the obtaining of communications data from communications service providers.

This is not the first time the Court has looked at bulk interception. Most recently, in June 2018 it found that Swedish legislation and practice in the field of signals intelligence did not violate the European Convention on Human Rights (Centrum För Rättvisa v. Sweden). Among other things, it found that the Swedish system provided adequate and sufficient guarantees against arbitrariness and the risk of abuse. Some ten years ago, it considered similar provisions in the G10 Act in the case of Weber and Saravia v. Germany, and in Liberty v. the United Kingdom it considered the predecessor to the current bulk interception regime. However, Big Brother Watch is the first case in which the Court specifically considered the extent of the interference with a person's private life that could result from the interception and examination of communications data (as opposed to content).

The obtaining of communications from communications service providers has also been considered in earlier judgments, including the recent case of Ben Faiza v. France.

Intelligence sharing has not, however, been considered by the Court in any previous judgment. In the present case it examines, for the first time, the way in which authorities request and receive signals intelligence from foreign Governments.

Finally, in Big Brother Watch the Court expressly stated that the UK's special body for reviewing complaints about alleged secret surveillance, the Investigatory Powers Tribunal, is now a remedy that has to be used as part of the admissibility procedure of exhausting domestic remedies. That goes for whether the complaint is a specific complaint or whether it is a general complaint about the surveillance regimes. In Kennedy v. the United Kingdom (2010) the Court had previously expressed concerns about whether the IPT could be an effective remedy for complaints about the general compliance with the Convention of the UK's secret surveillance regime.

[1] See press release.

Does the finding of several violations of the Convention in this case mean that the UK has to overhaul its regimes for the bulk surveillance of communications and requesting data from communications service providers?

The United Kingdom has updated its surveillance rules under new legislation, the Investigatory Powers Act 2016, which has not yet fully come into force. The Court did not examine the new legislation in its decision.

Isn't it important that States are able to carry out secret surveillance in order to fight against terrorism?

The Court expressly recognised the severity of the threats currently facing many Contracting States, including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, the sexual exploitation of children and cybercrime. It also recognised that advancements in technology have made it easier for terrorists and criminals to evade detection on the Internet. It therefore held that States should enjoy a broad discretion in choosing how best to protect national security. Consequently, a State may operate a bulk interception regime if it considers that it is necessary in the interests of national security.

That being said, the Court could not ignore the fact that surveillance regimes have the potential to be abused, with serious consequences for individual privacy. In order to minimise this risk, the Court has previously identified six minimum safeguards which all interception regimes must have.

The safeguards are that the national law must clearly indicate: the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their communications intercepted; a limit on the duration of interception; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which intercepted data may or must be erased or destroyed. In the case of Roman Zakharov v. Russia, in determining whether the legislation in question was in breach of Article 8, it also had regard to the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law.

Is this the final judgment?

After a Chamber judgment has been delivered, the parties may request referral of the case to the Grand Chamber and such requests are accepted on an exceptional basis. A panel of judges of the Grand Chamber decides whether or not the case should be referred to the Grand Chamber for fresh consideration.

What are the consequences of this judgment for other countries?

The Court looks at applications brought before it on a case by case basis. However, the other member States may, if necessary, draw consequences from a Court judgment so as to avoid findings of similar violations of the European Convention against them.

Are there are any similar cases pending?

The case of Association confraternelle de la presse judiciaire v. France and 11 other applications (nos. 49526/15, 49615/15, 49616/15, 49617/15, 49618/15, 49619/15, 49620/15, 49621/15, 55058/15, 55061/15, 59602/15 and 59621/15) involves complaints by lawyers and journalists, as well as legal persons connected with those professions, about the French Intelligence Act of 24 July

2015, which concerns electronic surveillance measures. The applications were communicated to the French Government on 26 April 2017.

Tretter and Others v. Austria (no. 3599/10), communicated to the Austrian Government on 6 May 2013, concerns 2008 amendments to the Police Powers Act, which extended the powers of the police authorities to collect and process personal data.

Breyer v. Germany (no. 50001/12), communicated to the Government on 21 March 2016, concerns the legal obligation of telecommunications providers to store the personal details of all their customers.

For further information see the Court's factsheets on Mass Surveillance.