Big Brother Watch and others v. the United Kingdom: A Victory of Human Rights over Modern Digital Surveillance?

Maria Tzanou 2018-09-18T12:52:24

On 13th September 2018, the European Court of Human Rights (ECtHR) (First Section) delivered its long-awaited judgment in *Big Brother Watch and others v. the United Kingdom*. In a ruling of significant length (more than 200 pages), the Court considered in detail the UK surveillance regime following the Edward Snowden revelations and found that certain aspects of this violated Articles 8 (right to respect for private and family life) and 10 (freedom of expression) of the Convention.

Judgment

The Court reviewed three main issues concerning the compliance of the UK surveillance framework contained in the Regulation of Investigatory Powers Act 2000 (RIPA) (now repealed by the Investigatory Powers Act 2016 (IPA)) with Article 8 ECHR: i) the bulk interception of communications under section 8(4) of RIPA; ii) the intelligence sharing regime between the USA and the UK whereby UK authorities received material intercepted by the NSA under the PRISM and UPSTREAM programmes; and, iii) the acquisition of communications data from Communications Service Providers ('CSPs') under Chapter II of RIPA.

The bulk interception of communications

The Strasbourg Court noted that bulk interception programmes operated in order to identify unknown threats to national security fall within States' margin of appreciation. Nevertheless, since all interception regimes (both bulk and targeted) have the potential to be abused, the Court held that the discretion afforded to States in operating such regimes 'must necessarily be narrower'.

In this regard, the Court ruled that interception programmes must set out in the law six minimum requirements, established in *Weber and Saravia*, 'in order to be sufficiently foreseeable to minimise the risk of abuses of power'. These are: 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. The Court decided to examine the justification for any interference in the present case by reference to these six minimum requirements having also regard to the three additional factors regarding secret surveillance measures for national security purposes identified in *Zakharov*, namely the arrangements for supervising the implementation of secret surveillance measures, notification mechanisms and the remedies provided for by national law.

Concerning the question at issue, the Court noted that Section 8(4) of RIPA permitted the bulk interception of both content and 'related communications data' (data about the 'who, when and where' of a communication – essentially metadata). Regarding the former, the ECtHR accepted that while anyone could potentially have the content of their communications intercepted, it was clear that the UK intelligence services were 'neither intercepting everyone's communications, nor exercising an unfettered discretion to intercept whatever communications they wish' as communications of individuals known to be in the British islands were excluded and the intelligence services employed targeted bearers to select these communications most likely to carry intelligence value. The Court, nevertheless, raised concerns regarding the safeguards governing the selection of bearers for interception and the selection of intercepted material for examination by an analyst because the UK regime lacked robust independent oversight of the selectors and search criteria used to filter intercepted communications.

What, however, proved fatal for section 8(4) was the exemption of 'related communications data' from the safeguards applicable to the selection, search and filtering of content data. Indeed, RIPA allowed UK intelligence services to search and examine without restriction 'related communications data' of all intercepted communications – even internal ones incidentally intercepted – on the grounds that metadata are less intrusive than content data and they were necessary to determine whether a person is or is not in the British islands. The Court was not persuaded by the UK government's arguments that metadata are less intrusive than content data. In fact, the ECtHR pointed out that the content of an electronic communication might be encrypted and, even if it were decrypted, might not reveal anything of note about the sender or recipient, while metadata could reveal the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. As the Court correctly observed:

'In bulk, the degree of intrusion is magnified, since the patterns that emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with'. The Court, therefore, held that section 8(4) did not provide real safeguards for the selection of metadata for examination and, thus, breached Article 8 ECHR as it did not meet the quality of law requirement and was incapable of keeping the interference to what is 'necessary in a democratic society'.

The intelligence sharing regime

The Court was asked to consider for the first time in the present case the compliance of an intelligence sharing regime with the Convention. Adapting the minimum requirements from *Weber* (see above), it examined the circumstances in which intercept material can be requested; the procedure followed for examining, using and storing the material obtained; the precautions taken when communicating the material obtained to other parties; and the circumstances in which the material obtained must be erased or destroyed and concluded that there were no significant shortcomings in the application and operation of the US-UK intelligence sharing regime and, therefore, no violation of Article 8 ECHR.

The acquisition of communications data from CSPs

The third issue that the Court had to consider under Article 8 was Chapter II of RIPA, which allowed certain UK public authorities to acquire communications data from CSPs. The Court's analysis was rather short in this respect drawing extensively from the CJEU's judgments in *Digital Rights Ireland* and *Watson*, according to which a communications' retention scheme is lawful under EU law where access to communications is limited to the objective of fighting serious crime; is subject to prior review by a court or independent administrative authority; and the data concerned are retained within the EU. The Court found a violation of Article 8 ECHR on the basis that Chapter II RIPA permitted access to retained data for the purpose of combating crime (rather than 'serious crime') and such access was not subject to prior review by a court or independent administrative body – flaws that had already been identified by the High Court.

Communications surveillance and Article 10 ECHR

The Court was also asked to examine the compatibility of section 8(4) and Chapter II of RIPA with Article 10 ECHR. It held that the bulk interception regime violated Article 10 ECHR because of the potential chilling effect that this created to the confidentiality of communications and the absence of any 'above the waterline' arrangements limiting the intelligence services' ability to search and examine confidential material. Finally, the Court concluded that Chapter II also breached Article 10 ECHR due to the lack of sufficient safeguards in respect of confidential journalistic material.

A Failed Update

This is without doubt a landmark decision of the Strasbourg Court marking a victory for the fundamental rights to privacy and freedom of expression over surveillance. The Court should be praised for recognising that bulk metadata surveillance can be as intrusive – or even more intrusive – than access to the content of communications. It is worth mentioning that the CJEU in its surveillance

case-law has followed a slightly different approach on this issue, holding that generalised access to the content of communications breaches ‘the essence of the right to privacy’, while this is not the case for metadata, therefore, revealing a differentiation between the two. This approach of the CJEU clearly disregards the fact that in the context of the internet and modern digital technologies such a distinction between accessing the content of communications or the metadata is very problematic because metadata can often reveal more precise and sensitive information than the data subject is aware about herself through aggregation and the use of modern data mining and algorithmic techniques. In addition, it is often the case that massive metadata internet surveillance is much more efficient and effective than content access.

However, while it should be recognised that the Court’s discussion of the UK surveillance regime in *Big Brother and others v. the UK* is comprehensive and elaborate, overall its analysis appears archaic. The Court’s reliance on authorities, principles and minimum requirements established many years ago (the *Weber and Saravia* case was decided in 2006) against which modern digital surveillance regimes should be evaluated is problematic. This criticism was raised by Judge Kostelo, joined by Judge Turkovic in their partly concurring, partly dissenting Opinion, but in my view it goes beyond the issue of *ex ante* judicial review of secret surveillance. The problem lies in the all-encompassing scope of modern digital surveillance – especially metadata surveillance but not only – that is undertaken in a bulk, indiscriminate way without any differentiation, limitation or exception being made for individuals with no link whatsoever to terrorism or serious crime, as the CJEU held in *Digital Rights Ireland*.

By rejecting the applicants' request to ‘update’ its list of minimum requirements against which surveillance regimes should be examined, the Strasbourg Court missed a chance in the present case to make its case-law more adaptable to present and future surveillance challenges.
