Big brother may continue watching you

October 12, 2018 Guest Blogger Big Brother Watch and Others v. UK, Mass Surveillance,Right to Private Life

By Judith Vermeulen (PhD Candidate, Law & Technology Research Group, Ghent University)

On 13 September 2018, more than five years after Edward Snowden revealed the existence of electronic (mass) surveillance programmes run by the intelligence services of the United States of America and the United Kingdom, the European Court of Human Rights ('ECtHR') found two UK data collection regimes – one of which will not be discussed here[1] – to violate Article 8 of the ECHR.[2] A third one, being part of the information sharing arrangements between these so-called "Five Eyes" countries was, on the contrary, considered to involve a justified interference with the right to respect for private life

While the long-awaited *Big Brother Watch and Others v. UK* judgment, which joined three actions, signifies another victory for civil liberties and privacy advocating non-profit organisations and activists – no less than 16 being the applicants in this case – some serious matters of concern remain. Indeed, the ECtHR did not regard a number of the most intrusive aspects of these highly contested surveillance practices to be problematic: interception of communications and related communications data in bulk continues to be possible (both by intelligence and law enforcement authorities) and information gathered by the US's National Security Agency ('NSA') under its infamous PRISM and Upstream programmes can still lawfully be requested and further processed by the UK's Government Communications Headquarters ('GCHQ').

A comparison with relevant case-law of the Court of Justice of the European Union ('CJEU'), who has, in a number of landmark judgments relating to surveillance by government authorities (*i.e. Digital Rights Ireland*, *Schrems*, *Tele2 Sverige* and *Opinion 1/15*), set rather high privacy and data protection standards, will help to put this judgment into perspective: the extensive safeguards established in Luxembourg should remain the point of reference within Europe. Strasbourg should not be lowering these thresholds instead. While it is true that the cases before the CJEU all concerned the processing of personal data for law enforcement purposes, the cited case-law is nevertheless relevant in the context of the assessment of secret surveillance conducted by intelligence services. Despite a recent formal contestationof the Court of Justice's competences in that regard, it is clear from its decision in *Schrems*, in which it invalidated the Safe Harbour Decision in view of the clear inadequacy of the United States' data protection regime following the Snowden revelations on the NSA run PRISM and Upstream programmes, that it already assessed intelligence practices.

Interception of communications and related communications data in bulk continues to be possible by both intelligence and law enforcement authorities …

Under Chapter I 'Interception' of the UK's Regulation of Investigatory Powers Act 2000 ('RIPA') bulk interception of communications can be permitted. More in particular, the Secretary of State may warrant "the interception of external communications in the course of their transmission by means of a telecommunications systems" when he believes that it is necessary in the interests of national security, for the purpose of preventing or detecting serious crime, or for safeguarding, in circumstances relevant to the interests of national security, the economic well-being of the United Kingdom. The conduct authorised must be proportionate to what is sought to be achieved and shall also be taken to include the obtaining of "related communications data", that is to say data which "relates to the communication or to the sender or recipient, or intended recipient, of the communication" or else "metadata". In a certificate accompanying the warrant, the Secretary of State must also set out a description of the intercepted material considered necessary to examine. It must be noted that, remarkably

enough, not only the intelligence services but also the law enforcement authorities may apply for such a warrant.

In the execution of the warrant, four stages of this so-called "section 8(4) RIPA regime" can be distinguished: firstly, communications are intercepted from a "small" percentage of Internet "bearers"[3], selected as being most likely to carry external communications of intelligence value; secondly, the intercepted communications being the least likely to be of intelligence value, will be filtered out and automatically discarded (in near real-time); subsequently, **simple selectors and complex search criteria** (application of the latter most likely involving "**profiling**") are being applied to the remaining communications, with those matching these selectors and criteria being retained and those that do not being discarded, in order to select communications that are likely to be of intelligence value; finally, some (if not all) of the remaining data are examined by an analyst. The Court noted that "[a]lthough the section 8(4) certificate sets out the general categories of information which might be examined, […] in practice, it is the selection of the bearers, the application of simple selectors […] and then complex searches which determined what communications were examined".

The applicants, bearing in mind the ECtHR's judgment in *Roman Zakharov v. Russia*, argued that the *Weber* criteria[4] – being the minimum requirements established by the Court that have to be set out in law in order to avoid abuses of power contrary to the "in accordance with the law" and "necessary in a democratic society" conditions of Article 8(2) of the ECHR in relation to a (targeted or untargeted) secret surveillance regime –, were not met and in any event did no longer suffice in the light of "technological developments [following which] Governments [can] now create detailed and intrusive profiles of intimate aspects of private life by analysing patters of communications on a bulk basis". They accordingly proposed an "update" of those conditions by including, amongst others, a requirement for "objective evidence of reasonable suspicion" in relation to the persons for whom data was being sought.

The Court, accepting – very blatantly and explicitly in the case at hand – that bulk interception regimes do not *per se* fall outside the wide margin of appreciation that Governments have in choosing how best to achieve the legitimate aim of protecting national security, disagreed by stating that "[b]ulk interception is by definition untargeted, and to require "reasonable suspicion" would render the operation of such a scheme impossible". What *was* on the other hand considered to be of great concern is the lack of robust independent oversight of both the selectors and the search criteria during the third execution stage of the warrant (see *supra*). On top of that, the Court required the categories that are set out in the stage four certificates to be spelled out in less general terms and instead "by reference to specific operations or mission purposes". Though the Court also considered it desirable for the selection of Internet bearers in the first stage of the warrant's execution to be subjected to greater oversight, it did not find that fact alone to be fatal for the Article 8 compliance of the section 8(4) regime. The absence of pre-authorisation for the stage four selection of material by analysts was also not considered, in and of itself, to amount to a failure to provide adequate safeguards against abuse. Taken together, however, the establishment of the nearly unsupervised discretion – especially in stage 3 – for the British authorities to determine which of the intercepted communications are to be examined, led the ECtHR to conclude that there had been a violation of Article 8 of the Convention. More specifically, domestic law was not considered to give citizens an adequate indication of the circumstances in which their communications could be intercepted and subsequently selected for examination. As such, the second *Weber* criterion, requiring a definition of the categories of people liable to have their private life interfered with, had been infringed.

The other five *Weber* requirements were all considered to be complied with. A discussion of the Court's reasoning in this regard, including an assessment of the Chapter I section 15 and 16 RIPA safeguards, is, however, not included in this blog. It is nevertheless important to note

that the exemption (!) of related communications data, in the section 8(4) regime from all requirements of section 16 was found to violate Article 8 ECHR.

… in spite of the by the CJEU established standards in that regard

The CJEU, in *Digital Rights Ireland* and especially in *Tele2 Sverige*, made clear that, in restricting the right to respect for private life and the right to protection of personal data, a law providing for the general and indiscriminate *retention* by communications service providers of communications metadata exceeds the limits of what is "strictly necessary" as such legislation does not require there to be any relationship between the data which must be retained and the objective pursued. Targeted retention based on **objective criteria**, which may vary according to the nature of the measures, built on **objective evidence**, on the other hand, was not prohibited. In concrete terms, the Court required the retention measure to be limited with respect to the "**categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted**". Whereas in *Digital Rights Ireland* the delimitation of the public affected ("persons concerned") was still portrayed as optional, it became mandatory after the judgement in *Tele2 Sverige*. The Court suggested a geographical criterion in that regard.

More recently, however, in *Opinion 1/15*, the transfer of the PNR data of all air passengers, regardless of whether there is any objective evidence that can link them to terrorism or serious transnational crime, flying between the European Union and Canada, was nonetheless regarded to be in compliance with the principle of proportionality. Upon receipt, the Canadian authorities run the PNR data against **pre-established models and criteria** – "**profiles**" – for the purpose of newly identifying certain passengers liable to present a risk to public security, which might give rise to additional checks and potential arrests of those persons at the border. The Court stipulated that considering the extent of the interference "essentially depends on those models and criteria" they "should be specific and reliable, making it possible, as the Advocate General […] observed […] to arrive at results targeting individuals who might be under a '**reasonable suspicion**' […]" . The latter had, as have done the applicants in *Big Brother Watch v. UK*, based himself in that regard on the ECtHR's judgment in *Roman Zakharov v. Russia* in which it ruled that the Russian mobile communications and communications data retention regime violated the Convention as it regarded the judicial scrutiny of the authorisation of *access* by the intelligence authorities to the retained data to be limited in scope, since it was neither provided with sufficient information to assess whether there was a sufficient factual basis to reasonably suspect a particular person nor instructed to verify the existence of a reasonable suspicion against the person concerned.[5]

PNR schemes are, however, while thus comparable to a certain extent, notably less intrusive than the section 8(4) regime as described above. Not in the least because the latter system concerns mainly, though not exclusively, the actual content of communications, whereas the Court of Justice, in *Opinion 1/15*, dealt with air passengers travel information. According to the Court in Luxembourg, the essence of the right to respect for private life would even be affected by the "acquisition of knowledge of the content of […] electronic communications". On top of that, anyone's data could potentially be intercepted with a section 8(4) warrant. The public affected by the draft PNR Canada Agreement – air passengers flying from the EU to Canada – is, to the contrary, clearly delimitated[6], which is one of the reasons why the CJEU adopted a different approach in *Digital Rights Ireland* and *Tele2 Sverige* on the one hand, and *Opinion 1/15* on the other. However, as opposed to what the CJEU decided in the former two cases – where it concerned data retained for law enforcement purposes –, Strasbourg did not consider the bulk *retention**[7]** of data as such* for national security reasons by communication service providers to be problematic in *Roman Zakharov v. Russia* and as such could not be said to have deviated now, in *Big Brother Watch v. UK*, from its previous case-law. Yet, assuming that a somewhat more lenient approach vis-à-vis the *collection* of data in bulk could be justified on the basis of the nature[8] of the authorities concerned, it must be reiterated that the tools

foreseen in the section 8(4) regime are not only available for intelligence services but also for law enforcement agencies (see *supra*).

In any event, the ECtHR, as did the CJEU in *Opinion 1/15*, should, in *Big Brother Watch v. UK*, have put forward the **"reasonable suspicion" criterion** as the condition to be complied with when determining the **selectors and search criteria** in stage 3 – and thus not in the initial phase of interception – of the warrant's execution, instead of merely requiring them to be subjected to (non-public) independent oversight. Admittedly, had the Court in Strasbourg applied this **criterion** in stage 1 instead, as suggested by the applicants in this case, it would indeed have gone further than it had done previously in *Roman Zakharov v. Russia*. Nevertheless, this does not change the fact that the Court in Strasbourg, unlike the CJEU, gave no indication whatsoever as to how the **selectors and search criteria** should be determined and as such on how to constrict the *access* by the intelligence authorities to bulk amounts of personal data of individuals.

PRISM and Upstream do not involve your right to respect for private life

Without going into all the details of the information sharing arrangements that exist between the US and the UK and the latter's own rules in that regard, it may, bearing in mind the *Schrems* case-law, moreover surprise that, the ECtHR regarded the request and use – provided the section 8(4) safeguards are applied in this context as well – by the UK's intelligence services of personal data potentially gathered by the NSA in the context of its aforementioned secret surveillance programmes to be in accordance with Article 8 of the Convention. In fact, Strasbourg did not consider the interception itself of communications in this regime to be part of "the interference under consideration" as "[it does] not […] occur within the United Kingdom's jurisdiction, and was [thus] not attributable to the State under international law". In the reasoning of the Court, a circumvention of a State's own rules or of their Convention obligations can be prevented when the circumstances in which such a request can be made are sufficiently circumscribed. The level of circumscription could, however, never undo or remedy a violation – in European standards – of privacy and data protection rights that occurred in a third country still in the phase of collection. On top of that, it need be noted that, as is the case in stage 2 and 3 in the execution of a section 8(4) regime warrant, nowhere is mentioned, that the data received in bulk are filtered and partly discarded before being examined by analysts. In that regard, judge Koskelo and judge Turkovic noted in a separate opinion that "the shortcomings referred to […] in the context of the section 8(4) regime also attach to the intelligence-sharing regime".

Referring to *Big Brother Watch v. UK* as a long and complicated case would be an understatement. This blog does not therefore contend to be exhaustive in its description and assessment of the judgment. It is clear, however, that the issues identified above are not the least. Violations of Article 8 ECHR have been established, but big brother may continue watching you.

[1] The Chapter 2 RIPA regime.

[2] The ECtHR also had to assess whether the regimes violated Articles 10, 6, and 14 in combination with Articles 8 and 10 of the Convention. However, the Court's respective conclusions in that regard will not be discussed for the purposes of this blog.

[3] See §9 *Big Brother Watch and Others v. UK*.

[4] The *Weber* requirements (see §370 *Big Brother Watch and Others v. UK*): the nature of the 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.

[5] In *Roman Zakharov v. Russia*, the applicant complained about the requirement for mobile network operators in Russia to create databases in which they had to store all mobile telephone communications and related communications data of their subscribers for three years. He also challenged the subsequent direct remote access the authorities had thereto.

[6] In that sense, the transfer of PNR data could even be considered targeted.

[7] To be distinguished from the subsequent access by the intelligence authorities to the retained data; “retention” is here compared with “interception”.

[8] Intelligence services v. law enforcement authorities.