# *Big Brother Watch and Others v UK*: Lessons from the Latest Strasbourg Ruling on Bulk Surveillance

Bart van der Sloot* and Eleni Kosta*

*Big Brother Watch and Others v the United Kingdom, Apps No 58170/13, 62322/14 and 24960/15, European Court of Human Rights, 13 September 2018*

*A United Kingdom mass surveillance law, allowing for bulk interception by intelligence agencies and data sharing with foreign counterparts, violated both Article 8 and Article 10 of the European Convention on Human Rights. The European Court of Human Rights found that, inter alia, the lack of oversight of the entire selection process and the absence of any real safeguards applicable to the selection of related communications data for the examination violated the right to privacy. A similar conclusion is drawn by the Court because the UK law permitted access to retained data for the purpose of combating crime, which was not subjected to prior review by a court or independent administrative body.*

*Article 8 ECHR; Sections 8 and 16 of the Regulation of Investigatory Powers Act 2000 (RIPA)*

## I. Introduction

In Europe, in the aftermath of the Snowden revelations, the UK surveillance activities have been in the spotlight of privacy and civil rights organisations, as well as of individuals. In 2013, a number of Civil Rights Organisations (incl. Big Brother Watch) filed an application at the European Court of Human Rights (ECtHR or Court) against the Government Communications Headquarters' (GCHQ) secret interception of communications and data claiming a violation of the right to privacy.[1] In 2014, a second application was filed by the Bureau of Investigative Journalism, a UK not-for-profit media organisation, against the UK claiming that the generic surveillance carried out by the GCHQ constitutes an interference with their right to privacy and freedom of expression.[2] In these two cases the applicants filed an application directly to the ECtHR, without first filing their case in front of national courts and tribunals.

Ten Human Rights Organisations[3] chose a different path and started a legal battle at the national level before turning to the ECtHR. They filed separate applications[4] at the UK Investigatory Powers Tribunal (UK IPT or Tribunal), where their cases were joined. After the publication of the judgment of the UK IPT in 2015, the Ten Human Rights Organisations

[1] Joint application under art 34, *Big Brother Watch, Open Rights Group, English PEN, Dr Constanze Kurz v the United Kingdom* App no 58170/13 (ECtHR, lodged 4 September 2013).
[2] Joint application under art 34, *Bureau of Investigative Journalism and Alice Ross v the United Kingdom* App no 62322/14 (ECtHR, lodged 11 September 2014).
[3] Amnesty International Limited (Amnesty International), Bytes for All (B4A), The National Council for Civil Liberties (Liberty), Privacy International, The American Civil Liberties Union (ACLU), The Canadian Civil Liberties Association (CCLA), The Egyptian Initiative for Personal Rights (EIPR), The Hungarian Civil Liberties Union (HCLU), The Irish Council for Civil Liberties (ICCL) and The Legal Resources Centre (LRC).
[4] Case numbers: IPT/13/77/H, IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH, IPT/13/204/CH.

filed an application against the UK at the ECtHR.[5] The main arguments raised by the applicants were that the UK legal framework governing the interception of communications and communications data and the receipt of foreign intercept material is not 'in accordance with the law' and thus amounted to an interference with the rights to privacy and freedom of expression.

The First Section of the European Court of Human Rights delivered its judgment on 13 September 2018 finding violation of Articles 8 and 10 of the European Convention on Human Rights (ECHR or Convention). However, the Court did not find that the operation of a bulk interception regime did not as such violate the ECHR, as the applicants would have wished it to. The judges of the First Section of the Court were significantly divided, as only three judges agreed with the final judgment in its entirety, while four of the judges raised significant points in their separate opinions: two judges, Judge Koskelo joined by Judge Turkovic, delivered a partly concurring, partly dissenting opinion, while two other judges, Judge Pardalos and Judge Eicke, delivered a joint partly dissenting and partly concurring opinion. In February 2019 the case was referred to the Grand Chamber of the ECtHR. In this case note, we present the main findings of the Court and we assess the positions of the First Section in view of earlier case law of the ECtHR and in light of technological developments.

## II. History of Legal Proceedings and Facts of the Case

The application of Big Brother Watch, Open Rights Group, English PEN and Constanze Kurz, a German internet activist, against the United Kingdom was lodged soon after the Snowden revelations, in September 2013. The ECtHR prioritised the case, but stayed it until the decision of the UK IPT on the *Ten Human Rights Organisations v United Kingdom* case. In September 2014, the Bureau of Investigative Journalism (BIJ) and Alice Ross, a reporter with the BIJ, lodged another application against the UK at the ECtHR.[6] Following the Snowden revelations, Ten Human Rights Organisations claimed that they believed that the content of their communications and their communications data[7] could have been intercepted by the UK intelligence services. Their claim was based on the fact that they regularly used means such as email, text messages, phone calls, video calls, social media and instant

[5] *The 10 human rights organisations (the American Civil Liberties Union, Amnesty International, Bytes for All, the Canadian Civil Liberties Association, the Egyptian Initiative for Personal Rights, the Hungarian Civil Liberties Union, the Irish Council for Civil Liberties, the Legal Resources Centre, Liberty, Privacy International) v UK* App no 24960/15 (ECtHR, lodged 20 May 2015).

[6] *Bureau of Investigative Journalism and Alice Ross v the United Kingdom* App no 62322/14 (ECtHR, lodged 11 September 2014).

[7] s 21(4) of the UK Regulation of Investigatory Powers Act 2000 defines ''communications data' as ''any of the following—

(a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;

(b) any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person—

(i) of any postal service or telecommunications service; or

(ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;

(c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service'.

messaging for their communications and on the sensitivity of the communication with their contacts that range from NGOs and lawyers to victims of human rights abuses and whistle-blowers. In particular the Ten Human Rights Organisations turned against the UK's practice and legal regimes governing the receipt of foreign intercept material collected by the US authorities pursuant to Prism and Upstream programmes and the 'bulk' interception of communications pursuant to Tempora and claimed breach of Articles 8 (privacy) and 10 (freedom of expression) ECHR.[8]
As part of the proceedings, a 'closed' hearing took place where neither the applicants, nor their advocates were allowed to participate. The applicants submitted a renewed request for disclosure of material relating to the internal policies and guidance, especially those concerning the handling of confidential information obtained pursuant to the interception of private communications according to section 8(4) Regulation of Investigatory Powers Act 2000 (RIPA), claiming infringement of their right to privacy.[9] More concretely the applicants focused on section 8(4) RIPA that regulated

> bulk interception, inspection, retention and disclosure of communications and communications data is not 'in accordance with the law' as required by Article 8(2) ECHR [claiming that] the interception regime under s. 8(4) cannot be characterised as either 'necessary in a democratic society' or proportionate under Article 8(2) ECHR' [and finally that the] receipt, inspection and retention of intercepted communications and communications data under Prism and Upstream is not carried out 'in accordance with the law'.[10]

RIPA allows the interception of internal and external communications, after the issuing of a relevant warrant, containing different provisions for warrants for interception of communications. Warrants for communications that are both transmitted and received within the United Kingdom (internal communications) are regulated in section 8(1) of RIPA and warrants for communications between the United Kingdom and abroad (external communications) are regulated in section 8(4) of RIPA.

The UK IP Tribunal published three rulings on the cases initiated by the Ten Human Rights Organisations: one in December 2014, one in February 2015 and in June 2015 its open determination.[11] In its first judgment, the UK IPT made extensive references to the jurisprudence of the ECtHR in order to reach its conclusion on the case and admitted that activities relating to Prism engage the rights to privacy and freedom of expression, as protected in Articles 8 and 10 ECHR respectively.[12]

---

[8] Judgment of 5 December 2014, [2014] UKIPTrib 13_77-H, para 3.
[9] The 10 Human Rights Organisations, 'Additional submissions on the facts and complaints' (2015) para 19 <https://www.amnesty.org/en/documents/ior60/1415/2015/en/> accessed 17 November 2017.
[10] *10 Human Rights Organisations and Others v UK* Application Form to the ECtHR App no 24960/15, 7.
[11] The functioning of the UK IPT is regulated in ss 65-70 of RIPA and in The Investigatory Powers Tribunal Rules 2000 (IPT Rules 2000), no 2665.
The procedures in the UK IPT differ from the procedures valid for ordinary courts, as it is allowed to hold closed sessions without the participation of the applicants, to have some parts of the hearing closed and some open and it is not obliged to necessarily provide justifications for its decisions: David Anderson, 'A Question of Trust Report of the Investigatory Powers Review' (Crown Copyright 2015), 122 https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf accessed 17 November 2017.
[12] Judgment of 5 December 2014 [2014 ] UKIPTrib 13_77-H, para 36.

The UK IP Tribunal in its 5 December 2014 judgment summarised two requirements for the interference with Article 8 ECHR to be 'in accordance with the law'. The first one required that there should not exist an unfettered discretion for executive action and that there must be controls on the arbitrariness of that action.[13] According to the second requirement the nature of rules should be clear and their ambit should be in the public domain to the extent that this would be possible, so that the existence of interference with privacy could in general terms be foreseeable.[14] While the UK IPT concluded that the first requirement was satisfied both before and after the disclosures made in the UK IPT judgment, it found that the second one was not satisfied before the public was informed.[15]

On the basis on these findings the question remained open whether there was a breach of Articles 8 and 10 ECHR prior to the disclosure of the intelligence sharing regime, and invited the parties to the case for submissions on the topic,[16] which became a subject of the second judgment.

Based on the submission of the parties, the UK IPT concluded in February 2015:

> (i) that prior to the disclosures made and referred to in the First Judgment [of 5 December 2014] and the Second Judgment [of 6 February 2015], the regime governing the soliciting, receiving, storing and transmitting by UK authorities of private communications of individuals located in the UK, which have been obtained by US authorities pursuant to Prism and/or (on the Claimants' case) Upstream, contravened Articles 8 or 10 ECHR,
> (ii) that it now complies with the said Articles.17

The disclosures following the Snowden revelations in the UK IPT judgment of 5 December 2014 were considered sufficient by the Tribunal in order to justify the legitimacy of the surveillance regime by the UK intelligence services. In this way the UK IPT considers that the accessibility and foreseeability requirements are satisfied when the public is informed about the circumstances of the surveillance regime, even when such information does not originate for the government or the legislator.

In June 2015 the UK IPT published its amended open determination on the heard cases, addressing two remaining issues.[18] The Tribunal made determinations in favour of two of the human rights organisations; for the rest, it did not confirm whether their communications had been intercepted. Relating to the Egyptian Initiative for Personal Rights, their communications had been intercepted lawfully and proportionately under section 8(4) RIPA, however, the retention time exceeded the one specified in the internal policies of the GCHQ, even though it had not been accessed. The destruction of documents was ordered, but no compensation was awarded. In respect to the Legal Resources Centre, the interception was again lawful and proportionate, however, the selection for examination was not done pursuant to the internal procedure. As the material was not used, and no record had been retained, no

[13] ibid para 37.
[14] ibid para 37.
[15] Judgment 6 February 2015, [2015] UKIPTrib 13_77-H, para 22.
[16] Judgment of 5 December 2014 [2014] UKIPTrib 13_77-H, para 154.
[17] Order of 6 February 2015 UKIPTrib 13_77-H (emphasis added).
[18] Open determinations of 22 June 2015, amended by 1 July letter (correcting the name of one of the human rights organisations).

compensation was awarded.[19] It is striking that on 1 July 2015 the Tribunal sent a letter to Amnesty International recognising that the open determination should have referred to Amnesty and not the Egyptian Initiative for Personal Rights, wishing to apologise and correct the error.[20]

As expected, the Ten Human Rights Organisations that were the claimants in the cases in front of the Tribunal, were not satisfied with the findings of the Tribunal and filed an application against the UK at the ECtHR.[21] They alleged that the legal framework governing the interception of communications and communications data and the receipt of foreign intercept material is not 'in accordance with the law' and thus amounts to an interference with Articles 8 and 10 ECHR. The applicants complained also under Article 6 ECHR, claiming that the proceedings before the UK IPT infringed their right to a fair trial. Furthermore, relying on Article 14 (prohibition of discrimination) together with Articles 8 and 10 of the Convention, they argued that section 8(4) RIPA is indirectly discriminatory on grounds of nationality and national origin, as section 16 RIPA differentiates between people known to be in the British Islands and abroad, providing additional safeguards only to the former.[22] The ECtHR joined their application with the ones submitted by Big Brother Watch and the Bureau of Investigative Journalism, and the hearing took place on 7 November 2017.[23] As already mentioned above, The First Section of the European Court of Human Rights delivered its judgment on 13 September 2018,[24] while in February 2019 the referral to the Grand Chamber of the ECtHR was accepted.

## III. Judgment of the ECtHR

### 1. *In Abstracto* Claims

Following Article 34 ECHR, '[t]he Court may receive applications from any person, non-governmental organisation or group of individuals claiming to be the victim of a violation'[25] of right(s) protected by the Convention. The ECtHR as a principle does not consider it its task to review laws and practices *in abstracto*, 'but to determine whether the manner in which they were applied to, or affected the applicant gave rise to a violation of the Convention.'[26] However, occasionally the Court has allowed the submission of cases where the applicants suspect interference of their rights that are protected under the Convention, even when they

[19] Statement of facts, *10 Human Rights Organisations and Others v The United Kingdom* App no 24960/15, s A3(d) <http://hudoc.echr.coe.int/eng?i=001-159526> accessed 17 November 2017.
[20] President of the Investigatory Powers Tribunal, 'Letter to Amnesty International Ltd and others' (1 July 2015) <http://www.ipt-uk.com/docs/IPT_to_Liberty_Others.pdf> accessed 17 November 2017.
[21] Statement of facts, *10 Human Rights Organisations v UK* (n 19).
[22] ibid.
[23] The Chamber hearing of 7 November 2017 on the cases *Big Brother Watch and Others v UK* App no 58170/13, *Bureau of Investigative Journalism and Alice Ross v UK* App no 62322/14 and *10 Human Rights Organisations and Others v UK* App no 24960/15 <https://bit.ly/2AkeS2N > accessed 17 November 2017.
[24] *Big Brother Watch and Others v UK* Apps no 58170/13, 62322/14 and 24960/15 (ECtHR, 2018).
[25] art 34 ECHR.
[26] *Roman Zakharov v Russia* App no 47143/06 (ECtHR, 2015), para 164 citing *NC v Italy* App no 24952/94 (ECtHR, 2002), para 56; *Krone Verlag GmbH & Co KG v Austria (no 4)* App no 72331/01 (ECtHR, 2006), para 26; and *Centre for Legal Resources on behalf of Valentin Câmpeanu v Romania* App no 47848/08 (ECtHR, 2014), para 101.

cannot prove it, especially in relation to secret surveillance.[27] In the recent cases *Zakharov* and *Szabó and Vissy*, the Court made concrete reflections on admissibility in surveillance cases. The Court accepted that 'the secret nature of surveillance measures would deprive individuals of access to effective review [seeing] the mere existence of surveillance laws as a threat'[28] and explicitly stated that it accepts *in abstracto* claims.[29] Mass surveillance typically does not affect one specific individual, but rather large parts of society. The legal question with respect laws that grant powers of bulk interception to intelligence agencies is not so much whether concrete harm has been done to a person in a concrete instance, and whether such interference would be legitimate. Rather, what is at stake is whether the law itself conforms to the principles of legality, legitimacy and incorporates sufficient checks and balances to mitigate the risk of abuse of power.[30] In *Big Brother Watch and Others v UK* the Court repeated the two criteria under which such *in abstracto* claims would be accepted:

> first, the Court would examine whether the applicant could possibly be affected by the legislation permitting secret surveillance measures; and secondly, it would take into account the availability of remedies at the national level and adjust the degree of scrutiny depending on the effectiveness of such remedies.[31]

## 2. Exhaustion of Domestic Remedies

A major point of interest in the *Big Brother Watch and Others v UK* judgment is exactly the exhaustion of domestic remedies; before a complaint is declared admissible by the European Court of Human Rights, applicants need to exhaust all domestic remedies, which normally means going to a national court, a court of appeal and the supreme court. The ECtHR is willing to make an exception when the domestic remedies are not effective, for example when intelligence agencies are subjected to marginal judicial control; in such matters, it is willing to be the court of first instance. The national legislation in the UK does not allow complaints on human rights against the UK Intelligence agencies to be heard by the UK High Court. Such complaints are under the exclusive jurisdiction of the UK IPT.[32] In the case of *Big Brother Watch and Others v UK*, the applicants have not exhausted the domestic remedies and the ECtHR has to assess to what extent the UK IPT provides an effective legal remedy. The ECtHR comes to the conclusion that it does, among others, because it has

---

[27] For more about (in)admissibility of '*in abstracto* claims' and their differentiation from claims in which the Court recognised 'hypothetical harm' as sufficient for granting applicants the victim status see, for instance, Bart van der Sloot, 'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities' in Serge Gutwirth, Ronald Leenes and Paul de Hert (eds), *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection* (Springer 2016), 419-422 and 426-429.

[28] Mark Cole and Annelies Vandendriessche, 'From *Digital Rights Ireland* and *Schrems* in Luxembourg to *Zakharov* and *Szabó/Vissy* in Strasbourg: What the ECtHR made of the deep pass by the CJEU in the recent cases on mass surveillance' (2016) 2(1) EDPL 121,129.

[29] *Zakharov v Russia* (n 26) para 178. For some further throughts on the fact that the Court accepts *in abstracto* claims, see Bart van der Sloot, 'Editorial' (2016) 2(1) EDPL 1.

[30] *Szabó and Vissy v Hungary* App no 37138/14 (ECtHR, 2016), para 32: ''in recognition of the particular features of secret surveillance measures and the importance of ensuring effective control and supervision of them, the Court has accepted that, under certain circumstances, an individual may claim to be a victim on account of the mere existence of legislation permitting secret surveillance, even if he cannot point to any concrete measures specifically affecting him.'

[31] *Big Brother Watch and Others v UK* (n 24) para 392, citing *Zakharov v Russia* (n 26) para 171

[32] Adam Tomkins, 'Justice and security in the United Kingdom' (2014) 47(3) Israel Law Review 4.

authority to judge cases in full, because it is manned by high quality judges and because it also has access to 'below the waterline' documents, which cannot be made public for reasons of national security.[33]

However, in an earlier case, *Kennedy v The United Kingdom*[34] of 2010, the Court examined domestic remedies in the UK and the role of the UK IPT in the context of interception of internal communications. The ECtHR had judged that the UK IPT at that point did not provide an effective remedy, at least in that case. Since then, a number of changes have been made, so that it should now be considered effective, according to the Court. Moreover, the reason why the UK IPT did not provide an effective remedy for Kennedy does not directly apply to the case at hand. Unlike the present case, in *Kennedy*, the Court was not being called upon to consider the general complaint entirely *in abstracto*. The Court, however, does not conclude that the case of the applicants must consequently be declared inadmissible:

> while the Court acknowledges that since Kennedy was decided in 2010 the IPT has shown itself to be an effective remedy which applicants complaining about the actions of the intelligence services and/or the general operation of surveillance regimes should first exhaust in order to satisfy the requirements of Article 35 § 1 of the Convention, it would nevertheless accept that at the time the applicants in the first and second of the joined cases introduced their applications, they could not be faulted for relying on Kennedy 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.[35]

This means that the criterion for judging whether there are effective remedies on a national level is no longer an objective, but a subjective one. The question is not whether the remedies available to the applicants were in fact effective or not, but whether the applicants had reason to believe that they were effective or not. Such may have a considerable impact on the subsequent case law of the ECtHR. That is why two judges, namely Pardalos and Eicke, disagree on this point in their joint partly dissenting and partly concurring opinion. They stress that the UK IPT does provide an effective remedy due to the changes made, that this case is different from that of *Kennedy*, that the applicants in this case were informed by the government that their claim could be received by the UK IPT and that the applicants should consequently be denied in their claim.[36]

### 3. Ex-Ante and Ex-Post Authorisation

Referring to the question whether the interference with Article 8 ECHR is 'in accordance with the law', the Court stresses that there are six minimum standards that must be respected by the legislative power when drafting laws. What makes this interesting is that the original focus of the Court when assessing whether an interference was 'in accordance with the law' was to evaluate the use of power by the executive branch and whether the use of power had a basis in a legislative measure adopted by the legislative branch. In recent years, the Court has been increasingly willing to use the same criterion check whether the national judiciary acted

[33] *Big Brother Watch and Others v UK* (n 24) para 250.
[34] *Kennedy v The United Kingdom* App no 26839/05 (ECtHR, 2010).
[35] *Big Brother Watch and Others v UK* (n 24) para 268.
[36] *Big Brother Watch and Others v UK* (n 24) Joint partly dissenting and partly concurring opinion, para 14.

conforming to the principles contained in the European Convention on Human Rights, albeit it only applied a marginal test. The national legislator, however, was largely free from the gaze of the ECtHR until about a decade ago. In more recent years, the ECtHR is increasingly willing to assess the role of the national legislator; it fears, inter alia, that national legislators, under pressure of popular sentiments, will attribute too much power to the executive branch in the fight against terrorism, and include too limited checks and balances.

That is why the Court is increasingly willing to check laws *in abstracto*, meaning that it will assess a law or policy without analysing its application in the concrete case at hand. Rather it will assess whether the law itself abides by the minimum principles of the rule of law; in a sense, this can be viewed as a move from providing material justice to providing procedural justice. This is called the 'quality of law' doctrine by the ECtHR; in addition, it speaks of applying a Conventionality or Convention compliance check. Like a constitutional court would do, it assesses laws *in abstracto* on their conformity with basic principles of legitimacy and legality.
The six minimum principles the Court lays down for national laws is that they must specify: (1) the nature of offences which may give rise to an interception order; (2) a definition of the categories of people liable to have their communications intercepted; (3) a limit on the duration of interception; (4) the procedure to be followed for examining, using and storing the data obtained; (5) the precautions to be taken when communicating the data to other parties; and (6) the circumstances in which intercepted data may or must be erased or destroyed.[37]

In this case, the applicants suggest that the Court should add to its list of minimum requirements the need for objective evidence of reasonable suspicion in relation to the persons for whom data is being sought, prior independent judicial authorisation of interception warrants, and the subsequent notification of the surveillance subject. Such an addition could be in line with the position held by the Court in *Szabó and Vissy v Hungary*, where the Court recognised that the 'guarantees required by the extant Convention case-law on interceptions need to be enhanced so as to address the issue of such surveillance practices.'[38] The ECtHR, however, rejects their argument, among others stressing that it would be wrong to automatically assume that bulk interception constitutes a greater intrusion into the private life of an individual than targeted interception, which by its very nature is more likely to result in the acquisition and examination of a large volume of his or her communications. In addition, it stresses that by requiring objective evidence of reasonable suspicion in relation to the persons for whom data is being sought and the subsequent notification of the surveillance subject would intervene with the state's margin of appreciation. While

> judicial authorisation is an 'important safeguard against arbitrariness' to date it has not considered it to be a 'necessary requirement' or the exclusion of judicial control to be outside 'the limits of what may be deemed necessary in a democratic society.[39]

Although the Court considers judicial authorisation to be an important safeguard, and perhaps even 'best practice', by itself it can neither be necessary nor sufficient to ensure compliance

[37] *Weber and Saravia v Germany* App no 54934/00 (ECtHR, 2006-XI), para 95.
[38] *Szabó and Vissy v Hungary* (n 30) para 70.
[39] *Big Brother Watch and Others v UK* (n 24) paras 318-319.

with Article 8 of the Convention.

Along this line of argumentation, the Court in *Big Brother Watch and Others v UK* did not find a violation of Article 8 in relation to effective oversight:

> while the Court considers judicial authorisation to be highly desirable […] the authorisation of section 8(4) warrants by the Secretary of State does not, in and of itself, give rise to a breach of Article 8 of the Convention.[40]

So, in the case of the United Kingdom the Court departed from its position held when assessing Russian or Hungarian oversight schemes. Interestingly Christakis wonders on this point whether the Court runs a two-speed control. While there are Eastern European countries whose surveillance laws the Court has found to be in violation of the Convention, there are Western countries that seem to benefit from a more 'flexible' evaluation. Christakis suggests that the ECtHR may believe democratic systems as such would be a pledge against abuse.[41]

It is on this point that judges Koskelo and Turkovic disagree in their partly concurring, partly dissenting opinion. They agree with the majority that the Contracting States must enjoy a wide margin of appreciation in determining whether the protection of national security requires the kind of surveillance of communications which is at issue in the present case. However, the two judges stress that given the high risks of abuse, which at worst may undermine not only individual rights and freedoms but democracy and the rule of law more generally, the margin must be narrow when it comes to the necessary safeguards against abuse. In light of the changes in both the nature and scope of surveillance and in the prevailing factual realities, they feel that stricter requirements should be in place. In particular, they question the approach according to which prior independent control by a judicial authority should not be a necessary requirement in the system of safeguards. They believe that there should not only be safeguards ex post, but also independent control ex ante, because the authorisation and implementation of the surveillance are wholly in the hands of the executive authorities.

## 4. Protection of Metadata

The Court does find a violation on the point of a partial exemption in national law from regulation of the meta-data, which is called the 'related communication', or in the words of the court the 'who, when and where' data. The Court suggests that the processing of content data and of metadata can be equally intrusive. Metadata, for example,

> could reveal the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. In bulk, the degree of intrusion is magnified, since the patterns that will 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.[42]

---

[40] ibid para 381.

[41] Theodore Christakis, 'A fragmentation of EU/ECHR law on mass surveillance: initial thoughts on the Big Brother Watch judgment' (*European Law Blog*, 20 September 2018) https://europeanlawblog.eu/2018/09/20/a-fragmentation-of-eu-echr-law-on-mass-surveillance-initial-thoughts-on-the-big-brother-watch-judgment accessed 28 May 2019.

[42] *Big Brother Watch and Others v UK* (n 24) para 356.

Therefore, the Court argued that there should

> be sufficient safeguards in place to ensure that the exemption of related communications data from the requirements of section 16 of RIPA is limited to the extent necessary to determine whether an individual is, for the time being, in the British Islands.[43]

This is in line with the position of the Court in *Benedik v Slovenia*, where the Court found that

> what would appear to be peripheral information sought by the police, namely the name and address of a subscriber, must in situations such as the present one be treated as inextricably connected to the relevant pre-existing content revealing data.[44]

Such data, it believed, might reveal a good deal about the online activity of an individual, including sensitive details of his or her interests, beliefs and intimate lifestyle.

The now established position that metadata does not deserve lesser protection compared to content data is also in line with the CJEU case law, according to which metadata

> is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them … In particular, that data provides the means … of establishing a profile of the individuals concerned, information that is no less sensitive, having regard to the right to privacy, than the actual content of communications.[45]

Of course, both by the CJEU and the ECtHR refer to cases where bulk collection of metadata was involved. However, given the technical developments and the potential of information technologies, even limited amounts of metadata can provide rich information about individuals. Potentially, the findings of the judgment may have a significant impact on the future protection of metadata.

Judge Yudkivska in her concurring opinion, joined by Judge Bosnjak, gave an even stronger description of the importance they assign to metadata. They suggest that by analysing the wealth of metadata available of most citizens,

> an outstandingly intrusive portrait is obtained of the person concerned, revealing his or her personal and professional relationships, ethnic origin, political affiliation, religious beliefs, membership of different groups, financial status, shopping or disease history, and so on.[46]

## 5. Sharing Intelligence Data

[43] ibid para 357.

[44] *Benedik v Slovenia* App no 62357/14 (ECtHR, 2018), para 109. For a full analysis of the case, see Nataša Pirc Musar, 'Benedik v Slovenia: Dynamic IP and Communication Privacy' (2018) 4(4) EDPL 554 – 562.

[45] Joined cases C-203/15 and C-698/15 *Tele2/Watson* [2016] ECLI:EU:C:2016:970, para 99. For a full analysis of this CJEU judgment, see Will R Mbioh, 'Post-och Telestyrelsen and Watson and the Investigatory Powers Act 2016' (2017) 3(2) EDPL 273 – 282.

[46] *Benedik v Slovenia*, concurring opinions of Judge Yudkivska joined by Judge Bosnjak.

Privacy International, a British NGO, issued in April 2018 a report where it revealed that modern intelligence sharing allows access to ‘

> ‘raw’ (i.e. unanalysed) information, such as internet traffic intercepted in bulk from fibre optic cables by another government; information stored in databases held by another government or jointly managed with another government [, as well as receipt of] results of another government’s analysis of information, for example, in the form of an intelligence report[47].

Therefore Privacy International called for *urgent development of safeguards*.

It is revolutionary that the ECtHR explicitly recognises the threat of sharing intelligence data between the various intelligence agencies. It has been suggested for years by civil society organisations that agencies may circumvent the legal restrictions applicable to them by either explicitly requesting or conveniently getting the data they are not themselves allowed to gather from foreign intelligence agencies that are not bound by those restrictions. The Court is not only willing to acknowledge this threat, but is also explicit in applying the minimum requirements for laws to this context:

> It is true that the interference in this case is not occasioned by the interception of communications by the respondent State. However, as the material obtained is nevertheless the product of intercept, those requirements which relate to its storage, examination, use, onward dissemination, erasure and destruction must be present. Indeed, as the Venice Commission noted, as States could use intelligence sharing to circumvent stronger domestic surveillance procedures and/or any legal limits which their agencies might be subject to as regards domestic intelligence operations, a suitable safeguard would be to provide that the bulk material transferred could only be searched if all the material requirements of a national search were fulfilled and this was duly authorised in the same way as a search of bulk material obtained by the signals intelligence agency using its own techniques. Furthermore, while the first and second of the six requirements may not be of direct relevance where the respondent State is not carrying out the interception itself, the Court is nevertheless mindful of the fact that if Contracting States were to enjoy an unfettered discretion to request either the interception of communications or the conveyance of intercepted communications from non-Contracting States, they could easily circumvent their obligations under the Convention.[48]

The Court did not find a violation of the ECHR in relation to the sharing of intelligence data. The Court noted that

> Due to the nature of global terrorism, and in particular the complexity of global terror networks, the Court accepts that taking such a stand – and thus preventing the perpetration of violent acts endangering the lives of innocent people – requires a flow of information between the security services of many countries in all parts of the

[47] Privacy International, ‘Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards’ (24 April 2018) 5 <https://privacyinternational.org/report/1741/secret-global-surveillance-networks-intelligence-sharing-between-governments-and-need> accessed 8 October 2018.

[48] *Big Brother Watch and Others v UK* (n 24) paras 423-424.

> world. As, in the present case, this 'information flow' was embedded into a legislative context providing considerable safeguards against abuse, the Court would accept that the resulting interference was kept to that which was 'necessary in a democratic society'[49].

However, Judge Koskelo joined by Judge Turković in their partly concurring, partly dissenting opinion found that there were no adequate safeguards in place and that there was also a violation of Article 8 ECHR in respect of the UK regime on data sharing.[50]

## IV. Conclusion

The reasoning of the First Section of the Court appeared to be in line with recent case law when examining the admissibility of the cases. It once again underlined that in a limited number of cases, it would allow for *in abstracto* claims. The Court found that the UK IPT provides an effective legal remedy in cases of bulk surveillance, but that because the claimants had sufficient reason to believe it did not, the requirement of the exhaustion of domestic remedies did not apply. The question whether domestic remedies are 'effective' or not thus becomes a subjective instead of an objective criterion.

On the issue of oversight and ex-ante authorisation of surveillance measures the Court departed from its recent case law and after examining the overall UK situation and taking into account 'the pre-authorisation scrutiny of warrant applications, the extensive post-authorisation scrutiny provided by the (independent) Commissioner's office and the IPT, and the imminent changes to the impugned regime' and it did not find a violation of Article 8 ECHR despite the lack of ex-ante authorisation. As the Court does not seem to rely on clear and objective criteria for determining this issue, legal consistency and the foreseeability of its decisions may be undermined when it assesses future situations.

The Court in the *Big Brother Watch and Others v UK* judgment, in line with *Benedik v Slovenia*, as well as the CJEU case law declared that metadata do not deserve lesser protection than content data. This is a clear statement against the claims of law enforcement authorities, and security and intelligence agencies that metadata are not revealing the same richness of information as content data.

The final point of our analysis focused on the issue of intelligence data sharing. The ECtHR acknowledged for the first time the importance of intelligence data sharing. It also stressed that the minimum requirements it has developed for gathering data also apply to sharing the data. Here, it explicitly engaged with the danger of circumventing legal limitations by sharing data with foreign agencies that are not subjected to those rules. What is left unaddressed is the question of oversight over such cross-border sharing of data. Who is responsible for authorising such transfers and who is auditing the conditions for it? This is a challenging issue and it would be interesting to see the Court discussing it in further detail in the future.

As to the content of the arguments of the applicants, the Court seemed in general receptive to

[49] ibid para 446.
[50] *Big Brother Watch and Others v UK* (n 24) Partly concurring, partly dissenting opinion of Judge Koskelo joined by Judge Turković, paras 30-31.

their arguments, underlying the general gist of their application, while at the same time stressing that the problems and dilemmas they raise are not in themselves of such nature that they should be considered a violation of Article 8 ECHR. For example, the existence of 'below the waterline documents' can be problematic in terms of a fair trial, but can be accepted when necessary in the national interest. The Court agreed that it would be preferable for the selection of material by analysts to be subject at the very least to pre-authorisation by a senior operational manager, given that analysts are carefully trained and vetted, records are kept and those records are subject to independent oversight and audit. Nevertheless, the Court also stated that the absence of pre-authorisation does not, in and of itself, amount to a failure to provide adequate safeguards against abuse.

The Court did not condemn bulk interception of communications and mass state surveillance as violating fundamental rights as such. As a response to this fact, the applicants in the *Big Brother Watch and Others v UK*, filed two separate requests for a reference to the Grand Chamber.[51] The Grand Chamber panel of five judges decided on 4 February 2019 to refer *Big Brother Watch and Others v UK* to the Grand Chamber of the European Court of Human Rights. The Grand Chamber will have the opportunity to assess the overall compatibility of the UK bulk surveillance regime with the ECHR and to reflect in detail on the tension points between the judges of the First Section, as presented in their partly concurring and partly dissenting opinions.

[51] *Big Brother Watch and Others*, Applicants' Request for a Reference to the Grand Chamberhttps://www.privacyinternational.org/sites/default/files/2019-01/2018.12.13_BBW_v_UK_Request_for_Referral_to_Grand_Chamber.pdf accessed 28 May 2019; Ten Human Rights Organizations, Request for Referral to the Grand Chamberhttps://privacyinternational.org/sites/default/files/2019-03/2018.12.11_10_HR_Orgs_v_the_UK_-_GC_referral.pdf accessed 28 May 2019.