bB

European Court of Human Rights
Application No. 58170/13
Big Brother Watch and Others v. the United Kingdom
Amsterdam, 9 February 2016

WRITTEN SUBMISSIONS

In the case of Big Brother Watch and Others v. The United Kingdom

On behalf of:

1. Mr. Bart Nooitgedagt;
2. Mr. Brenno de Winter;
3. Mr. Johannes van Beek;
4. Mr. Robbert Gonggrijp;
5. Mr. Mathieu Paapst;
6. The Dutch Association for Criminal Attorneys;
7. The Dutch Association of Journalists;
8. The Internet Society Netherlands;
9. The Privacy First foundation.

Represented by Mr. Chr. A. Alberdingk Thijm, LLM and Ms. C.F.M. de Vries, LLM

bB

Introduction and summary

1. The Dutch Against Plasterk coalition (hereinafter: the "Coalition") is grateful for the opportunity to submit written submissions in the pending case between *Big Brother Watch and Others v. The United Kingdom*. The Coalition consists of five citizens (Mr. Bart Nooitgedagt, Mr. Brenno de Winter, Mr. Johannes van Beek, Mr. Robbert Gonggrijp and Mr. Mathieu Paapst) and four organizations (the Dutch Association for Criminal Attorneys, the Dutch Association of Journalists, the Internet Society Netherlands, and the Privacy First Foundation). Each member of the Coalition has a special interest in resisting mass surveillance practices such as those revealed by Edward Snowden and has reason to believe that they could be the subject of interception by foreign intelligence services, such as the National Security Agency (the "NSA") and the Government Communications Headquarters ("GCHQ").

2. The Coalition are plaintiffs in a proceeding on the merits against the State of the Netherlands initiated in November 2013 (the "Dutch case"). The Dutch State has recognized that collections of data are exchanged with foreign intelligence partners and also that it cannot be excluded that the Dutch State in the course hereof receives information acquired by foreign services while using methods that unlawfully infringe fundamental rights. In these proceedings, the Coalition demands that the Dutch government stops using data which is, or might have been, illegally obtained by foreign intelligence agencies. Moreover, the Coalition claims that the Dutch State should take steps to actively protect the right to privacy of its citizens. The District Court of The Hague rendered a judgment in first instance on 23 July 2014.[1]

3. The District Court of The Hague ruled, in short, that the Dutch intelligence agencies, the General Intelligence and Security Service ("AIVD") and the Defense Intelligence and Security Service ("MIVD"), may proceed with the current manner of cooperation with foreign agencies and the exchange of data that comes with it, even if this cooperation is merely based on "trust". According to the District Court, the important interest of national security is decisive in this regard.

4. The District Court held, in short, that the right to privacy, protected under Article 8 of the European Convention of Human Rights ("ECHR"), carries less weight when international cooperation between intelligence agencies is involved. According to the District Court, the requirement that any interference with the exercise of the right to privacy must be "in accordance with the law", as provided in Article 8 paragraph 2 ECHR, should be interpreted less strictly in such a situation. Moreover, according to the District Court, less safeguards are required when the receipt of bulk data from foreign services is involved, as this data has not yet been assessed on relevance.

5. The Coalition does not agree with the (far-reaching) judgment of the District Court. The judgment implies that as soon as a data transfer bears the stamp of "national security", the rule of law should give way. The Coalition is of the opinion, to the contrary, that *particularly* when secret surveillance measures are concerned, it is essential that adequate safeguards are set out in law in order to avoid abuses of power, as such measures are not open to scrutiny by the

[1] District Court of The Hague 23 July 2014, ECLI:NL:RBDHA:2014:8966.

individuals concerned nor by the public at large. The Coalition lodged an appeal to the Court of Appeal in The Hague, where the case is currently pending. The Coalition submitted its statement on appeal on 2 February 2016.[2]

6. This intervention addresses the important question of whether a Member State, in the course of international cooperation between intelligence authorities, is permitted to receive (either solicited or unsolicited) and use data obtained from a foreign intelligence partner that might not have been collected legally. The Coalition is of the opinion that the present case offers the European Court of Human Rights (hereinafter: "the Court") an opportunity to prolong its existing case-law and to apply the principles contained therein to this situation as well.

7. The Coalition does not contest the necessity and importance of (transatlantic) cooperation between intelligence services as such. It is, however, of the opinion that the authority to receive and use data obtained from foreign intelligence partners should be subject to adequate and effective guarantees against abuse, as the Court also requires for other kinds of secret measures of surveillance. The Snowden-revelations concerning the activities of intelligence services, in particular those of the NSA and the GCHQ, make it clear that "trust" cannot form a sufficient basis (if it ever was) for the exchanging of data with foreign intelligence services. The revelations have shown that the NSA and the GCHQ, on a mass and undifferentiated basis, collect and have access to the personal data of – essentially – everyone. Much of Edward Snowden's revelations are not in dispute.[3]

8. In the pending application before the Court, Big Brother Watch argues, *inter alia*, that the receipt of foreign – possibly illegally generated – material by the United Kingdom is not "in accordance with the law". This claim is identical to the claim of the Coalition in the Dutch case. The Coalition endorses the position of Big Brother Watch,[4] that the information-sharing between intelligence services and the receipt and use of vast quantities of data that was captured by foreign authorities as a part thereof, is only permitted if such an authority has a sound legal basis and is provided with sufficient safeguards. The Coalition requests the Court to make a decision especially with regard to this aspect, also with a view to process efficiency.

9. If it were otherwise, the authority to receive and use data via foreign intelligence partners, would result in a circumvention – and undermining – of the high level of protection of the right to privacy guaranteed by Article 8 ECHR, or the "laundering" of illegal data. This is true because the data received was obtained by foreign agencies based on authorities that – we know now – make no differentiation whatsoever and contain no (significant) safeguards, and that are much broader than the national laws would permit. As a consequence, a State obtains data that it would never have been allowed to collect based on its own national laws. The European Court of Justice ("CJEU") has recently emphasized in its *Schrems*-judgment that such circumvention is impermissible and results in a violation of Articles 7 and 8 of the Charter of Fundamental Rights of the EU ("the Charter").[5]

[2] See (in Dutch) http://www.bureaubrandeis.com/burgers-tegen-plasterk-formuleert-grieven-tegen-vonnis-rechtbank/.
[3] Opinion of Advocate General Bot, delivered on 23 September 2015, case C-362/14 (*Schrems*).
[4] Par. 4.1 and 6.1 of the Application.
[5] CJEU 6 October 2016, case C-362/14 (*Schrems*).

10. Moreover, the Coalition is of the opinion that the signatories to the ECHR have a positive obligation to actively take measures to protect the fundamental right to privacy of its citizens. Such a positive obligation is not compatible with simply accepting foreign intercept material while hiding behind the "modus operandi" of intelligence services, as the Dutch State does.

International cooperation and data transfers should be "in accordance with the law"

11. The right to privacy is protected by Article 8 ECHR and Article 7 and 8 of the ("the Charter").

12. It is established case law that the collecting and processing of personal data amounts to an interference with Article 8 ECHR,[6] as does the storage of personal data in secret government databases.[7] Metadata, or traffic data, that provides information about a communication, also falls under the scope of Article 8 ECHR.[8] In fact, the Court has repeatedly emphasized that the mere existence of legislation permitting secret measures amounts in itself to an interference with Article 8 ECHR.[9]

13. In the case *Weber and Saravia*, the Court held that the cooperation between intelligence agencies and the transmission of data as a part thereof, constitutes a separate interference with the right under Article 8 ECHR and must comply with the requirements set out in paragraph 2.

> *Furthermore, the Court, like the Federal Constitutional Court, takes the view that the transmission of data to and their use by other authorities, which enlarges the group of persons with knowledge of the personal data intercepted and can lead to investigations being instituted against the persons concerned, constitutes a further separate interference with the applicants' rights under Article 8* [...].[10]

14. Pursuant to paragraph 2 of Article 8 ECHR, any interference with the exercise of the right to privacy can only be justified when such interference is in accordance with the law and necessary in a democratic society in the interest of, *inter alia*, national security.[11]

Case law of the Court

15. From the Court's established case law on secret measures of surveillance, it follows that the wording "in accordance with the law" requires that the law that forms the basis of the measure must be adequately accessible to the persons concerned and foreseeable as to its effects.[12]

[6] ECHR 2 August 1984, no. 8691/79 (*Malone/UK*), par. 84.
[7] ECHR 24 May 2011, nos. 33810/07 and 18817/08 (*Association "21 Decembre 1989" a.o/Romania*), par. 115.
[8] ECHR 24 May 2011, nos. 33810/07 and 18817/08 (*Association "21 Decembre 1989" a.o/Romania*).
[9] ECHR 29 June 2006, no. 54934/00 (*Weber & Saravia*), par. 78; in reference to ECHR 6 September 1978, no. 5029/71 (*Klass/Germany*), par. 41; ECHR 2 August 1984, no. 8691/79 (*Malone/UK*), par. 64.
[10] ECHR 29 June 2006, no. 54934/00 (*Weber & Saravia*), par. 77.
[11] Art. 52 of the Charter contains the following clause: "Any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others." The Charter incorporates the ECHR and the jurisprudence of the Court in full.
[12] ECHR 26 April 1979, no. 6538/74 (*Sunday Times*), par. 49; see also ECHR 4 May 2000, no. 28341/95 (*Rotaru/Romania*), par. 52; ECHR 4 December 2008, nos. 30562/04 and 30566/04 (*S. and Marper/UK),* par. 95; ECHR 18 May 2010, no. 26839/05 (*Kennedy/UK*), par. 151.

16. Although foreseeability in the context of secret measures of surveillance cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly, the Court has consistently emphasized that especially when secret powers are concerned, it is essential that there exist adequate and effective guarantees against abuse.[13] This is true because, according to the Court, "especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident."[14] Secret surveillance measures of intelligence agencies are not subjected to democratic control and precisely for that reason it is essential that the domestic law is sufficiently clear in its terms as to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measure.[15]

17. Moreover, the Court has repeatedly held that "it would be contrary to the rule of law for the discretion granted to the executive or to a judge to be expressed in terms of an unfettered power."[16] The law must therefore indicate the scope of the discretion on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.[17]

18. According to the Court, the need for safeguards is all the greater now the technology is continually becoming more sophisticated.[18] The same is true where the protection of personal data undergoing automatic processing is concerned.[19] In its case law, the Court thus explicitly takes into account the fact that recent technological developments mean that the State's capacity to capture, store and use private communications is greater than ever before.

> *In the face of this progress the Court must scrutinize the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanies by a simultaneous development of legal safeguards securing respect for citizens' Convention rights.*[20]

19. In its recent case law, the Court also explicitly refers to the relevant case law of the CJEU to emphasize the importance of safeguards.[21] In *Digital Ireland* the CJEU, under reference to the Court's case law, stresses the need for clear and precise rules governing the scope and

[13] See, among other decisions, ECHR 6 September 1978 (*Klass/Germany*), 5029/71, par. 49: "The Court must be satisfied that, whatever system is adopted, there exist adequate and effective guarantees against abuse".
[14] ECHR 12 January 2016, no. 37138/4 (*Szabó & Vissy/Hungary*), par. 62; ECHR 4 December 2015, no. 47143/06 (*Roman Zakharov/Russia*), par. 229.
[15] ECHR 2 August 1984 (*Malone/UK*), no. 8691/79, par. 67; ECHR 26 March 1987, no. 9248/81 (*Leander/Sweden*), par. 51; ECHR 24 April 1990, nos. 11801/85 and 11105/84 (*Huvig/France*), par. 29; ECHR 30 July 1998, no. 27671/95 (*Valenzuela Contreras/Spain*), par. 46; ECHR 4 May 2000, no. 28341/95 (*Rotaru/Romania*), par. 55; ECHR 29 June 2006, no. 54934/00 (*Weber & Saravia*), par. 93; ECHR 28 June 2007, no. 6250/00 (*Association for European Integration and Human Rights and Ekimdzhiev/Bulgaria*), par. 75.
[16] ECHR 2 August 1984, no. 8691/79 (*Malone/UK*), par. 68; ECHR 26 March 1987, no. 9248/81 (*Leander/Sweden*), par. 51; ECHR 24 April 1990, nos. 11801/85 and 11105/84 (*Huvig/France*), par. 29; ECHR 29 June 2006, no. 54934/00 (*Weber & Saravia*), par. 94.
[17] ECHR 4 December 2015, no. 47143/06 (*Roman Zakharov/Russia*), par. 230; under reference to: ECHR 2 August 1984, no. 8691/79 (*Malone/UK*), par. 68; ECHR 26 March 1987, no. 9248/81 (*Leander/Sweden*), par. 51; ECHR 24 April 1990, nos. 11801/85 and 11105/84 (*Huvig/France*), par. 29; ECHR 29 June 2006 (*Weber & Saravia*), no. 54934/00, par. 94.
[18] ECHR 29 June 2006, no. 54934/00 (*Weber & Saravia*), par. 93; ECHR 25 March 1998, no. 23224/94 (*Kopp/Zwitserland*), par. 72; ECHR 30 July 1998, no. 27671/95 (*Valenzuela Contreras/Spain*), par. 46.
[19] ECHR 4 December 2008, nos. 30562/04 and 30566/04 (*S. and Marper/UK),* par. 103; ECHR 18 October 2011, no. 16188/07 (*Khelili/Zwitserland*), par. 62.
[20] ECHR 12 January 2016, no. 37138/4 (*Szabó & Vissy/Hungary*), par. 68.
[21] ECHR 4 December 2015, no. 47143/06 (*Roman Zakharov/Russia*), par. 147; ECHR 12 January 2016, no. 37138/4 (*Szabó & Vissy/Hungary*), par. 23, 68, 70 and 73.

application of a measure, as well as the need for safeguards against abuse, especially when the automatic processing of data is concerned.[22] In the subsequent *Schrems*-case, which nota bene concerned the transfer of personal data between the EU and the US, the CJEU confirmed that legislation involving interferences with the right to privacy must "lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the persons whose personal data is concerned have sufficient guarantees enabling their data to be effectively protected against the risk of abuse and against any unlawful access and use of that data."[23]

20. In the case *Weber and Saravia*, which concerned the recording of telecommunications, the Court formulated the following minimum safeguards that should be set out in statute law to avoid abuse of power: (i) the nature of the offences which may give rise to an interception order; (ii) a definition of the categories of people liable to have their telephones tapped; (iii) a limit on the duration of telephone tapping; (iv) the procedure to be followed for examining, using and storing the data obtained; (v) the precautions to be taken when communicating the data to other parties; and (vi) the circumstances in which recordings may or must be erased or the tapes destroyed.[24]

21. In *Liberty,* the Court ruled that, whereas the *Weber*-requirements were first developed in connection with measures of surveillance targeted at specific individuals, there is not any ground to apply different principles to more general programs of surveillance.[25]

22. The *Weber*-minimum safeguards are consistently repeated and applied in the Court's case law regarding secret measures.[26] In later jurisprudence, the requirements are summarized as follows:

> *[B]ecause of the lack of public scrutiny and the risk of abuse intrinsic to any system of secret surveillance, the following minimum safeguards should be set out in statute law to avoid abuses: the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law.*[27]

Application to the authority to exchange data between intelligence services

23. From the above it follows that safeguards are essential to protect citizens against abuse particularly when legislation set up to protect national security is involved.

24. The Coalition is of the opinion that the legal framework described above – and thus the same minimum safeguards – should be applied to the authority of national intelligence agencies to receive and use large amounts of data collected by foreign intelligence agencies.

[22] CJEU 8 April 2014, case C-293/12 (*Digital Rights Ireland*), par 54-55.
[23] CJEU 6 October 2015, case C-362/14 (*Schrems*), par. 91.
[24] ECHR 29 June 2006, no. 54934/00 (*Weber & Saravia*), par. 95.
[25] ECHR 1 July 2008, no. 58243/00 (*Liberty*), par. 63.
[26] See, *inter alia*, ECHR 4 December 2015, no. 47143/06 (*Roman Zakharov/Russia*); ECHR 21 June 2011, no. 30194/09 (*Shimovolos/Russia*); ECHR 2 December 2010, no. 35623/05 (*Uzun/Germany*); ECHR 4 December 2008, nos. 30562/04 and 30566/04 (S. *and Marper/UK*); ECHR 30 January 2008, no. 62540/00 (*Association for European Integration and Human Rights/Bulgaria*); ECHR 3 July 2007, no. 62617/00 (*Copland/UK*).
[27] See, for example, ECHR 21 June 2011, no. 34869/05 (*Shimovolos/Russia*), par. 68.

25. The Coalition fails to see why – as the District Court in the Dutch case has ruled – in such a situation a less strict regime would apply, as the power to receive foreign intercept material is undisputedly an important source of intelligence gathering and could easily lead to a circumvention of the level op privacy-protection guaranteed under national laws.

26. The need for safeguards is all the greater now that we have learned from Snowden's disclosures that the United States authorities engage in a mass and indiscriminate surveillance and interception of data that is not in line with the level op protection of fundamental rights in the European Union, making it very plausible that national agencies indeed receive data that was illegally collected.

27. In the Dutch case, the District Court found of relevance that the information-sharing in the course international cooperation allegedly only concerned collections of "raw" "bulk" data (consisting of both content and metadata). The District Court suggests that this leads to a less severe infringement of the right to privacy and therefore justifies a less strict regime. The Coalition is of the opinion that the opposite is true. If anything, the fact that the exchange of massive, indiscriminate bulk data is concerned, only underlines the necessity for strict safeguards.

28. This also follows from the Court's jurisprudence, in which it is emphasized that the greater the scope and the amount of data collected, the more important the content of the safeguards becomes.[28] In the case *Szabó* the Court held that it could not be ruled out that the national legislation in question could be taken to enable "strategic, large-scale interception", which according to the Court was "a matter of serious concern".[29]

29. Not only the Court, but also the CJEU stresses that the severity of the breach of the right to privacy increases when the collection of large, undifferentiated data is concerned, as this by definition also affects innocent persons.[30]

> *Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its use.*[31]

30. It is for the same reason that the Council of Europe Commissioner for Human Rights in its issue paper "Democratic and effective oversight of national security services" advocates that

[28] ECHR 13 November 2012, no. 24029/07 (*M.M/UK*), par. 200; see also ECHR 18 May 2010, no. 26839/05 (*Kennedy/UK*), par. 160 and 162.
[29] ECHR 12 January 2016, no. 37138/4 (*Szabó & Vissy/Hungary*), par. 69.
[30] CJEU 8 April 2014, case C-293/12 (*Digital Rights Ireland*), par. 58.
[31] CJEU 6 October 2015, case C-362/14 (*Schrems*), par. 93; CJEU 8 April 2014, case C-293/12 (*Digital Rights Ireland*), par. 57-61.

independent *ex ante* authorization should be extended to untargeted bulk collection of information.[32]

31. For the reasons above, the Coalition is of the opinion that national legislation allowing for the receipt of (bulk) data from foreign intelligence agencies must be sufficiently clear in its terms as to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to such power. Moreover, there must be safeguards in place, both in relation to the circumstances in which a state can *receive* data collected by foreign intelligence agencies as well as the subsequent *use* thereof.

32. In the Dutch case, the Coalition argues that Article 59 of the Dutch Intelligence and Security Services Act 2002 does not meet this threshold. To the contrary, the Article merely speaks of a duty of the Dutch services to "maintain relations" with intelligence and/or security services in other countries. It does not even mention the authority to receive intelligence from foreign services, let alone that it provides for any safeguards in this regard.

33. Mere "trust" in foreign agencies cannot form a sufficient basis for the exchange of vast quantities of data between states. That is also the conclusion of the Dutch Review Committee on the Intelligence and Security Services (the "CTIVD"). In its review report of 5 February 2014 the CTIVD concludes that it is desirable to verify whether the trust in foreign services is still justified.

> *In the close cooperation relationships investigated by the Committee, GISS and DISS generally trust that the foreign services respect human rights and act within the parameters of their own national laws and regulations, unless they have evidence to the contrary. The recent revelations can be considered to be such evidence and make it desirable to verify whether the trust is still justified.*[33]

34. In the same report, the CTIVD concludes that "the services must refrain from using data received from foreign services if there are concrete indications that the data was acquired in a manner which by Dutch criteria constitutes unlawful infringement of privacy or of another fundamental or human right".[34] This is precisely what the Coalition has been arguing in the Dutch case.

States have a positive obligation to protect their citizens privacy

35. It follows from the foregoing that the UK and Dutch provisions allowing for the exchange of data without sufficient safeguards, are not in accordance with the law. Moreover, the Coalition is of the opinion that signatories to the ECHR have a positive obligation to protect its citizens privacy

[32] Issue paper published by the Council of Europe Commissioner for Human Rights, *Democratic and effective oversight of national security services*, May 2015, p. 24 (the report can be found at: www.commissioner.coe.int).
[33] Review Report on the processing of telecommunications data by GISS and DISS, 5 February 2014, CTIVD no. 38, p. x, 29 (the report can be found at: http://english.ctivd.nl/investigations/r/review-report-38/documents/review-reports/2014/03/11/review-report-38-on-the-processing-of-telecommunications-data-by-giss-and-diss).
[34] Review Report on the processing of telecommunications data by GISS and DISS, 5 February 2014, CTIVD no. 38, p. ix, 30 (the report can be found at: http://english.ctivd.nl/investigations/r/review-report-38/documents/review-reports/2014/03/11/review-report-38-on-the-processing-of-telecommunications-data-by-giss-and-diss)

and cannot disregard the fact that there is a strong likelihood that data received from foreign intelligence services is collected unlawfully.

36. It is generally accepted that "although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference. In addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private and family life".[35]

37. The Court has accepted the existence of such positive obligations in the context of Article 8 ECHR in a number of cases.[36] According to the Court, the applicable principles between a State's negative and positive obligations are similar. In both instances "regard must be had to the fair balance that has to be struck between the competing interests."[37]

38. The Coalition is of the opinion that there is urgent cause for Member States to adopt measures designed to secure respect for the right to privacy in the course of international cooperation between intelligence agencies and the exchange of data as a part thereof. The Snowden revelations have exposed that foreign intelligence services collect data on a scale and by means of methods that unlawfully infringe fundamental rights. In fact, the CJEU has already ruled that the activities of the NSA go beyond what is strictly necessary and proportionate to the protection of national security.[38]

39. Under such circumstances, the receiving state cannot stand by and do nothing. To the contrary, the receiving State is under a duty to verify whether the data received was collected lawfully. If it were otherwise, this would give the receiving State a blanket license to collect illegal data via foreign partners and to "launder" such data, thereby circumventing the safeguards provided in national (and European) law. This is also rightly observed by Big Brother Watch is its application.[39]

40. It is precisely for this reason that the European Parliament called on Member States to fulfil their positive obligation in a resolution on electronic mass surveillance:

> *Calls on the Member States immediately to fulfil their positive obligation under the European Convention on Human Rights to protect their citizens from surveillance contrary to its requirements, including when the aim thereof is to safeguard national security, undertaken by third states or by their own intelligence services, and to*

[35] ECHR 4 December 2007, no. 44362/04 (*Dickson/The United Kingdom*), par. 70; ECHR 15 March 2012, nos. 4149/04 and 41029/04 (*Aksu/Turkey*), par. 50; ECHR 5 April 2005, no. 71099/01 (*Monory /Romania and Hungary*).
[36] ECHR 26 March 1985, no. 8978/80 (*X & Y/ The Netherlands*); ECHR 9 October 2012, no. 42811/06 (*Alkaya/Turkey*); ECHR 5 October 2010, no. 420/07 (*Köpke/Germany*).
[37] ECHR 4 December 2007, no. 44362/04 (*Dickson/The United Kingdom*), par. 70.
[38] CJEU 6 October 2015, case C-362/14 (*Schrems*), par. 90-93. The United Nations Human Rights Committee has also expressed serious concerns regarding the activities of the NSA and GCHQ, that – according to the Committee – fail to effectively protect the rights of the persons affected. See: United Nations Human Rights Committee, Concluding observations on the fourh periodic report of the United States of America, 23 April 2014, CCPR/C/USA/CO/04, par. 22 and United Nations Human Rights Committee, Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland, 17 augustus 2015, CCPR/C/GBR/CO/7, par. 24.
[39] Application no. 124, 130-131.

ensure that the rule of law is not weakened as a result of extraterritorial application of a third country's law.[40]

41. The Coalition is of the opinion that a State cannot hide behind the "modus operandi" of intelligence services, that it is generally not customary in international dealings between intelligence and security services to ask the foreign service about the source or method used to collect data. The Dutch State relies heavily on this argument in the Dutch case. The Coalition argues that this "modus operandi", however, does not provide the Dutch State with an unlimited and absolute privilege and cannot justify the use of data that was acquired by foreign services while using a method which unlawfully infringes fundamental rights.

42. This is also the opinion of the European Parliament. In a resolution adopted on 12 March 2014, it states that "whereas the fact that a certain level of secrecy is conceded to intelligence services in order to avoid endangering ongoing operations, revealing "modi operandi" or putting at risk the lives of agents, such secrecy cannot override or exclude rules on democratic and judicial scrutiny and examination of their activities, as well as on transparency, notably in relation to the respect of fundamental rights and the rule of law, all of which are cornerstones in a democratic society."[41]

43. In the Dutch case, the Coalition has argued that the Dutch State wrongly embraces a "black and white" approach, suggesting that it is either revealing all sources and methods, or none at all. In reality, however, one can conceive many degrees in which intelligence partners provide openness as to their sources. The question of whether sources and/or methods can be revealed, depends of course to a great extent on the *type* of source and the *type* of method used. It seems obvious, for example, that the identity of a natural person that served as a source (human intelligence) should be kept secret, as revealing this information might expose this person to potential risks. Such considerations do not come into play, however, when non-human sources or methodologies are concerned. It is difficult to see why it would not be possible, as a general rule, for a State to ask foreign agencies for a general description of the techniques used to collect data. This is all the more true now that many of the programs used by US and British intelligence agencies are no longer confidential.

44. The Coalition is of the opinion that the Snowden-revelations call for a re-evaluation of the cooperation between intelligence agencies and the acceptance of positive obligations of the receiving state. National intelligence services cannot look on powerlessly, but must actively take steps to protect the right to privacy of its citizens by making inquiries into the technical possibilities and methods used by foreign services. Moreover, a State must periodically review whether the other country ensures an adequate level op protection of fundamental rights. If that is not the case, it is simply not permitted to continue the exchange of information with such foreign authorities on the same foot, according to the CJEU in *Schrems*. The CJEU in that case

[40] *European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*, 2013/2188 (INI).
[41] European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)).

emphasizes that "such a check is required, in any event, when evidence gives rise to a doubt in that regard."[42]

45. The Europe Commissioner for Human Rights stresses in this regard that supervisors should be able to scrutinize information about intelligence cooperation:

> *Access to information arising from and pertaining to international intelligence co-operation merits special consideration. In view of the extensive international co-operation between security services (and the impact that such co-operation can have on human rights) it is essential that overseers are able to scrutinise information about such co-operation, including information that has been received from or sent to foreign bodies.*[43]

46. It cannot be seen how a State can meet this obligation in practice without – to a greater or lesser extent – asking foreign services about the source of method used to collect data.

Conclusion

47. For the reasons explained above, the Coalition submits that the Court should prolong its existing case law to the authority of national intelligence agencies to receive and use data that was captured by foreign authorities, by declaring that such an authority is only "in accordance with the law" if it has a sound legal basis and is provided with sufficient safeguards. Moreover, the Coalition urges the Court to declare that States have a positive obligation to ensure that the level op protection guaranteed by Article 8 ECHR is not circumvented and weakened by means of the exchange of data with foreign intelligence partners.

48. Given the similar nature of the Big Brother Watch-claim, the facts on which it is based, and for the sake of judicial efficiency, the Coalition would be honored to take part in a hearing before the Court and explain their arguments in more detail.

Acting lawyers:
Chr.A. Alberdingk Thijm, LLM and C.F.M. de Vries, LLM
bureau Brandeis
Apollolaan 151 1077 AR Amsterdam The Netherlands
T: +31 20 7606 505 / F: +31 20 7 606 555
info@bureaubrandeis.com / bureaubrandeis.com

[42] CJEU 6 October 2015, case C-362/14 (*Schrems*), par. 76-77.
[43] Issue paper published by the Council of Europe Commissioner for Human Rights, *Democratic and effective oversight of national security services*, May 2015, p. 64.