ENNHRI European Network of National Human Rights Institutions

Third Party Intervention
in the European Court of Human Rights

Big Brother Watch and Others v. the United Kingdom (Application Nos. 58170/13, 62322/14 and 24960/15)

Written submissions of the European Network of National Human Rights Institutions

1. These written observations are prepared and submitted by the European Network of National Human Rights Institutions (ENNHRI), pursuant to leave granted by the President of the Grand Chamber of the European Court of Human Rights (ECtHR) on 3 April 2019 in accordance with rule 44 (3) of the Rules of the Court. ENNHRI is a registered association representing National Human Rights Institutions (NHRIs) within the Council of Europe region. Its membership currently comprises 44 NHRIs from 40 countries across wider Europe of which 37 are accredited with 'A' or 'B' status under the United Nations 'Paris Principles'. As NHRIs, ENNHRI members are institutions independent from both government and civil society organisations with a broad constitutional or legal mandate to promote and protect human rights. Many NHRIs have, as part of their statutory functions, the ability to appear as *amicus curiae* in human rights cases before national, regional and/or international courts and tribunals in cases concerning constitutional and international human rights provisions. In this capacity NHRIs regularly appear before the European Court of Human Rights as neutral parties providing expertise on human rights matters which the parties may not put before the Court.

Summary

2. For the first time the case *Big Brother Watch and Others v. the United Kingdom* brings the question if a regime of international intelligence sharing is compliant with Article 8 ECHR to the attention of the Grand Chamber. In this submission, ENNHRI provides examples from member states showing that the nature of international intelligence cooperation has changed significantly so that it has become increasingly difficult to differentiate between "solicited" and "unsolicited" data which poses new challenges for independent and effective oversight of intelligence sharing. Secondly, the submission provides an overview of recommendations from UN and European human rights bodies and special procedures as well as good practice by national oversight bodies on how these challenges should and may be addressed to ensure (in legal, organisational and technical terms) robust and effective independent oversight of intelligence sharing.

3. These submissions do not address the facts or merits of the case.

4. It is established that, in interpreting ECHR provisions and the scope of the States' obligations in specific cases, the European Court of Human Rights will look "for any consensus and common values emerging from the practices of European States and specialised international instruments [...] as well as giving heed to the evolution of norms and principles in international law." [1]

Changes in international intelligence cooperation

5. International intelligence cooperation is nothing new as demonstrated by the long-standing close "Five Eyes" alliance among intelligence services from the United States, the United Kingdom, Canada, Australia and New Zealand dating back to 1947.[2] With globalisation it is, however, now seen as imperative by most intelligence and security services to maintain extensive networks of contacts with partner agencies across the globe. In 2009, the head of the French foreign intelligence service DGSE, for example, publicly reported established contacts with more than 200 intelligence and security services in other countries.[3] In 2019, the German foreign intelligence service BND reported contacts with 450 intelligence services in 160 countries.[4] Seconded experts or liaison officers from national intelligence services meet and work together at international organisations such as the EU and the NATO, or at the operational platform of the Counter Terrorism Group, an informal network of domestic intelligence services from 30 European countries, that was established in 2016/17 to host meetings for face-to-face exchange of information on (alleged) foreign terrorist fighters.[5]

6. For many years, international intelligence sharing involved the transfer of evaluated data ("finished intelligence") in response to a request for specific information. The advent of new technologies has changed the nature of intelligence sharing significantly. Unevaluated "raw" data are increasingly exchanged by automated means in the context of signals intelligence (SIGINT) cooperations or through international intelligence databases. The independent Dutch intelligence oversight body CTIVD reported in 2016 that the two Dutch intelligence services AIVD and MIVD "exchange unevaluated data on a structural basis with foreign intelligence and security services within five topically or geographically oriented cooperative partnerships", authorised by the responsible ministers for an indefinite period.[6] In

---

[1] European Court of Human Rights (2009): Opuz v Turkey, Judgement of 9 June 2009. Application No. 33401/02, para. 164.

[2] Born, Hans; Leigh, Ian; Wills, Aidan (2015): Making international intelligence cooperation accountable. Geneva: Centre for the Democratic Control of Armed Forces, p. 27.

[3] "Les mutations du renseignement extèrieur français", interview with DGSE director Erard Corbin de Mangoux, *Questions internationals*, No. 35, January-February 2009, pp. 29-33.

[4] BND, Kooperationen, https://www.bnd.bund.de/DE/Die_Arbeit/Kooperationen/kooperationen_node.html. (accessed at 25 April 2019).

[5] Dutch Review Committee on the Intelligence and Security Services (CTIVD) (2018): The multilateral exchange of data on (alleged) jihadists by the AIVD (CTIVD Review Report, 56), p.10. Online: https://english.ctivd.nl/binaries/ctivd-eng/documents/review-reports/2018/04/24/index/CTIVD+Review+report+NO56.pdf (accessed at 26 April 2019).

[6] Dutch Review Committee on the Intelligence and Security Services (CTIVD) (2016): Review Report on the exchange of unevaluated data by the AIVD and the MIVD. Investigation into the execution of Dutch House of Representative motion no. 96,

Germany, the investigation of the cooperation between the German foreign intelligence service BND and the US National Security Agency (NSA) by an ad hoc committee of the parliament found that in the course of the so-called Joint SIGINT Activity, which was one cooperation project among several others, that was operated at Bad Aiblingen from 2004 to 2012, an estimated number of 14 million selectors (e.g. email addresses, phone numbers or IP addresses) were fed by the NSA to the automated filter programmes jointly used to sift and analyse international communication collected through bulk interception by the BND. Eventually the operation was stopped as around 40,000 of the NSA selectors were found to violate the Memorandum of Agreement regulating the cooperation by targeting persons and institutions whom the German government did not wish to be intercepted and their communication automatically forwarded to the United States for legal or political reasons.[7] In 2016, the BND Act was amended to explicitly authorise such automated joint SIGINT projects with foreign partners and provide for some form of regulation and oversight.[8] Also regulated was the establishment of international intelligence databases used to automatically share personal information for purposes such as counterterrorism or cybersecurity.[9] A known example for such a form of electronic collaboration is the joint database on (alleged) jihadists of the above-mentioned Counter Terrorism Group that was established in 2016/17 without any written agreement and which is operated by the Dutch intelligence service AIVD in its headquarter near The Hague.[10]

7. The changing nature of intelligence sharing, illustrated by these selected examples, makes it increasingly difficult to differentiate between "solicited" and "unsolicited" data. Even if a written agreement governs a bilateral or multilateral intelligence cooperation the advent of automation and big data makes it much more challenging to evaluate what kind of information one party receives from the other party, including whether the information exchanged remains within the parameters of the original intelligence request.

The call for robust oversight of intelligence sharing

, p.5. Online: https://english.ctivd.nl/binaries/ctivd-eng/documents/review-reports/2016/12/22/index49/CTIVD_Rapport_Tweede+Kamermotie+96_NR49_ENG_LR.pdf (accessed: 26 April 2019).

[7] Deutscher Bundestag (2017): Beschlussfassung und Bericht des 1. Untersuchungsausschusses nach Artikel 44 des Grundgesetzes (Drucksache, 18/12850), 23 June 2017. Online: http://dipbt.bundestag.de/doc/btd/18/128/1812850.pdf (accessed 25 April 2019).

[8] Sections 6-18 of the German Act on the Federal Intelligence Service (*Gesetz über den Bundesnachrichtendienst*). https://www.gesetze-im-internet.de/bndg/BJNR029790990.html.

[9] Sections 26-31 of the German Act on the Federal Intelligence Service.

[10] Dutch Review Committee on the Intelligence and Security Services (CTIVD) (2018): The multilateral exchange of data on (alleged) jihadists by the AIVD (CTIVD Review Report, 56), p.10; Deutscher Bundestag (2016): Geheimhaltung wesentlicher Informationen zu einem als operative Plattform bezeichneten europäischen Geheimdienstzentrum in Den Haag. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Annette Groth, Dr. André Hahn, weiterer Abgeordneter und der Fraktion DIE LINKE (Drucksache 18/9323). 3 August 2016. Online: http://dipbt.bundestag.de/doc/btd/18/093/1809323.pdf (accessed: 26 April 2019)

8. In the light of its changing nature, the potential for international intelligence sharing to violate human rights has become an issue of increasing concern, including for the European Court of Human Rights. In Szabó and Vissy v. Hungary the ECtHR noted: ***"The governments' more and more widespread practice of transferring and sharing amongst themselves intelligence retrieved by virtue of secret surveillance – a practice, whose usefulness in combating international terrorism is, once again, not open to question and which concerns both exchanges between Member States of the Council of Europe and with other jurisdictions – is yet another factor in requiring particular attention when it comes to external supervision and remedial measures."*** [11]

9. At the United Nations level, the General Assembly emphasised very recently *"that States must respect international human rights obligations regarding the right to privacy when they intercept digital communications of individuals and/or collect personal data, when they share or otherwise provide access to data collected through, inter alia, information- and intelligence-sharing agreements and when they require disclosure of personal data from third parties, including private companies"*.[12]

10. Concerns about the lack of sufficient safeguards in regard to international information sharing were explicitly expressed by the Human Rights Committee in its Concluding Observations on the state reports of the United Kingdom (2015),[13] Sweden (2016),[14] New Zealand (2016) [15] and Pakistan (2017).[16] The Committee recommended that the state parties should ensure that robust and independent oversight systems are in place for international intelligence cooperation.

11. The Special Rapporteur for the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, had already raised the issue of international intelligence cooperation in 2009, noting that *"legitimate cooperation often poses accountability problems"*. He therefore recommended: *"Intelligence cooperation must be clearly governed by the law (including human rights safeguards) and by transparent regulations, authorized according to strict routines (with proper "paper trails") and controlled or supervised by parliamentary or expert bodies."* [17]

12. Scheinin's successor, Ben Emmerson, warned in his 2014 report on mass surveillance to the UN General Assembly: *"The absence of laws to regulate information-sharing agreements between States has left the way open for intelligence agencies to enter into classified bilateral and multilateral arrangements that are*

---

[11] European Court of Human Rights (2016): Szabó and Vissy v. Hungary, Judgment of 12 January 2016, Application No. 37138/14, para. 78.

[12] UN Document A/RES/73/179, 17 December 2018.

[13] UN Document CCPR/C/GBR/CO/7, 21 July 2015, para. 24.

[14] UN Document CCPR/C/SWE/CO/7, 23 March 2016, paras. 36-37.

[15] UN Document CCPR/C/NZL/CO/6, 24 March 2016, para. 16.

[16] UN Document CCPR/C/PAK/CO/1, 26 July 2017, paras. 35-36.

[17] UN Document A/HRC/10/3, 4 February 2009, paras. 48 and 70.

beyond the supervision of any independent authority. […] Such practices make the operation of the surveillance regime unforeseeable for those affected by it and are therefore incompatible with article 17 of the Covenant [on Civil and Political Rights]." [18]

13. Scheinin and Emmerson's findings are echoed in the report of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age that was submitted to the Human Rights Council in 2018: *"Governments across the globe routinely share intelligence on individuals outside any legal framework and without adequate oversight. Intelligence-sharing poses the serious risk that a State may use this approach to circumvent domestic legal constraints by relying on others to obtain and then share information. Such a practice would fail the test of lawfulness and may undermine the essence of the right to privacy. The threat to human rights protections is particularly acute where intelligence is shared with States with weak rule of law and/or a history of systematically violating human rights. Intelligence received by one State from another may have been obtained in violation of international law, including through torture and other cruel, inhuman or degrading treatment. The human rights risks posed by intelligence-sharing are heightened by the current lack of transparency, accountability and oversight of intelligence-sharing arrangements."*[19]

14. Most recently, Joseph Cannataci, the Special Rapporteur on the right to privacy, recommended: *"All UN Member States should amend their laws to empower their independent authorities entrusted with oversight of intelligence activities, to specifically and explicitly, oversight of all personal information exchanged between the intelligence agencies of the countries for which they are responsible."* [20]

Limits and good practices of overseeing intelligence cooperation

15. Intelligence oversight is often limited in scope when it comes to international cooperation. Research by the European Union Agency for Fundamental Rights (FRA) found that in 17 of the 28 EU member states oversight bodies have no clear legal mandate to oversee the cooperation of national intelligence or security authorities with foreign partners. In some countries the absence of a specific mandate may be understood as implicit permission for oversight bodies to apply the domestic oversight regime to international cooperation. In other countries lack of a mandate may be utilised to inhibit oversight, in particular by reference to the "third party rule" that specifies – as a dominant principle of international intelligence cooperation – that an agency which has received information or other assets from a foreign

[18] UN Document A/69/397, 23 September 2014, para. 44.

[19] UN Document A/HRC/39/29, 3 August 2018, para. 21.

[20] UN Document A/HRC/40/63, 27 February 2019, para. 48.

partner must not share these with a third party without consent of the originator.[21] In Germany, this prevented, for example, the G 10 Commission, tasked to authorise and oversee the intelligence agencies' interception of communications, to review the above mentioned 40,000 NSA selectors although these were used by the BND in an interception operation authorised by the G 10 Commission. The G 10 Commission failed in an attempt to challenge the German government's denial of access to selectors as the Federal Constitutional Court decided that the G 10 Commission had no legal standing.[22] In other countries such as France or Spain, information originating from foreign services is explicitly excluded by law from the mandate of oversight bodies. According to the FRA study, only four EU Member States provide intelligence oversight bodies with powers unlimited by legal constraints or the "third party rule" to control all matters of international cooperation by their intelligence services.[23]

16. In the light of this situation, several international human rights bodies strongly recommend to ensure that oversight of international intelligence cooperation by independent bodies is neither limited by national law nor the "third party rule":

    a. The compilation of good practices that ensure respect for human rights by intelligence agencies which was drafted by Special Rapporteur Martin Scheinin recommends: *"Independent oversight institutions are able to examine intelligence-sharing arrangements and any information sent by intelligence services to foreign entities."* [24]

    b. The Venice Commission concludes in its report on the democratic oversight of signals intelligence agencies: *"[I]t is important to stress that these [expert oversight bodies] must have unrestricted access to the personal information contained in the signals intelligence agency's databanks if they are to be a meaningful safeguard. The "originator" or third party rule cannot apply to the oversight body. While an expert body in this respect mainly functions to check that the signals intelligence agencies own routines on minimization etc. are functioning correctly, to do this task they must be able to do spot checks and thematic studies of the actual data. Thus, they must*

[21] European Union Agency for Fundamental Rights (2017): Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update. Luxembourg: Publications Office of the European Union, pp. 104-106. Online: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf (accessed: 25 April 2019)

[22] Bundesverfassungsgericht (German Federal Constitutional Court), Decision of 20 September 2016, 2 BvE 5/15.

[23] European Union Agency for Fundamental Rights (2017): Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update. Luxembourg: Publications Office of the European Union, p. 105.

[24] Scheinin, Martin (2010): Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight. Human Rights Council. UN Document A/HRC/14/46. 17 May 2010, Practice 34.

have their own, residual, investigative capability, preferably (as with the Dutch and Swedish oversight bodies) having direct access to databanks holding personal information."[25]

c. The Commissioner for Human Rights of the Council of Europe (CoE) calls on the member states to: *"Mandate oversight bodies to scrutinise the human rights compliance of security service co-operation with foreign bodies, including co-operation through the exchange of information, joint operations and the provision of equipment and training. External oversight of security service co-operation with foreign bodies should include but not be limited to examining: a. ministerial directives and internal regulations relating to international intelligence co-operation; b. human rights risk assessment and risk-management processes relating to relationships with specific foreign security services and to specific instances of operational co-operation; c. outgoing personal data and any caveats (conditions) attached thereto; d. security service requests made to foreign partners: (i) for information on specific persons; and (ii) to place specific persons under surveillance; e. intelligence co-operation agreements; f. joint surveillance operations and programmes undertaken with foreign partners. […] Ensure that access to information by oversight bodies is not restricted by or subject to the third party rule or the principle of originator control. This is essential for ensuring that democratic oversight is not subject to an effective veto by foreign bodies that have shared information with security services."* [26]

d. Joseph Cannataci, Special Rapporteur for the right to privacy, details his recommendation, mentioned in paragraph 14 above, on the oversight of intelligence sharing as follows: *"(b) Whenever possible and appropriate, the independent oversight authorities of both the transmitting and the receiving States should have immediate and automated access to the personal data exchanged between the intelligence services and/or law enforcement agencies of their respective States; (c) All UN Member States should amend their legislation to specifically empower their national and state Intelligence Oversight Authorities to have the legal authority to share information, consult and discuss best oversight practices with the Oversight Authorities of those States to which personal data has been transmitted or otherwise exchanged by the intelligence agencies of their respective States; (d) When an intelligence agency transmits intelligence analysis containing personal information or other forms of personal data received from another State to a third State or group of States, this latter exchange should be subject to those States' intelligence oversight authorities."* [27]

---

[25] Venice Commission (2015): Update of the 2007 report on the democratic oversight of the security services and report on the democratic oversight of signals intelligence agencies. Adopted by the Venice Commission at its 102nd Plenary Session (Venice, 20-21 March 2015) on the basis of comments by Mr Iain Cameron (Member, Sweden). CDL-AD(2015)006. Council of Europe. Strasbourg (Study), para. 136.

[26] Commissioner for Human Rights (2015): Democratic and effective oversight of national security services. CommDH/IssuePaper(2015)2. Prepared by Aidan Wills. Strasbourg; Council of Europe, pp. 12-13.

[27] UN Document A/HRC/40/63, 27 February 2019, para. 38.

17. Special Rapporteur Cannataci, thus, also addresses a further barrier to effective oversight of intelligence cooperation, even in those countries where the responsible bodies have full powers to access information and other assets transferred from abroad – namely walls of secrecy that hinder the exchange of information between oversight bodies about classified matters. Such walls of secrecy may also undermine effective oversight of international intelligence cooperation within the boundaries of a national jurisdiction, if, for example, oversight is fragmented and complementary competencies are allocated to different bodies.

18. To overcome at least some of the problems related to walls of secrecy that separate oversight bodies, some of them have started to conduct joint investigations. Within the limits of their mandate, oversight bodies from Belgium, Denmark, the Netherlands, Norway and Switzerland have launched a review of their intelligence services' exchange on (alleged) jihadists in 2016 in response to the new model of intelligence cooperation signalled by the joint international database of the Counter Terrorism Group. In their joint statement the oversight bodies explain their approach: *"We conducted the national investigations more or less at the same time, each from our national context and within the framework of our national mandate. We have met regularly to compare investigation methods, interpret legal frameworks, discuss legal and practical problems and to collate our findings and conclusions. Classified information was not exchanged."*[28] The reasoning behind the initiative is summarised as following: *"Where intelligence and security services cross national borders, oversight bodies cannot. Oversight is limited to national mandates. This reflects one side of data exchange: either oversight will focus on the provision of data and its prior collection, or it will focus on the reception of data and its use. National oversight bodies will not independently be able to acquire a full picture of personal data exchange, let alone review the lawfulness of the entire process of exchange. Such a limit to national oversight does not necessarily constitute an oversight gap. When oversight is exhaustive and effective on both sides of the border, no gap exists between the mandates of the oversight bodies. However, when it comes to cooperation between intelligence and security services - predominantly multilateral cooperation - the cooperation of oversight bodies is only as strong as its weakest link."* [29]

19. Preceding Special Rapporteur Cannataci, the group of oversight bodies outlines their future vision as follows: *"In order for oversight bodies to keep up with developments in international cooperation between intelligence and security services, we need to do just that: intensify our cooperation. A valuable and necessary step towards closer cooperation is to minimize secrecy when sharing information between oversight bodies. At the minimum, oversight bodies could be able to discuss concrete bilateral and multilateral cooperative arrangements between the intelligence and security services they oversee. A logical*

[28] Belgian Standing Intelligence Agencies Review Committee; Danish Intelligence Oversight Board; Dutch Review Committee on the Intelligence and Security Services (CTIVD); The Norwegian Parliamentary Intelligence Oversight Committee (EOS Committee); Swiss Independent Oversight Authority for Intelligence Activities (2018): Strengthening oversight of international data exchange between intelligence and security services. Joint statement. 14 November 2018. Online: https://english.ctivd.nl/binaries/ctivd-eng/documents/publications/2018/11/14/index/Joint+Statement_for+publication+20181114_final.pdf (accessed: 26 April 2019).

[29] Ibid., p. 7.

additional step could be to share information with other oversight bodies that has already been shared by the intelligence and security services themselves. Once data has been exchanged, there is no need for oversight to lag behind." [30]

20. Besides the formal limitations that may inhibit a robust and effective oversight of international intelligence cooperation, relevant bodies may face practical limitations in terms of insufficient resources or expertise. Given the technical complexity of modern SIGINT (co-)operations that are often networked and taking place at several locations, investigations by oversight bodies can be very challenging and time-consuming if, for example, on-site inspections are to be conducted and technical manuals are to be read and digested in order to understand new methods of interception or data analysis.

21. The CoE Commissioner for Human Rights, thus, calls on the member states of the Council of Europe to: *"Ensure that external oversight bodies – including parliamentary oversight committees and expert oversight bodies – are authorised by law to hire independent specialists whose expertise is deemed to be relevant. In particular, oversight bodies should have recourse to specialists in information and communications technology who can enable overseers to better comprehend and evaluate surveillance systems and thus to better understand the human rights implications of these activities. Make sure that all institutions responsible for the oversight of security services have the necessary human and financial resources to fulfil their mandates. This should include recourse to technological expertise that can enable overseers to navigate, understand and evaluate systems for the collection, processing and storage of information. The adequacy of such resources should be kept under review and consideration should be given as to whether increases in security service budgets necessitate parallel increases in overseers' budgets."* [31]

22. The FRA research found that oversight bodies in several countries are already tackling these issues and have begun to recruit external technicians, either on an *ad hoc* or more permanent basis, despite difficulties in competing financially with private sector pay rates. Respondents to the FRA research also referred to promising digital oversight tools capable of carrying out automated checking of databases or technical verification at regular intervals.[32]

Conclusion

23. ENNHRI submits that the clear implication from the information set out above is that:

---

[30] Ibid., p.9.

[31] Commissioner for Human Rights (2015): Democratic and effective oversight of national security services. CommDH/IssuePaper(2015)2. Unter Mitarbeit von Aidan Wills. Council of Europe. Strasbourg (Issue Paper), p. 14.

[32] European Union Agency for Fundamental Rights (2017): Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update. Luxembourg: Publications Office of the European Union, pp. 84-86.

a. robust independent oversight of international intelligence sharing is needed without distinction between solicited and unsolicited data;

b. robust independent oversight bodies should be legally mandated to:

    i. oversee all matters of international cooperation by their national intelligence services, not restricted by national law or the "third party rule",

    ii. within their national mandate, cooperate with independent oversight bodies from the third states involved in the international intelligence sharing;

    iii. hire independent specialists where required, for example those with expertise in modern information and communications technology;

c. robust independent oversight bodies should be adequately resourced and staffed to effectively carry out their functions in relation to international intelligence cooperation.

***

ENNHRI

26 April 2019