UtrechtLawReview

This article is published in a peer-reviewed section of the Utrecht Law Review

Access to Justice for Communications Surveillance and Interception: Scrutinising Intelligence-Gathering Reform Legislation

Quirine A.M. Eijkman*

1. Introduction

The advances in information and communications technology, increased connectivity and the Snowden revelations have led to legislation that reform intelligence and security services' powers across the globe. Over the last decade states including Brazil, Denmark, France, Germany, Japan, New Zealand, Poland, Pakistan, the United Kingdom, the United States, Singapore, South Africa and the Netherlands have proposed bills or implemented acts that legalise the powers to (indiscriminately) intercept digital communications by intelligence and security services. Innovative communications technologies, such as big data, real-time tracking devices and hacking tools, are considered a strategic asset in anticipating, preventing or responding to national security threats. By collecting and retaining mass or targeted groups of personal data of targets and non-targets alike, communications surveillance programs allow states to conduct more sophisticated cybersecurity and counterterrorism measures. Simultaneously, this development in communications surveillance leads to an increased lack of power and autonomy by individuals who want to have an influence on how they are governed.[1] For instance, what happens to their private (digital) data once it is intercepted?

Communications surveillance is pervasive within society, but academic research on the subject in the context of law and national security has been progressing modestly.[2] Surveillance, essentially the systematic monitoring of large numbers of people without discrimination, can be defined as 'the garnering of personal data for detailed analysis'.[3] It is deployed either *en masse* (also known as dragnet or blanket), directed at

* Quirine Eijkman Ph.D. is the Chair of the Research Group Access2Justice at the Centre for Social Innovation (KSI), HU University of Applied Sciences Utrecht, and the Deputy President of the Netherlands Human Rights Institute. Email: quirine.eijkman@hu.nl. This article was writtten in her personal capacity.

1 B. Hayes, 'State of Surveillance: The NSA Files and the Global Fightback', *State of Power Report 2014: Exposing the Davos Class*, 21 January 2014, pp. 10-30, <http://www.tni.org/sites/www.tni.org/files/download/state_of_power-6feb14.pdf> (accessed 21 January 2018).

2 C. Aradau, 'Assembling Non-Knowledge: Security, Law and Surveillance in a Digital World', (2017) *International Political Sociology*, https://doi: 10.1093/ips/olx019; M. Eoyang, 'Beyond Privacy and Security: The Role of the Telecommunications Industry in Electronic Surveillance', (2017) 9 *Journal of National Security Law & Policy*, no. 2, <http://jnslp.com/2017/08/04/beyond-privacy-security-role-telecommunications-industry-electronic-surveillance/> (accessed 6 December 2017); D. Gray & S.E. Henderson (eds.), *The Cambridge Handbook of Surveillance Law* (2017); Institute for Information Law, University of Amsterdam, 'Ten Standards for Oversight and Transparency of National Intelligence Services' (2015); M.D. Lyon, 'The Snowden Stakes: Challenges for Understanding Surveillance Today', (2015) 13 *Surveillance & Society*, no. 2, pp. 139-152; R.A. Miller (ed.), *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair* (2017).

3 D. Lyon, *Surveillance as Social Sorting: Privacy, Risk and Social Digital Discrimination* (2013), p. 1. See also A. Arnbak & S. Goldberg, 'Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad', (2015) 21 *Michigan Telecomm. & Technology Law Review*, pp. 317-360; D. Bigo et al., 'Mass Surveillance of Personal Data by EU Member States and Its Compatibility with EU Law', Liberty and Security in Europe Papers, no. 61, 6 November 2013; E.D. Cohen, *Mass Surveillance and State Control: The Total Information Awareness Project* (2015); The Intelligence and Security Committee of Parliament (ISC), *Privacy and Security: A Modern and Transparent Legal Framework* (2015).

a person, or targeted, which is focused on an individual.[4] There are various forms of surveillance including human agents, computer programs such as Global Positioning Satellite (GPS) devices in our vehicles, cookies tracking IP addresses, social media messages, apps, the use of visual surveillance cameras (including drones) to monitor suspicious or unusual behaviour, Radio Frequency Identification (RFID) equipped on public highways or even the metering and billing of utilities.

Just like physical surveillance practices, communications surveillance programs fall under the responsibility of various state services, and sometimes private actors. However, in contrast to human intelligence gathering (also known as Humint), the study of the (indiscriminate) collection of advanced electronic signals or systems (Signals Intelligence or Sigint), in particular communications intelligence (Comint), and human rights implications has yet to be fully understood. The literature on the law, effectiveness and efficiency of these information and communication technologies is emerging.[5] At the same time the effect of communications interception (following communications, actions and practices in cyberspace) is intrusive given the increasing role that online and app activities play in our everyday life. This is observed in the momentum generated from the political and public debate on accountability at the national and international level.

During the past few years, parliamentary inquiries, national courts, legal scholars, technology experts and non-governmental organisations have concluded that communications surveillance programs and especially (indiscriminate) interception by intelligence and security services should meet specific criteria. As proposed by international human rights treaties this entails that these activities should have a law-standard quality (to be accessible and foreseeable), should have a legitimate aim (to protect national security) and that the interference must be necessary and proportionate.[6] The UN, the UN High Commissioner for Human Rights, the European Parliament, and the Council of Europe have expressed their concern about an effective remedy for (indiscriminate) Sigint, which in public discourse is known as 'mass surveillance', whereas the executive prefer to refer to this as 'bulk interception'. Also, they have warned about the consequences for particular human rights.[7] Nonetheless, although states take notice of these international calls for access to justice for those who are affected, due to a wide range of (perceived) national security threats, including terrorism and cyberespionage, they are likely to continue to invest in communications surveillance tools.

On a state level, the extent to which accountability mechanisms adequately deal with the (side-)effects of (indiscriminate) communications interception differs. For those concerned, access to justice is a key method to remedy an alleged intrusion by the intelligence and security services, in addition to oversight bodies. In the EU, for instance, some states have effective complaint and remedy procedures to handle unlawful communications interception, whereas in other Member States this appears to be lacking.[8] Meanwhile,

4 H. Bos-Ollermann, 'Mass Surveillance and Oversight, in D. Cole et al. (eds.), *Surveillance, Privacy and Trans-Atlantic Relations* (2017), p. 40.

5 M. Levi & D.S. Wall, 'Technologies, Security, and Privacy in the Post-9/11 European Information Society', (2014) 31 *Journal of Law and Society*, no. 2, p. 194; H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (2014); Surveille, *Surveillance: Ethical Issues, Legal Limitations, and Efficiency*, European Commission FP7 Project (2012-2015), <https://surveille.eui.eu/research/publications/> (accessed 2 July 2017).

6 Arts. 8 and 13, 2000 Charter of Fundamental Rights of the European Union; Arts. 8 and 13, 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms; Arts. 2 and 17, 1966 International Covenant on Civil and Political Rights; Art. 12, 1948 Universal Declaration of Human Rights.

7 COE European Commission for Democracy through Law (COE Venice Commission), 'Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Services', CDL-AD(2007)006 (2007); COE Venice Commission, 'Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Services', CDL-AD(2007)016 (2015); CTIVD, 'The CTIVD's View on the ISS Act 20 Bill' (CTIVD 2016); European Parliament (EP), 'National Programmes for Mass Surveillance of Personal Data in EU Member States and their Compatibility with EU Law', Directorate for Internal Policies Policy Department Citizen's Rights and Constitutional Affairs PE.493.032 (2014); International Principles on the Application of Human Rights to Communications Surveillance (IPAHRC), 10 July 2013, <https://en.necessaryandproportionate.org/text> (accessed 21 January 2018); E. MacAskill, 'The NSA's Bulk Metadata Collection Authority Just Expired. What Now?', *The Guardian*, 28 November 2015, <https://www.theguardian.com/us-news/2015/nov/28/nsa-bulk-metadata-collection-expires-usa-freedom-act> (accessed 21 January 2018); The Minister of the Interior and Kingdom Affairs, 'WIV 2017 en Regeerakkoord [WIV 2017 and Coalition Agreement], *Kamerstukken II*, no. 2017Z18166, 15 December 2017; UN High Commissioner for Human Rights, 'The Right to Privacy in the Digital Age, report by the Office of the UN High Commissioner for Human Rights presented to the United Nations Human Rights Council', UN DOC A/HRC/27/37 (2014); UN Human Rights Council, 'Report by Special Rapporteur M. Scheinin', UN Doc A/HRC/14/46 (2010); UN Human Rights Council, 'Report by Special Rapporteur M. Scheinin', UN Doc A/HRC/13/37 (2009); UN General Assembly, 'The Right to Privacy in the Digital Age', UN DOC A/RES/68/167 (2013); US National Research Council, 'Bulk Collection of Signals Intelligence: Technical Options' (2015), https://doi.org/10.17226/19414.

8 Fundamental Rights Agency (FRA), 'Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU' (FRA 2015a); FRA, 'Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU, Volume II: Field Perspectives

in Latin America, despite some good practices, overall surveillance legislation has not kept up with new technology and therefore access to justice is absent in most countries across the region.[9] In particular the question across the globe is when is an effective remedy required? Academic, legal and policy debates often focus on individual interference. Yet due to the rapid development of information and communication technologies the issue remains: when does the actual interference take place? From this perspective, what constitutes access to justice in relation to indiscriminate communications intrusion? Henceforth, in light of the debate on accountability this article discusses how access to justice for those affected by (indiscriminate) communications interception is protected.

For several reasons the Dutch statutory framework on the (special) powers of the intelligence and security services, the 2017 Intelligence and Security Services Act (hereinafter SIS 2017)[10] was selected as a case study. Firstly, the Ombudsman and, to a lesser extent, a judge[11] used to be formally in charge of dealing with complaints. In practice, however, most complainants relied on the Review Committee for the Intelligence and Security Services (hereinafter CTIVD) procedure, which advised the responsible minister on what to do.[12] In the SIS 2017 the Ombudsman will no longer play a role. It is still unknown if the new judicial complaints authority is able to provide adequate binding remedies for suspected grievances in relation to (indiscriminate) communications interception.[13] Secondly, the strategic importance of the Dutch satellite dishes[14] and transatlantic fibre optic cables, which connect continental Europe to Great Britain and the United States, is imperative for international Sigint cooperation. Last but not least, the Netherlands is internationally known for supporting human rights in its foreign policy. However, local issues such as access to justice for special powers of the intelligence and security services are not primarily labelled as a human rights concern in both political and public debate.[15]

Henceforth, in view of these (inter)national political, legal and public debates on accountability for the use of information and communications technology by the intelligence and security services, this article assesses if the Dutch intelligence gathering reform act, the SIS 2017, guarantees sufficient access to justice for complainants. At first the concept of access to justice in relation to the interception of (meta) data by intelligence and security services is introduced. In particular the possibility to hold the responsible minister or a security official mandated on the minister's behalf accountable for unlawful communications surveillance and interception is discussed. Are there, for example, effective complaint procedures in the Dutch intelligence gathering reform act? What about the remedies for special groups? And do individuals affected by (indiscriminate) communications interception receive access to justice? In the conclusion, access to justice for bulk and targeted interception by the intelligence and security services is reflected upon.

2. Access to justice for communications interception

Access to justice is a concept that assists in reviewing whether or not all human beings can equally deal with a perceived injustice such as an indiscriminate data intrusion or third party hacking by intelligence and security services. Although the intelligence and security services have a broader discretion than other law

and Legal Update' (2017); J.P. Loof, J. Uzman, T. Barkhuysen, A. Buyse, J.H. Gerards & R. Lawson, *Het Mensenrechtenkader voor het Nederlandse Stelsel van Toezicht op de Inlichtingen- en Veiligheidsdiensten* [The Human Rights Framework for the Dutch Oversight System for Intelligence and Security Services] (2015).

9 K. Rodríquez Perada, *Comparative Analysis of Surveillance Laws and Practices in Latin America* (2016).

10 Wet op de inlichtingen- en veiligheidsdiensten 2017 [Intelligence and Security Services Act 2017] (SIS 2017), *Staatsblad* [Bulletin of Acts and Decrees], no. 317, 17 August 2017.

11 Art. 83, Intelligence and Security Services Act 2002 (SIS 2002) and Art. 9:2, 1992 General Administrative Law Act; C. Fijnaut, 'Toezicht op de Inlichtingen- en Veiligheidsdiensten: De Noodzaak van een Krachtiger Samenspel' [Oversight of the Intelligence and Security Services: The Need for More Effective Concerted Action], (CTIVD 2012).

12 Intelligence and Security Services Act, Explanatory Memorandum (SIS 2017 memo), *Kamerstukken* II 2016/17, 34588, no. 3; CTIVD (2012), supra note 11.

13 Even though the Ombudsman is now formally responsible for dealing with complaints, in practice the CTIVD has usually advised the responsible minister (SIS 2017 memo). Unlike the CTIVD the Ombudsman and a judge, for example in a civil case, do not have access to secret files (Art. 83, SIS 2002 and Art 9:2, 1992 General Administrative Law Act); CTIVD (2012), supra note 11.

14 Located in Burum in the province of Friesland.

15 COE Venice Commission (2007) and (2015), supra note 7; UN Special Rapporteur (2010), supra note 7; P.R. Baehr et al., *Human Rights in the Foreign Policy of the Netherlands* (2002); B. Oomen, *Rights for Others: The Slow Home-Coming of Human Rights in the Netherlands* (2013); FRA (2015a), supra note 8; FRA, 'Access to Justice in Europe: An Overview of Challenges and Opportunities' (FRA 2015b).

enforcement services to gather, retain and process (digital) data, any individual who believes that he or she has been affected should have some method to challenge an infringement, whether this is in a court or an another judicial body that can provide an effective remedy.[16]

When considering access to justice there are three key dimensions to be distinguished: 1) access to the law, 2) access to a legal institution and 3) access to a fair and just solution.[17] With access to the law it is implied that each human being has the ability to obtain knowledge and understand the law, whilst having the opportunity to file a complaint. It is crucial that people are able to understand what the alleged infringement entails and how they can attempt to obtain an adequate solution for this. As Susskind[18] argues, a key issue is whether or not people are appropriately empowered to obtain their right.[19] And whether they are able to assess whether it is more opportune to avoid the dispute.

2.1 A human rights perspective

Furthermore, if people decide to file a complaint, the issue remains whether or not there is a legal entity that is willing to listen to the complainant and adjudicate the issue in a fair manner. From a human rights[20] perspective these aforementioned dimensions of access to justice could be perceived as the right to file a complaint and have an effective remedy against an alleged infringement by the intelligence and security services. In addition, these are key components of access to justice in relation to communications interception.[21] However, the use of (indiscriminate) data collection, data mining, data profiling techniques and hacking makes it challenging for complainants to establish a causal link between the (secret) surveillance and the personal harm suffered. This is generally considered to be a precondition for being able to claim one's right.

In particular, human rights questions relate to the transparency of communications surveillance programs as well as the efficiency of a remedy in a domestic context. For instance, even though the Netherlands as an EU Member State is subjected to Union law, intelligence and security services are exempted from this.[22] However, this does not mean that EU privacy and data protection principles do not apply or that meaningful enveloping standards do not play a role.[23] Furthermore, Article 13 of the 1950 European Convention on Human Right protects the right to an effective remedy, which also applies to so-called (secret) surveillance for national security purposes. As the jurisprudence of the European Court of Human Rights (ECHR) states, the right to complain in a (secret) surveillance case is recognised if the claimants, individuals or a group can demonstrate a personal interest and the possibility of having suffered personal harm. Furthermore, the effectiveness of the solution is based on the context of the complaint.[24]

Nonetheless, there are concerns about access to justice for data collection, processing, storage, analysis and sharing on the basis of communications surveillance programs.[25] Although nation states assert that they engage in the bulk interception of communications and afterwards, during a selection phase, identify what they need, it is still open to debate when the actual interference takes place. Is it, for example, after the bulk collection, storage or the selection phase? Or only in the analysis phase? When can those affected by

16 United Nations Development Programme (UNDP), 'Programming for Justice: Access for All: A Practitioner's Guide to a Human Rights-Based Approach to Access to Justice' (2005), p. 5.

17 R. Susskind, *The Future of Law* (1996); D.L. Rhode, *Access to Justice* (2004); D.L. Rhode, 'Whatever Happened to Access to Justice', (2009) 42 *Loyola of Los Angeles Law Review*, pp. 869-911; B. Hubeau, 'The Legacy and Current Relevance of Cappelletti and the Florence Project on Access to Justice', (2015) *Recht Der Werkelijkheid*, no. 3, p. 6.

18 Susskind (1996), supra note 17.

19 Hubeau (2015), supra note 17.

20 Arts. 8 and 13, 2000 Charter of Fundamental Rights of the European Union; Arts. 8 and 13, 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms; Arts. 2 and 17, 1966 International Covenant on Civil and Political Rights; Art. 12, 1948 Universal Declaration of Human Rights.

21 FRA (2015a), supra note 8; UN Special Rapporteur (2010), supra note 7.

22 Art. 4, 2007 European Union Lisbon Treaty.

23 Art. 29, Working Party, Opinion 04/2014 on Surveillance of Electronic Communications for Intelligence and Security Purposes, 819/14/ENG WP215, 10 April 2014, (Art. 29, Working Party 2014).

24 *Klass and Others versus Germany*, Decision of 6 September 1978, [1978] ECHR (App. no. 5029/17); *Liberty and Others versus the United Kingdom*, Decision of 1 July 2008, [2008] ECHR (App. no. 58243/00); *Szabó and Vissy versus Hungary*, Decision of 12 January 2016, [2016] ECHR (App. no. 37138/14).

25 D. Broeders et al., *Big Data in een Veilige en Vrije Samenleving* [Big Data in Safe and Free Society] (2016); COE Venice Commission (2015) and (2007), supra note 7; FRA (2015a), supra note 8.

alleged (indiscriminate) interception,[26] as revealed by Snowden, claim to be a victim of a privacy violation under human rights law such as Article 8 of the 1950 European Convention on Human Rights. This is defined as the right to respect for one's private and family life, home and correspondence.[27]

2.2 Filing a complaint and an effective remedy

On the one hand, when considering an international human rights point of view these aforementioned criteria of access to the law, a legal institution and a fair and just solution could be perceived as the right to file a complaint and have an effective remedy against an infringement by the intelligence and security services. On the other hand, as, among others, Van der Sloot[28] has argued, the individual interest criteria should perhaps be less restrictive in relation to large-scale data surveillance by intelligence and security services.[29] Even though the jurisprudence of the ECHR is consistent in emphasising that the effect of the intervention should be suffered directly, usually labelled as individual harm,[30] when we consider violations such as social media interception or hacking this becomes unrealistic. People are often not aware of their computer being hacked or their personal communications being interfered with, retained or shared. Neither are groups of persons who are affected. In the post-Snowden era a few communications surveillance cases that address these issues have been forwarded to the ECHR.[31] These are still pending.

Furthermore, it is not inconceivable that the Court and other international human rights bodies will impose stricter and more specific conditions on (secret) mass surveillance programs, the interception of communications, direct access, and the searching of 'automated works' (computers, phones etc.) by the intelligence and security services.[32] Yet, how this will affect access to justice for the (indiscriminate) interception of communications data will depend on an evaluation of the sufficiency of a state's entire oversight system for surveillance and interception.[33] As the ECHR re-emphasized in *Szabó and Vissy versus Hungary*,[34] national systems do have some discretion in the way they provide for a combination of accountability mechanisms.[35] In relation to access to justice for (indiscriminate) interception the complainant is better off with an independent scrutinising body that can definitively decide on the alleged infringement and provide remedies. Nonetheless, effective remedies should include the right to put individual grievances before a court or equivalent juridical entity, as described by the European Fundamental Rights Agency,[36] thereby ensuring that access to justice is one of the accountability mechanisms for unlawful, disproportionate or unnecessary communications interception.

26 The European Court of Human Rights has determined in earlier cases that the indiscriminate acquisition of (bulk) data without proper safeguards is illegal (see among others *Kennedy versus the United Kingdom*, Decision of 18 May 2010, [2010] ECHR (App. no. 58243/05); *Zakharov versus Russia*, Decision of 4 December 2015, [2015] ECHR (App. no. 47143/06).

27 *Big Brother and Others versus the United Kingdom*, Decision of 7 January 2014, [2014] ECHR (App. no. 58170/13).

28 B. van der Sloot, 'Is the Human Rights Framework Still Fit for the Big Data Era: A Discussion of the ECtHR' Case Law on Privacy Violations Arising from Surveillance Activities', in S. Gutwirth et al. (eds.), *Data Protection on the Move* (2016); B. van der Sloot et al., *Exploring the Boundaries of Big Data* (2016); B. van der Sloot, 'A New Approach to the Right to Privacy, or How the European Court of Human Rights Embraced the Non-Domination Principle', (2017) *Computer Law & Security Review*, in press, 7 December 2017.

29 B.J. Koops, 'On Decision Transparency, or How to Enhance Data Protection after the Computional Turn', in M. Hildebrandt & K. de Vries (eds.), *Privacy, Due Process and the Computational Turn* (2013), p. 196; Broeders et al. (2016), supra note 25; J. van Hoboken, 'From Collection to Use in Data Regulation? A Forward-Looking Comparison of European and US Frameworks for Personal Data-Processing', in B. van der Sloot et al., *Exploring the Boundaries of Big Data* (2016), p. 231.

30 J.H. Gerards & L.R. Glas, 'Access to Justice in the European Convention on Human Rights System', (2017) 35 *Netherlands Quarterly of Human Rights,* no. 1, pp. 11-30.

31 *Big Brother*, supra note 27; Q. Eijkman, 'Indiscriminate Bulk Data Interception and Group Privacy: Civil Society Payback through Strategic Litigation?', in L. Taylor et al. (eds.), *Group Privacy: Challenges of Data Technologies* (2017), pp.123-138; *Bureau of Investigative Journalism and Alice Ross versus the United Kingdom*, [2014] ECHR (App. no. 62322/14); *10 Human Rights Organisations versus the United Kingdom*, [2015] ECHR (App. no. 24960/15).

32 Loof et al. (2015), supra note 8.

33 The European Court of Human Rights did so by citing its earlier jurisprudence (*Klass*, *Szabó*, supra note 24).

34 *Szabó*, supra note 24, para. 25 and paras. 85-86; *Liberty*, supra note 24.

35 COE Venice Commission (2015), supra note 7.

36 FRA (2015a), supra note 8; FRA (2015b), supra note 15.

3. The checks and balances

Due to communications technology advancements and their utilisation by the Dutch security services, the Government proposed a new statutory framework in 2015, upon a recommendation by an ad-hoc Intelligence Review Commission (also known as the Dessens Commission II[37]). In June 2015 this legislative proposal, which will replace the Intelligence and Security Services Act 2002, was open for public consultation. The public response to the act was considerable: 1,100 people/organisations responded.[38] Subsequently an amended version was sent for mandatory advice to the Council of State and the bill was passed in the House of Representatives as well as the Senate. Although the SIS 2017 is due to be implemented, it continues to be part of the political and public debate.[39] Not only is it part of the 2018-2022 Coalition Agreement, but a consultative referendum is scheduled on March 21st 2018. The petitioners, five students from the University of Amsterdam, exceeded the required amount of votes to have the referendum. However, it is likely that the Government will disregard the outcome as not only does it support the new act, but it also announced that it will end the existing consultative referendum system.

3.1 Technology-independent interception powers

From a communications surveillance perspective, the expansion of powers including the suggested transformation of technology-dependent to technology-independent special powers is relevant. Essentially, by allowing any (indiscriminate) interception, irrespective of the type of communication taking place, the new technology-neutral based approach has become fact. Thereby ensuring that bulk cable-bound telecommunications and non-cable-bound (e.g. via satellite and radio waves) interception has become lawful for the Military Intelligence and Security Service (hereinafter MIVD) as well as the General Intelligence and Security Service (hereinafter AIVD).

In 2013 the Dessens Commission II evaluated the existing legislation, the Intelligence and Security Services Act 2002, and concluded, as the CTIVD had done earlier, that the special powers in relation to the bulk interception of cable-bound communications (both traffic and meta data) should be modified.[40] Just like the MIVD, the AIVD should be authorised to investigate non-evaluated, or bulk,[41] telecom and internet traffic data, which is now predominately transferred through fibre cables. Simultaneously, as the invasion of privacy and confidentiality of (big) data is being challenged, the 2013 Dessens Commission II emphasised the importance of striking a balance between more Sigint powers and accountability.[42] In others words more technology-independent interception powers, such as the interception of (secret) bulk cable-bound or telecom data, would have to be compensated by stronger safeguards and transparency. As the 2016 Privacy Impact Assessment Report commissioned by the Government reemphasises, checks and balances become even more important for future technology including the Internet of Things, predictive profiling and big data analytics.[43]

37 Earlier the Dessens Commission I had also conducted a review (Dessens Commission I, *Inlichtingen en Veiligheid, Defensie: Kwaliteit, Capaciteit en Samenwerking* [Intelligence and Security, Defence: Quality, Capacity and Cooperation] (2016); Dessens Commission II, *Dutch Intelligence and Security Services Act 2002 Evaluation* (2013).

38 SIS 2017 memo, supra note 12.

39 The Minister of the Interior and Kingdom Affairs (2017), supra note 7; *Het Sleepnet Referendum* [The Dragnet Referendum], <https://sleepwet.nl/> (accessed 15 December 2017).

40 CTIVD, 'Over de Inzet van SIGINT door de MIVD' [About the Use of SIGINT by the Military Intelligence and Security Service], Report 28 (2011); Dessens Commission II (2013), supra note 37; CTIVD, 'Over Gegevensverwerking op het Gebied van Telecommunicatie door de AIVD en de MIVD' [Review Report on the Processing of Telecommunications Data by the General Intelligence and Security Service and the Military Intelligence and Security Service], Report 38 (2014).

41 The legislative authorities state that non-evaluated data is not the same as indiscriminate or bulk data interception (SIS 2017 memo, supra note 12). However, among others the Human Rights Institute and the Privacy Impact Assessment, which was commissioned to evaluate the bill SIS 2017, labels it as such (Privacy Impact Assessment (PIA), 'Privacy Impact Assessment op de Wet op Inlichtingen- en Veiligheidsdiensten' [Privacy Impact Assessment of the Intelligence and Security Services Act] (2016)); Netherlands Institute for Human Rights, 'Status Report Human Rights in the Netherlands 2015' (2016).

42 Dessens Commission II (2013), supra note 37.

43 PIA (2016), supra note 41.

3.2 Prior (judicial) authorization

Existing oversight mechanisms have, to a large extent, been preserved or somewhat amended in the SIS 2017. In relation to communications interception it legalises the general and special powers to collect, process and retain (big) data.[44] An entirely renewed system, which requires that a non-targeted communications interception is directed towards an 'investigation-related purpose', has been proposed.[45] In essence, it legitimises the distinction between the three pre-analysis phases of collection, pre-treatment and searching or selection of communications data, which are safeguarded by increasing levels of oversight, and the analysis phase.[46] In the initial version of the act in 2015 the prior authorization for the deployment of this special power was, as in the past, an executive decision by the responsible minister or a security official mandated on the minister's behalf.

Despite some extra safeguards, a considerable number of individuals and organisations complained during the public consultation about the lack of prior judicial consent.[47] Since then the legislative authorities have amended parts of the act. Now the executive decision is subjected to a prior judicial binding assessment focussing on lawfulness and justification by an independent specialised judicial commission, the Assessment Committee on the Use of Powers (*Toetsingscommissie Inzet Bevoegdheden* hereinafter TIB). Although two of the TIB members have to have considerable experience as judges and one as a technical expert, are appointed by the Crown upon Parliament's recommendation and have authority to revoke an executive decision, there is some public debate as to whether or not this prior judicial consent procedure should be perceived as a sufficient safeguard.[48] Among other things, their assessment is purely legal, they unlike the CTIVD have no access to classified information kept by the AIVD or the MIVD and oversight during the entire phase of authorized (special) powers should be preferred.

3.3 Internal and external oversight

Other accountability mechanisms include internal and external oversight, which are to some extent connected to each other. Internally the responsible ministers, the Ministers of the Interior and Kingdom Affairs and of Defence, as well as the coordinator[49] of the Ministry of General Affairs, play an important role. The coordinator, the Secretary-General of the Ministry of General Affairs (the highest civil servant), presides over the so-called Intelligence and Security Services Committee, which consists of assigned high-ranking civil servants from several ministries.[50] External oversight mechanisms include democratic oversight committees, the external oversight committee, ordinary civil, administrative and criminal courts, and for accountability in relation to expenditure, administration and policy, the National Audit Court.

Democratic oversight consists of two parliamentary commissions that primarily focus on general issues. The first is the Committee on Home Affairs and Kingdom Relations or the Defence Committee. If necessary the entire House of Representatives or the Senate could meet. The second is the Committee on Intelligence and Security Services (publicly known as 'the Secretive Commission'). This committee, which is composed of the chairpersons of the five largest political parties in the House of Representatives, has access to state secrets. They may be briefed on national security by the responsible minister or civil servant on the basis of confidential, secret and top secret information. The politicians, however, are not authorized to disclose any classified information about the briefings. Even though there has been some concern about the need for the transparency and thoroughness of the oversight as provided by the chairpersons, Parliament has decided to continue with the Secretive Commission in its current form.[51]

44 Arts. 17-27, SIS 2017.
45 Arts. 48, SIS 2017.
46 PIA (2015), supra note 41; SIS 2017 memo, supra note 12.
47 SIS 2017 memo, supra note 12, pp. 224-225.
48 Netherlands Institute for Human Rights, 'Brief over de Wet op Inlichtingen- en Veiligheidsdiensten (34.588)' [Letter on the Intelligence and Security Services Act 20XX (34.588)], 2017/0005/AvD/JB/LR (2017); Arts. 32-38, SIS 2017.
49 The Prime Minister, who is also the Minister of General Affairs, is responsible for the coordinator, who is the Secretary-General of his or her ministry.
50 Arts. 1-5, SIS 2017.
51 C.W. Hijzen, 'More Than a Ritual Dance: The Dutch Practise of Parliamentary Oversight and Control of Intelligence', (2014) 24 *Security and Human Rights*, no. 3/4, pp. 227-238; Art. 22, Regulation of Order of the Second Chamber of the States General, no. 34727, 30 May 2017

The specialised review committee, the CTIVD, has become an influential external oversight body, relatively stronger than parliamentary and, possibly also, judicial control. Its oversight review reports, solicited and unsolicited advice and annual reports will continue to assess the Dutch intelligence and security services' compliance with the law, but not their efficiency.[52] In order to conduct their assessment, the oversight department of the CTIVD has direct (digital) access to classified information kept by the AIVD and MIVD. Moreover, their employees are required to cooperate. Their review reports, which have both disclosed and undisclosed sections, assess topics including operations, administration, policies and national and international cooperation. The responsible minister must determine whether he or she endorses the findings and recommendations of the CTIVD or puts them aside.

In the SIS 2017 the legislative authorities have decided to extend the powers of the external oversight committee. It will no longer advise the executive, which are the ministers concerned, on the handling of complaints, but a separate complaint department will now deal with these in a binding manner. However, in contrast to the recommendations of influential stakeholders, the lawmakers did not want binding oversight for the use of all (special) powers by the intelligence and security services,[53] thereby essentially limiting the effect of oversight on the (indiscriminate) interception of communications. Last but not least, according to the Council of State and the CTIVD the assessment of automated data processing and analysis phases should be broader.[54] It should not only be focussed on lawfulness, but other factors including efficiency should also be taken into account.

3.4 Complaint procedure

Henceforth, a second branch within the CTIVD, separate from the oversight department, will function as a quasi-judicial body that provides a binding remedy for a (suspected) grievance.[55] In order to do so, it should be able to hear the complainant, examine the files of the intelligence and security service involved and consult its employees. Essentially the three members of the complaints department, including the president who will be the only member of the CTIVD, will assess if a complaint is grounded. They do so on the basis of reviewing the so-called (alleged) appropriate conduct of the civil servant or the minister in question. This will include assessing lawfulness. Also there are relatively strict criteria about who is allowed to complain: only those who are affected by (suspected) acts by the intelligence and security services.

The complainant is required to inform the accountable administrative authority, the minister in charge.[56] There are a few criteria that the written complaint must meet. A description of the (alleged) infringement, whom it concerns (the conduct of the responsible minister, the coordinator, the head of the intelligence or security services or the civil servant in question and the person who it affects) and the grounds for filing the complaint are the most important. If the complaint is either partially or fully well-founded and/or unlawful the CTIVD can order the minister to remedy the infringement by halting an ongoing investigation, ending the use of a special power or deleting and destroying processed data. The complaints department's remedial powers do not include the awarding of compensation nor is there an appeal procedure. Thereafter, a complainant will need to initiate a separate civil action for damages against the state or an appeal, possibly on (legal) grounds. The role of the Ombudsman as an independent mechanism between complainants, who are affected by the acts of the intelligence and security services, and the Government ceases to exist.

(2017); SIS 2017 memo, supra note 12, pp. 228-230.

52 Council of State, Advice on the Bill on the Intelligence and Security Services Wiv 20XX and the Amendments to other Acts, *Kamerstukken II* 2016/17, 34588, no. 2, 21 September 2016; CTIVD (2012), supra note 11; Arts. 107-113, SIS 2017.

53 Dessens Commission II (2013), supra note 37; Ombudsman, Letter to the Minister of the Interior and Kingdom Relations Draft Bill WIV (2015); Loof et al. (2015), supra note 8; CTIVD (2016), supra note 7.

54 Council of State (2016), supra note 52; CTIVD (2016), supra note 7; CTIVD, Letter to the Senate on the Draft Bill on the Intelligence and Security Services Bill Wiv 20XX (CTIVD 2017a).

55 Arts. 97 and 114-124, SIS 2017; See Arts. 9:28, 9:29 and 9:30, 1992 General Administrative Law Act.

56 Arts. 114, SIS 2017 and Art. 9:12 (2), 1992 General Administrative Law Act.

3.5 Other safeguards?

Last but not least, other safeguards against (indiscriminate) interception by the intelligence and security services are worthwhile considering. These include the obligation to inform (notify) and data protection. Also there are special procedures to protect lawyers, journalists and whistleblowers, but not for doctors or non-governmental organisations. Notification is crucial in light of the secrecy surrounding the interception of communications. Being informed could empower those affected to file a complaint. Although notification continues to exist for a limited number of powers, in practice the obligation to notify will often be exempted for national security reasons. Nonetheless, this kind of transparency is important in light of the secrecy surrounding the interception of communications.[57] Being informed could empower those affected to file a complaint. Simultaneously, it may influence the intelligence and security services to protect personal data more thoroughly as well as minimalizing the amount of data that they store. It does not apply to bulk data intrusions, during the pre-analysis phases of data collection, mining and selection or in case of (inter) national data sharing.[58] To summarize, even though there is a right to access and to correct personal data, it is only related to the so-called evaluated data.[59]

Other data protection safeguards include the general duty to promote the correctness and completeness of processed data and to avoid data breaches. The Director General of the AIVD and the director of the MIVD must also take sufficient measures to protect the quality of data processing, including the models and algorithms.[60] Furthermore, the intelligence and security services are prohibited from promoting or taking any action against a person solely based on the outcome of automated data analysis. For example, if a big data algorithm finds a correlation between a certain individual and a violent extremism public podcast, the intelligence and security service cannot act based on the outcome of this result alone. Human decision-making should permanently complement automated decision making.[61] Additionally, there is some resemblance between a general duty of care and Dutch data protection law. Nevertheless, the intelligence and security context is exceptional, because it requires an efficiency review to be conducted by the intelligence and security services themselves, rather than by oversight mechanisms. In other words, for accountability during the data processing phase, complainants will have to rely on other safeguards rather than individual remedy procedures

Furthermore, whistleblowers can report (suspected) abuses to the aforementioned complaints department of the CTIVD.[62] Officials of the intelligence and security services and others, such as the personnel of telecommunications companies, may blow the whistle after reporting it first internally. The decision that is reached on the reported abuse by the CTIVD complaints department is published in a report. If the allegations are shown to be wholly or partially well founded, the whistleblower may read the draft report at the CTIVD headquarters in the Hague and respond to it before it is published. Yet, the responsible minister is under no obligation to ensure that the situation changes. Nor is he or she under any obligation to comply with the recommendations that the CTIVD complaints department issues.[63] Only parliamentary oversight can hold the minister fully accountable. For the use of special powers in relation to lawyers and journalists there are unique thresholds.[64] Indiscriminate collected data should be destroyed immediately and if an intelligence and security service intends to use it the relevant executive ministerial decision requires judicial authorisation from the District Court of The Hague.

57 Arts. 59(1) and 44(1), 47(1) and 58(1), SIS 2017; SIS 2017 memo, supra note 12; *Big Brother*, supra note 27; CTIVD, 'Over de Uitvoering van de Notificatieplicht' [About the Use of Notification by the AIVD and the MIVD], Report 51 (CTIVD 2017b).
58 Arts. 59 and 48-50, SIS 2017.
59 Arts. 76-85, SIS 2017.
60 Arts. 24 and 25, SIS 2017; The Minister of the Interior and Kingdom Affairs (2017), supra note 7.
61 SIS 2017 memo, supra note 12, pp. 175-176.
62 Arts. 125-131, SIS 2017.
63 Ibid.
64 Arts. 27(2), 29(2) and 30(2/3) SIS 2017.

4. Access to justice in law and practice?

The key question remains whether the Dutch Intelligence Gathering Act guarantees access to justice for (indiscriminate) communications' interception by the intelligence and security services. As mentioned earlier, access to the law, a legal institution and a fair and just solution can be regarded as the determining factors for those affected. By filing a complaint, some sense of ownership of the process is regained. Simultaneously, attaining an effective remedy against a (alleged) grievance is important, because it formally recognizes the harm suffered and may even lead to some sort of national security practice reform.

4.1 Complex to understand

As was the case before, the SIS 2017 is likely to be accessible online, on several governmental websites, and on paper. However, feedback on an earlier version of the act stated that it is fairly complex to understand for those who are not specialised in the law.[65] The legislative authorities recommend reading the explanatory memorandum to the Act in order to satisfy the specialised knowledge criteria; however, it still remains a question whether it is understandable for the general public.[66] The complexity of the act is a concern when considering the importance of access to justice. This is because the complainant is advised to describe and explicate the grounds for the complaint.[67] It is not unthinkable that someone would need legal advice in order to prepare his or her grievance or to be represented. Therefore, it is imperative that the CTIVD complaints department does not set too high a threshold for explicating the (legal) basis for the complaint and update its complaint-handling instructions, with a do-it-yourself assessment.[68]

4.2 A satisfactory legal institution at first sight

At first sight it appears that with the creation of the CTIVD complaints department, a satisfactory legal institution has been established. In fact this judicial body will be able to provide a binding solution for a suspected grievance. As the CTIVD complaints department consists of experts who are familiar with the topic they will be able to scrutinise the action of the intelligence and security services thoroughly. However, it has to be noted that the CTIVD complaints department is not a court.[69] It does have hearings, but it is unclear whether or not they will be held in public and whether both parties will be present.[70] Furthermore, although the members are selected by the House of Representatives, they are not required, unlike two of the three TIB members, to have experience as a judge.[71] It is possible that the legislator felt that, akin to other complaint administrative procedures, experts with a legal and perhaps even a security background would be more familiar with the work of security and intelligence services than a specialised judge. Yet, the District Court of The Hague could have been a realistic alternative for dealing with (suspected) grievances, with its experience in intelligence-related procedures such as in relation to opening letters and the privacy of correspondence.[72]

Moreover, questions related to the CTIVD complaints department's impartiality and independence are problematic. According to the Ombudsman, who responded to the public internet consultation of the SIS 2017, there is a risk that as the CTIVD will combine oversight and complaints handling the review committee will not be perceived to be impartial or free from bias.[73] The dual role that it plays may confuse people. In addition, it is possible that a contentious situation could occur such as if the oversight department were to

65 PIA (2016), supra note 41.
66 SIS 2017 memo, supra note 12, pp. 238-240 and 276.
67 Art. 115, SIS 2017.
68 See the CTIVD website <http://english.ctivd.nl/complaints-handling> (accessed 6 December 2017) and the Ombudsman's Office's website <https://www.nationaleombudsman.nl/file-complaint/criteria> (accessed 6 December 2017).
69 Institute for Information Law (2015), supra note 2.
70 Art. 117, SIS 2017.
71 Art. 99, SIS 2017.
72 Arts. 27 and 44, SIS 2017; Art. 13(1), 1815 Constitution.
73 Ombudsman (2015), supra note 53; SIS 2017 memo, supra note 12, p. 240.

determine that a practice is lawful whereas the complaints department would rule differently.[74] Thereby the same body could come to different conclusions. The Ombudsman recommended the establishment of a complete independent complaints body. This would be in line with other complaints procedures and there would be an appeal, which is not possible in the current proposal.[75] The legislative authorities, however, feel that the proposed oversight system and, in particular, the establishment of the binding complaints department meet the effective remedy criteria as established by human rights standards.[76] It is still unknown whether the general public will perceive the CTIVD complaints department to be completely independent from the oversight department.

4.3 A Fair and just solution?

Overall the new binding complaints procedure appears to provide an adequate remedy for a complainant addressing a (suspected) targeted surveillance intrusion against an individual or a defined network/ organisation. It assesses more broadly than on the basis of lawfulness alone. Previously, the number of complaints was relatively modest. For instance, in 2016 there were 13 complaints that the CTIVD advised upon.[77] Furthermore, since the implementation of the Intelligence and Security Services Act 2002 there have been 14 complaints addressed to the Ombudsman's Office.[78] The reasons behind the lack of affected individuals coming forward remain unclear, but it could be due to the secrecy or the lack of knowledge about the intelligence and security agency's practice.

However, in relation to indiscriminate communications interception it is less clear if the new complaints procedure could potentially remedy this. It appears as if the legislator implied that a suspected infringement in the context of indiscriminate communications interception is checked and balanced within different other safeguards, including once the collected data has been narrowed down with the increased levels of oversight.[79] This would entail previous ministerial permission, prior judicial approval by the TIB, specific retention periods during the phases of collection, pre-treatment, searching or selection and external oversight as provided by the CTIVD. Subsequently, the CTIVD complaints department will potentially not handle a complaint that addresses bulk interception in the earlier pre-analysis phases of collection and processing, nor will it be concerned with (inter)national non-evaluated (raw) data set sharing.[80] Therefore, someone with (alleged) grievances will have limited grounds to substantiate the basis of a complaint, due to the secrecy surrounding the interception.

Although it is possible for the complainant to resort to the courts, the success rate is low. According to jurisprudence they are required to demonstrate individual harm. In the *Citizens versus Plasterk* case[81] in 2014 the claimants, a group of civil society organisations, professional organisations and citizens, focused on the (alleged) intrusion caused by international bulk data sharing between the Dutch services and the American National Security Agency (NSA). Despite the fact that they had a rigorous profile, according to the court they could not prove that they or the people they represented had suffered individual harm.[82] A question is how the ECHR in the communications surveillance cases that are pending will address these kinds of issues.[83] Although the claimants, non-governmental organisations, journalism collectives and individuals, have passed the admissibility test, it remains to be seen if the Court in its decision will recognize that the

74 Eerste Kamer der Staten Generaal [Senate of the States General], Regels met Betrekking tot de Inlichtingen- en Veiligheidsdiensten alsmede Wijziging van Enkele Wetten [Rules in Relation to Act and Amending Several Acts] (The Intelligence & Security Services Act 2017), 3 May 2017, *Kamerstukken I,* 34588 no. C, 3, pp. 25-26.

75 Chapter 9, 1992 General Administrative Law Act; SIS 2017 memo, supra note 12; Senate of the States General, supra note 74.

76 Art. 13, 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms; SIS 2017 memo, supra note 12, pp. 249-277.

77 CTIVD, 'Annual Report 2016' (CTIVD 2017c), p. 23.

78 Senate of the States General, supra note 74.

79 Arts. 25-27, 32-37, 48-50, 97 and 112-113, SIS 2017; SIS 2017 memo, supra note 12, subsection 7; The Minister of the Interior and Kingdom Affairs (2017), supra note 7.

80 Arts. 61-70,88-90 and 91-96, SIS 2017; Senate of the States General, supra note 74; CTIVD (2016), supra note 7; CTIVD (2017a), supra note 54; The Minister of the Interior and Kingdom Affairs (2017), supra note 7.

81 The Hague District Court 23 July 2014, *Citizens versus Plasterk*, ECLI:N:RBDHA:2014:8966, no. C09/445237 HA ZA 13-1325.

82 Ibid.

83 *Big Brother*, supra note 27; Eijkman (2017), supra note 31, p.183; *Bureau of Investigative Journalism and Alice Ross*, supra note 31; *10 Human Rights Organisations*, supra note 31.

right to privacy of a group has been violated. Let alone how, in view of (indiscriminate) communications interception by the intelligence and security services, the ECHR will assess the entire British accountability system for secret surveillance, including the effectiveness of domestic remedies. Henceforth, a coalition of several organizations[84] have announced that they are preparing to challenge particular parts of the SIS 2017 after its implementation, it is likely that the ECHR will also assess how effective the accountability system for secret surveillance is in the Netherlands.

5. Conclusion

By scrutinising the Dutch intelligence gathering reform act this article contributes to debates about the complexity of access to justice and accountability for (indiscriminate) communications interception. In the aftermath of the Snowden revelations and due to developments in information and communications technology, states across the globe have created legislation that legalises intelligence and security services' (mass) communications surveillance programs. However, have adequate accountability mechanisms been established? Among other issues why is there prior judicial consent for some special powers, but not for others or the general powers? Especially, it remains a question if (newly) established complaint procedures contribute to more public legitimacy of communication interception powers.

The Netherlands has amended its accountability mechanisms for the intelligence and security services. For particular targeted interception grievances a more or less sufficient binding complaint system has been created. Yet from an individual perspective the checks and balances for bulk interception are less rigorous. It is as if the legislator felt that indiscriminate surveillance is not an intrusion that should be counterbalanced with a fair and just solution on an individual or group level. This is unfortunate, because by collecting, retaining and sharing huge swathes of personal data people can no longer control what happens to it. Also they have to rely on other broader mechanisms which may or may not provide for adequate oversight.

Subsequently, one wonders whether complaints procedures should be a remedy against a (suspected) indiscriminate interception intrusion. If in practice a complaints procedure is not able to provide for a fair and just solution to remedy the large-scale collection and processing of data by the intelligence and security services then from an access to justice perspective there is a concern. Even though a complainant could resort to the courts, he or she would have trouble in demonstrating the impact of individual harm. Thus mass surveillance programs lead to the creation of groups, but those affected can only invoke their individual right to privacy and not do so as a collective. Thereby access to a legal institution is limited.

Furthermore, a fair and just solution would only be available when the violation becomes more intrusive (e.g. targeted). In other words, during the data analysis phase direct human decision-making is checked and balanced by the possibility to file a complaint, but a question remains as to whether the intrusion does not take place earlier during the pre-analysis phases. In the context of, for example, international unevaluated data sharing there is no option to complain nor is it subject to prior judicial consent. This even though an individual or groups at home or abroad may be affected. Henceforth, despite the fact that other accountability mechanisms such as an external oversight committee could remedy this, it would not change anything on an individual or group level. This would result in limiting the avenues to redress indiscriminate communications interception by the intelligence and security services in the Netherlands.

84 Concept-Dagvaarding Tegen de WIV [Draft Summons Against the WIV] (2017), Privacy First Website <https://www.privacyfirst.nl/rechtszaken-1/item/1069-concept-dagvaarding-tegen-sleepnetwet-wiv.html> (accessed 17 December 2017).