Dutch National Security Reform Under Review

Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?

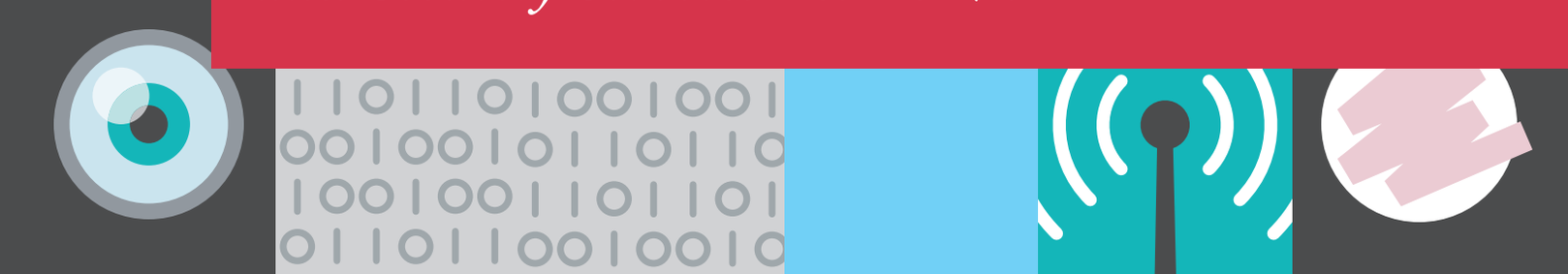
Eijkman, Q.; van Eijk, N.; van Schaik, R.

University of Amsterdam

University of Applied Sciences Utrecht

IViR (Institute for Information Law)

Dutch National Security Reform Under Review: *Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?*



Institute for Information Law (IViR, University of Amsterdam), 2018
This project has been carried out in full compliance with the Declaration of Scientific Independence of the Royal Netherlands Academy of Arts and Sciences.

Institute for Information Law
University of Amsterdam
The Netherlands
http://www.ivir.nl

Research Group Access2Justice
Centre for Social Innovation (KSI)
HU University of Applied Sciences Utrecht
The Netherlands

Dutch National Security Reform Under Review:

Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?

Quirine Eijkman
Nico van Eijk
Robert van Schaik

Utrecht/Amsterdam, March 2018

Contents

	Foreword	**9**
1.	**Introduction**	**11**
1.1	Background	11
1.2	Legislative process	11
1.3	Strategic litigation, referendum	12
1.4	Roadmap	13
2.	**Scope and guiding principles**	**15**
2.1	Organization of the intelligence and security services	15
2.2	Powers of the services	15
2.2.1	*Regular versus special powers*	*15*
2.2.3	*Examples of special powers*	*16*
2.3	Data processing	18
2.4	Data transfer	19
2.5	Technology-neutral approach	19
2.6	Bulk collection and processing: "investigation-related purpose"	21
2.7	Gaining access to computerized systems or devices: hacking	24
2.8	Cooperation by third parties	25
3.	**Political and internal accountability**	**27**
3.1	Introduction	27
3.2	Accountability of the intelligence services	27
3.2.1	*Organization of the intelligence services*	*27*
3.2.2	*Executive authorization*	*28*
3.2.3	*Duty of care*	*28*
3.3	Ministerial/executive responsibility	29
3.3.1	*Lawfulness versus appropriateness*	*29*
3.3.2	*Relationship between the executive and the intelligence services*	*30*
3.4.	International cooperation	31
3.4.1	*Adequacy procedure*	*31*
3.4.2	*Requests from foreign services*	*32*
3.4.3	*Cross-border data transfer*	*32*

4.	**Oversight and access to justice**	**35**
4.1	Introduction	35
4.2	Prior judicial consent: district court of The Hague	35
4.3	Prior judicial consent: the Review Board for the Use of Powers	36
4.4	Parliamentary oversight	37
4.5	External oversight: the Review Committee for the Intelligence and Security Services	38
4.6	Netherlands Court of Audit	39
4.7	Binding complaints procedure	39
4.8	Whistle-blower procedure	40
4.9	Transparency	40
5.	**Bottlenecks**	**43**
5.1	Introduction	43
5.2	Struggles with the concept of independent oversight	43
5.3	No binding oversight for special powers	45
5.4	International exchange of data	45
5.5	Review Committee for the Intelligence and Security Services vs. the Review Board for the Use of Powers	46
5.6	Legal uncertainty	46
5.7	Effectiveness of complaints and whistle-blower remedies	46
5.8	Open source information as intelligence?	47
5.9	Distinction between regular and special powers	48
	References	**51**
	ECtHR Jurisprudence	53
	Dutch Jurisprudence	53
	Newspaper articles	53
	List of terms/abbreviations	**55**
	About the Authors	**57**

Foreword

In May 2018, the new Dutch Intelligence and Security Services Act 2017 (Wet op de Inlichtingen- en veiligheidsdiensten, Wiv) will enter into force. It replaces the previous 2002 Act and incorporates many reforms to the information gathering powers of the two intelligence and security services as well as to the accountability and oversight mechanisms. Due to the technology-neutral approach, both the civil and the military intelligence services are now authorized to, for example, intercept communications in bulk, hack third parties, decrypt files, store DNA or use any other future innovative technology. Also, the national security legislation extends the possibilities for the indiscriminate collection of data, and for the processing, storage and analysis thereof. The process leading to the law includes substantial criticism from the various stakeholders involved. Upon publication of this report, an official consultative referendum is being organized on the new act.

The aim of this policy brief is to provide an international audience with a comprehensive overview of the most relevant aspects of the act and its context. In addition, there is considerable focus on the checks and balances as well as the bottlenecks of the Dutch intelligence gathering reform. The selection of topics is based on the core issues addressed during the parliamentary debate and on the authors' insights.

We thank all who participated in the process providing useful comments and suggestions. The project was funded by the Research Group Access2Justice of the HU University of Applied Sciences Utrecht with additional support from the Institute for Information Law of the University of Amsterdam. The research was conducted in compliance with the guidelines as set out in the Declaration of Scientific Independence by the Royal Netherlands Academy of Arts and Sciences (KNAW).

Utrecht/Amsterdam
March 2018

1. Introduction

1.1 Background

The adoption of the Intelligence and Security Services Act 2017 (ISS Act 2017) earmarks a new era in national security legislation in the Netherlands. The new act replaces the 2002 Act, which was implemented just before a period when cyber threats increased, and the impact of terrorist attacks was felt throughout Europe. The need to address these challenges is reflected in the new act, creating innovative technological powers to collect information and limiting accountability. In the Dutch context, this type of intelligence gathering legislation specifically regulates the tasks and the (special) powers of the intelligence and security services.

Before drafting a bill for a new act, a special state committee (the Dessens Committee) was requested to assess the existing law and to make recommendations. Its report, subtitled 'towards a new balance between powers and guarantees', was published in December 2013. The main conclusions pointed towards a technology-neutral approach allowing the instruction of new methods, including third party hacking and the bulk collection of data from wired networks (under the previous act, only bulk collection of data from wireless networks was allowed). On the 'guarantee' side, the report proposed to take a granular approach to the collection and processing of data, with more restrictions on the processing. In terms of oversight, the Committee only saw a need for prior, *ex ante*, oversight in the case of opening letters, as required by the Dutch constitution and to protect journalistic sources (based on recent jurisprudence by the European Court of Human Rights (ECtHR). The subsequent, *ex post*, oversight should have stronger remedies, but would be limited to questions relating to lawfulness. Other recommendations include better internal procedures and a strengthened complaints procedure.

1.2 Legislative process

The Dutch government's reaction to the report was to embrace many of the proposals, including the codification of jurisprudence by both the European and national courts. This resulted in a bill, which was published for public online consultation (July/August 2015). It prompted a huge response; more than 1,100 comments were received. A significant number came from engaged citizens. Furthermore, a considerable number of private companies, state advisory organs, scientists, professional organizations and non-governmental organizations (NGO) responded. A part of the public responses was coordinated by the NGO Bits of Freedom, which opposed the new so-called 'dragnet

surveillance'. Other comments addressed the limited oversight model, the technological-neutral approach, data minimization, international cooperation and the special protection of journalists. The bill sent to parliament early in 2017 only addressed some of these concerns and this influenced more advocacy not only from NGOs, private companies and academics but also from the judiciary, the Review Committee on the Intelligence and Security Services (CTIVD) and the Council of State in its capacity as the official advisor to the government. Over fifty amendments and motions were put to vote in the House of Representatives, but only three amendments and six motions were accepted. The body of the bill remained largely untouched and was passed with a large majority in both houses of the parliament. Final liberations and voting ended early July 2017, followed by rapid publication in the Bulletin of Acts and Decrees (August 2017). The act is due to be implemented in May 2018. The responsible ministers of the Interior and Kingdom Relations and Defence, pressed the need to have the new act implemented, and took the necessary steps to have the law entered into force. Furthermore, the new government, who was installed late in 2017, announced it will comply with all the so-called additional guarantees in the ISS Act 2017 and committed itself to a full assessment of the law which should take place within two years after its entry into force. Public organizations have made it clear that they are taking steps to challenge particular parts of the act when it becomes applicable.

1.3 Strategic litigation, referendum

In November 2017, parliament received a letter from the government stating that finding the right people for the new oversight committee was taking more time than expected. The entry into force of the law was moved to May 2018. On the same day of the announcement of the extension, the Electoral Council decided that an official consultative referendum on the new act could take place. The organizers of the referendum, five students from the University of Amsterdam supported by NGOs among which Amnesty International, political parties, including the Party for the Animals, and media such as the Arjen Lubach show (somewhat similar to John Oliver's 'Last Week Tonight') collected more than enough votes to make this possible. The referendum will be held in conjunction with local elections on 21 March 2018. The referendum is a consultative referendum and therefore the government can opt to ignore its outcome. This is likely to happen as the new Dutch government has not only expressed that it will continue to support the new act, but also decided to end the existing system of consultative referenda.

Various organizations are considering strategic litigation in order to get more clarity about the law being in line with European jurisprudence and as to its application and conditions (i.e. on data retention). One of the initiatives is a

coalition organized by 'the Public Interest Litigation Project'. According to their website, they are considering starting a legal procedure when the law enters into force. [1]

1.4 Roadmap

In the following chapters of this policy brief, we discuss the most relevant aspects of the ISS Act 2017. We focus on oversight and the allocation/extension of power as they are at the core of many political and public debates. Where appropriate we offer a broader perspective, and provide background, including on the bottlenecks. It is not our intention to provide a full and detailed analysis of the law but rather to offer guidance to those who want to read and discuss it.

The terminology used in this document is mainly based on English documents as drafted by the Dutch Government (including the translation provided as part of the EU notification procedure)[2] and the CTIVD.[3]

1 https://pilpnjcm.nl/en/dossiers/bill-intelligence-security-services-act-wiv/ (accessed 20 February 2018).

2 http://ec.europa.eu/growth/tools-databases/tris/en/search/?trisaction=search.detail&year=2016&num=188 (accessed 10 January 2018).

3 https://english.ctivd.nl/latest/news/2016/12/07/index (accessed 10 January 2018).

2. Scope and guiding principles

2.1 Organization of the intelligence and security services

In the Netherlands, intelligence gathering for national security purposes occurs through two different organizations. The two intelligence and security services enjoy their investigative powers based on the ISS Act 2017. The General Intelligence and Security Service (hereinafter 'AIVD'/'intelligence service') is responsible for both domestic national security and for collection of information, intelligence, from abroad. The Military Intelligence and Security Service (hereinafter 'MIVD'/'intelligence service') is responsible for the safety of the armed forces, collects relevant military information and assesses the political context of foreign missions. Together, the core business of the AIVD and MIVD is to collect and process data in order to perform risk and threat assessments, to collect (foreign) intelligence, investigate individuals or organizations, protect vital sectors and conduct security screenings. Organizationally, the AIVD and MIVD are sections of larger ministries. The AIVD is a directorate-general of the Ministry of the Interior and Kingdom Relations[4], and the MIVD is a so-called special organization unit, under direct authority of the Secretary-General of the Ministry of Defence.[5] Furthermore, the services conduct their work independently of law enforcement services. Nevertheless, the act permits cooperation between the services and other branches of government, including regional and supraregional law enforcement, tax authorities, the Immigration and Naturalization Service, and inspectors of the Ministry of Social Affairs and Employment.[6]

2.2 Powers of the services

2.2.1 Regular versus special powers

The tasks of the AIVD and MIVD are statutorily defined in the ISS Act 2017. The definition of their intelligence gathering tasks is especially relevant in light of the distinction within the ISS Act 2017 between (regular) "powers" and "special powers". Although the word "special" can be used in everyday language to indicate irregularity or anomaly, the term "special" has a different meaning in the ISS Act 2017. Rather, the term refers to the requirement that a service must

4 See https://english.aivd.nl/about-aivd (accessed 10 January 2018).

5 See https://www.defensie.nl/organisatie/bestuursstaf/eenheden/mivd (accessed 10 January 2018).

6 Articles 91-95. Unless stated otherwise, references to legal provisions in this text refer to the ISS Act 2017.

be performing a certain set of tasks. The distinction between regular and special powers is intended to limit the use of certain powers to highly prioritized tasks, while regulating such powers more carefully because of their raised impact on human rights.

Regular powers include the collection of information that is available through open sources, such as public social media platforms, including Twitter or Instagram.[7] Other regular powers exist to collect intelligence from sources to which services have been granted right of access, in case of cooperation with other bodies, and via informants (any person who is considered able to provide required data).[8] A separate provision has now been introduced that allows for a collection of personal data from open sources, when such collection occurs systematically.[9] [10]

Special powers, such as conducting DNA analysis or intercepting communications, may only be applied for the performance of a narrower set of tasks, such as defending a continuing democratic legal order, protecting national security, investigating other countries and their militaries, maintaining international legal order, or specific military activities. Since the recent reform, special powers may also be applied in support of these tasks, which may result in considering security measures for certain intelligence service employees, or determining whether people involved in data collection are trustworthy.[11]

2.2.3 Examples of special powers

Encryption, decryption and back doors

Intelligence services may approach any person who is reasonably expected to be knowledgeable in deciphering communications, and order such a person to decipher them.[12] The services can issue such an order in two scenarios. The first is when services apply their special power to gain access to computerized systems or devices, for example when accessing the memory of a printer on a local area network.[13] The second is when services intercept communications, such as a satellite phone used by foreign military. In both cases, ministerial authorization and authorization is required from the Review Board for the Use of Powers

7 Art. 25.
8 Arts. 25 and 39.
9 Art. 38.
10 In order to comply with Rotaru v. Romania.
11 Arts. 8, 10 and 28.
12 Sections 3.2.5.6-3.5.2.7 .
13 Art. 45.

(*Toetsingscommissie Inzet Bevoegdheden* hereinafter (the) 'TIB') (see sections 3.2.2. and 4.3).[14] A refusal to cooperate is subject to punishment under criminal law.[15]

Security and intelligence services around the world issue such decryption orders. For example, the FBI ordered Apple to decrypt the iPhone of San Bernardino terror suspects in 2016.[16] For the services, a regulatory framework to weaken or bypass the encryption of devices or to install back doors into systems would be a more preferred solution. This would grant the services access independent of cooperation by others. Nevertheless, orders to weaken encryption or install back doors are controversial. Not only do such orders impact the privacy of citizens, they also offer opportunities for abuse by third parties, such as foreign governments, intelligence agencies and even terrorists and criminals.

With these risks in mind, the Dutch government announced in 2016 not to take any legal measures to inhibit the development and use of encryption in the Netherlands. The government also committed itself to sponsor this policy internationally.[17] Around the same time, the explanatory memorandum attached to the government proposal for the ISS Act 2017 also conceded that no orders could be issued to bypass or weaken encryption, or to install back doors. However, there was no explicit legal basis prohibiting such orders. Subsequently, the act was altered by a parliamentary amendment, now incorporating this point in the final version of the statute.[18]

DNA analysis

DNA analysis was already permitted under the previous act but this power is now codified in further detail, partially in response to case law developments at the ECtHR.[19] DNA may be retained for a period of five years, a period which may be prolonged up to 30 years. Besides the provisions in the ISS Act 2017, the government has recently proposed additional legislation regulating DNA analysis.[20] It regulates the securing, registration, analysis and profiling of DNA material for security and intelligence purposes. It also permits the comparison of collected DNA material with other DNA databanks, such as those of law enforcement.[21]

14 Sections 3.2.5.6-3.5.2.7 and art 32.

15 Art. 45 and *Parliamentary Papers* II, 2016/2017, 34588, 3, pg. 108.

16 Lichtblau & Benner (17 February 2016). Apple Fights Order to Unlock San Bernardino Gunman's iPhone. *The New York Times*. https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html (accessed 10 January 2018).

17 Government policy on encryption, *Parliamentary Papers* II, 2015/2016, 26643, 383.

18 *Parliamentary Papers* II, 2016/2017, 34588, 13.

19 S. and Marper v. United Kingdom, see par. 99.

20 Besluit DNA-onderzoek Wiv 2017 (decision DNA-research WIV 2017).

21 Art. 8(1).

Other special powers

Besides these major powers, other special powers have been codified.[22] The intelligence and security services have the power to trace and conduct surveillance, possibly through agents either working for or recruited by the services, in order to record information, for example by tracking the GPS signal of a mobile phone. Agents may also be deployed in order to promote or take measures in the interest of the services. The services are authorized, with or without the aid of a technical instrument, to conduct a search of enclosed spaces or closed objects, or to investigate of objects aimed at establishing a person's identity. Similarly, they are authorized to open letters and other consignments without the consent of the sender or the addressee. Furthermore, they may access all places to install instruments and to exercise certain other powers. Finally, services have a codified power to establish legal entities and a catch-all power to promote or implement measures to protect the interests served by a service.

2.3 Data processing

One of the most elementary regular powers of intelligence and security services is their power to process data, provided that this occurs during fulfilment of their tasks.[23] Data must be processed in accordance with the law and in a proper and careful manner. All data processed must be provided with an indication concerning its trustworthiness/reliability.[24] Some uncertainty exists with regard to data relating to individual persons ('personal data'), which is commonly processed by the services. The Dutch Data Protection Act (DPA) does not apply to the Dutch security and intelligence services, as the services are excluded from its scope.[25] The safeguards otherwise applicable to personal data processing are therefore not applicable as such. It is also unclear which data subjects may be affected by the ISS Act 2017. On the one hand, if processed data is personal, it must relate to those persons who are involved when the services are fulfilling their tasks. On the other hand, a new provision also allows services to process data of any other persons, if the data involved are a logical and inseparable part of a dataset obtained or to be obtained.[26] Because it is often difficult to determine to which person collected data belongs, the legislator believes (and the Privacy Impact Assessment on the bill (PIA) agrees[27]) that this latter category cannot be demarcated more specifically.[28]

22 Arts. 40, 41, 42, 44, 58.

23 Arts. 17 and 18.

24 Art. 18.

25 Art. 2(2)(b) Dutch Data Protection Act.

26 Art. 19.

27 This independent Privacy Impact Assessment (PIA) was conducted by TNO/Pilab. See *Parliamentary Papers* II, 2015/2016, 33820, 7 (Koops *et al.* 2016).

28 *Parliamentary Papers* II, 2016/2017, 34588, 3, pg. 45.

Another completely new provision regulates automated data analysis, such as the search for a profile picture via a search engine.[29] The legislator admits that such automated data analysis already occurs on a large scale,[30] and now provides a codified legal basis. Services are permitted to perform automated data analysis on any dataset that they can access. In accordance with the new technology-neutral approach of the regulated (new) powers (see section 2.4), a definition of "automated data analysis" has been omitted. Rather, the law states that it includes at least automated comparison of data, searching through data with aid of profiles, and attempting to find patterns within data.[31] An important safeguard exists in that the services are prohibited from promoting or taking any action against a person solely based on the results of automated data analysis. For example, if a big data algorithm indicates that a certain person intends to commit a terrorist attack, an intelligence service cannot act based on the outcome of this algorithm alone. The legislator admits that human intervention (persons taking a decision, rather than automated decision making by computer software) is always desirable and that automated decision making should be enclosed.[32]

2.4 Data transfer

Another set of powers covers the transfer of data. Internally, data may only be transferred to civil or military servants employed by intelligence and security services if such transfer is necessary for these employees to perform tasks allocated to them.[33] For transfer of data outside of the services, a more detailed framework exists. All external data transfers must be recorded, and except emergencies, must occur in writing.[34] Without permission from the responsible minister, data may not be transferred to other civil servants or public bodies, to the public prosecutor, or to any other bodies or persons involved.

More information about the processing and transfer of data can be found in subsection 2.6 and 3.4 (bulk, transfer to other agencies).

2.5 Technology-neutral approach

Recent technological advances impact not only citizens and the corporate sector, but also the work of the intelligence and security services. Because communication increasingly occurs through digital means, methods of gathering

29 Art. 60.
30 *Parliamentary Papers* II, 2016/2017, 34588, 3, pg. 171.
31 Art. 60.
32 *Parliamentary Papers* II, 2016/2017, 34588, 3, pg. 175-176.
33 Art. 61.
34 Arts. 68, 70.

data are shifting away from analogue technology towards (cable-bound) digital data traffic. This change in focus also implies that the intelligence and security services are becoming increasingly dependent on how legal provisions relate to such innovative technology. In this regard, the AIVD and MIVD have argued that they have been facing new challenges during the last few years because untargeted bulk interception of communications was only permitted for non-cable-bound communications (through satellites or (V)HF radio). Bulk interception of cable-bound communications was prohibited, even though it was an increasingly important source for intelligence services.

Despite this difference, the explanatory memorandum of the ISS Act 2002 contained no explicit fundamental rights reason to distinguish between cable-bound and non-cable-bound interception.[35] Accordingly, the CTIVD (The Review Committee for the Intelligence and Security Services) and the Dessens Committee, evaluating the 2002 act, concluded that the level of intrusion in private communications should be the main standard to determine whether or not interception was permitted, rather than the technological state of the art. Because technology is only a proxy to intrusion, the Dessens Committee proposed a technological neutrality approach, both during oversight and in determining which powers should be permitted and authorized.[36]

By avoiding arbitrary technological distinctions, the technology-neutral approach in the new act aims to provide a future-proof framework for the intelligence services. This is most noticeable in the provisions on communications surveillance, as bulk cable-bound interception is now permitted under various safeguards. Still this principle also materializes through the general duties of care which rest upon the Director General of the AIVD and the director of the MIVD, as the provisions governing these duties have been drafted with the probability of technological advances in mind. Next to the general duty to promote correctness and completeness of processed information, the heads of the services must also take sufficient measures to safeguard the quality of data processing, including the algorithms and models used.[37] This requirement falls in line with obligations to consciously consider the nature of technology involved.

The technology-neutral approach is generally considered to be a step forward in the regulation of the powers of the intelligence and security services regulation. Nevertheless, the technology-neutral approach still entails significant risks. Technological neutrality can also result in services benefitting from unintended loopholes and opportunities. However, the PIA on the bill warned that the technology-neutral approach should always be balanced versus the need for

35 CTIVD (2014) pg. xii and 33.
36 Dessens Committee (2013), pg. 79, 106 and 172.
37 Art. 24.

legal certainty. If provisions are formulated too broadly, their scope cannot be overseen.[38] Similarly, some commentators[39] have argued that technological neutrality is an excuse to substantially broaden the powers of the intelligence and security services, regardless of the need for such expansion (see section 2.6 on the power to intercept communications).[40]

2.6 Bulk collection and processing: "investigation-related purpose"

The ISS Act 2017 has provided a considerably reformed communications interception system. On the one hand, the intelligence and security services are furnished with a legal basis to perform interception of (cable-bound and non-cable-bound) communications when such interception is targeted at specific persons, organizations, numbers (such as a telephone number) or other technical characteristics involved. This special power and the safeguards in place have remained largely the same.

On the other hand, perhaps the most fiercely debated reform was the introduction of the power to perform bulk communications interception.[41] This despite the fact that its existence was a public secret long before the Wikileaks and Snowden revelations and the ISS Act 2017: In the late 1990s, the so-called ECHELON system affair, which involved electronic cooperation and spying though signals intelligence (SIGINT) by the Five Eyes[42] intelligence alliance, had already caused great uproar in the EU with regard to communications surveillance.[43]

In reviewing the communications interception system, the Dessens Committee had in 2013 *already* concluded that the previous provisions for untargeted interception by the AIVD and MIVD had been formulated in a highly technology-dependent manner.[44] For example, the previous provisions used the term "military message traffic", implying a constant stream of messages in Morse or some other outdated code. Similarly, the previous system allowed for the surveillance of both cable-bound and non-cable-bound communications,

38 Koops *et al.* (2016), pg. 148, also pg. 14 public consultation response Netherlands Institute of Human Rights.

39 Jacobs (2016) pg. 257; Public consultation response KPN, pg. 5 onwards; Public consultation response, Amnesty International pg. 3 onwards; Public consultation response Nederland ICT, pg. 12 onwards.

40 *Parliamentary Papers* II, 2016/2017, 34588, 3, pg. 298.

41 Art. 48.

42 The Five (or Nine/Fourteen) Eyes agreement consists of 'FVEY' countries, Australia, Canada, New Zealand and the Unites States of America cooperate in signals intelligence (SIGINT). The Netherlands was added later to the agreement and is part of Nine Eyes.

43 Piodi & Mombelli (2014), The ECHELON Affair: The EP and the global interception system 1998 - 2002, Historical Archives Unit of the European Parliament European Parliament History Series November 2014, PE 538.877.

44 Dessens Committee (2013), pg. 171.

but permitted bulk interception and selection only for non-cable-bound communications. By allowing any indiscriminate, untargeted, bulk interception directed towards an "investigation related purpose" irrespective of the type of communications, the technology-based distinction has been removed. In other words, the services will be able to perform non-discriminatory communications interception in the future using any available technology.

What exactly is meant by an "investigation related purpose"? According to the law, every four years (but in reality every year), the Prime Minister, the Minister of the Interior and Kingdom Relations and the Minister of Defence together produce a (revised) policy document to inform the intelligence and security services of which priorities exist when performing the tasks for which the use of special powers is permitted.[45] In this legally binding document, the responsible ministers include the investigatory assignments that the services must perform during the four-year period. As assignments need to be given for such a relatively long period, they are expected to be broad in scope. However, these assignments can (and are) further detailed based on proposals by the parliamentary oversight committee or in ministerial guidelines and other types of lower regulation. For example, the explanatory memorandum mentions explicitly the discretionary power of each minister to give additional immediate investigatory assignments.[46] In short, the additional requirement that interception should have an investigation related purpose is somewhat meaningless as a similar requirement is more or less encapsulated in this assignment procedure itself.

The legislator has attempted to maintain a technology-neutral approach for communications interception by introducing a model with three pre-analysis phases: the collection, pre-treatment or searching and selection of communications data.[47] Each phase has different requirements, is bound by a higher level of safeguard (such as additional internal permissions) and is intended to fulfil a different role in working towards the investigation related purpose. The legislator maintains that although separate, the three phases are closely interrelated and will constantly influence each other.[48] In the consultation procedure however, the CTIVD (oversight body, see section 4.5) questioned whether the services will be able to apply these three phases separately at all.

45 Art. 6. In Dutch *'Geïntegreerde aanwijzing'*.
46 *Parliamentary Papers* II, 2016/2017, 34588, 3, pg. 31 and 118.
47 See also: Fundamental Rights Agency (2017), pg. 31.
48 *Parliamentary Papers* II, 2016/2017, 34588, 3, pg. 126.

Having consulting with experts in communication technology, the CTIVD now emphasized that in practice, acquisition, pre-processing and processing will not be separate processes that occur in consecutive order but will rather run in parallel to one another and constantly influence each other.[49]

The Council for the Judiciary, the Netherlands Bar Association, the Netherlands Institute for Human Rights, NGOs including Amnesty International, Bits of Freedom, the Dutch Commission of Jurists (NJCM), Internet Society the Netherlands, Free Press Unlimited and Privacy International, but also internet companies and providers of telecommunication services have carefully scrutinized issues such as the power to intercept communications for investigation related purposes.[50] Some of them refer to "dragnet surveillance". Before all else, many question the need for the new (special) powers, whereas others focus primarily on sufficient checks and balances. This is probably partly because they interpret the concept of (bulk) communications interception differently from those involved in intelligence and security, who emphasize that the real intrusion takes place in the analysis phase and to a lesser extent in the collection phase. Subsequently, those opposed to bulk communication interception portray this power as a disproportionate infringement of human rights and/or argue that the accountability system is insufficient. An adopted parliamentary motion, reflecting these concerns, and requiring the intelligence and security services to employ communications interception in a most targeted fashion, was rejected.[51] Nonetheless, the explanatory memorandum to the ISS Act 2017 holds that decreased opportunities for targeted interception, the unknown character of certain threats, cooperation with foreign intelligence services and cyberthreats each demand untargeted bulk interception for investigation based purposes. Furthermore, the provisions include various types of safeguards, including authorization mechanisms, a time limit for the various types of data retained, and limits in the access to data, with the intention to segregate knowledge obtained during the various phases from the persons exerting other (special) powers, duration of the data retention, and on data minimization (irrelevant data needs to be destroyed). On the other hand, the law provides a simple procedure to extend the scope of a given permission.

49 CTIVD (2015).

50 See for example their interventions during the public consultation (only in Dutch): https://www.internetconsultatie.nl/wiv/reacties (accessed 21 February 2018).

51 *Parliamentary Papers* II, 2016/2017, 34588, 66.

The new government, installed in October 2017, has stated in its political program that it will comply with all the additional guarantees in the ISS Act 2017 and excludes the possibility of a "dragnet".[52] Also, a full assessment of the law should take place within two years of its entry into force. Depending on the outcomes of the assessment, additional guarantees and oversight might also be put into place.

2.7 Gaining access to computerized systems or devices: hacking

The services have the special power to gain access to computerized devices or systems, such as mobile phones, computers or their peripheral devices. This is also referred to as the hacking power. In preparation, the services can explore technical characteristics of computerized devices or systems, for example by discovering relevant IP addresses with the aid of scanning software. Access may then be gained via auxiliary tools (such as malware), false signals, false keys, false representations, but also via interference of a computerized device or system of a third party. Computer or device security measures may be bypassed or broken. Subsequently, data on the device may be copied and saved. In case data is encrypted, software may be installed on the device to decrypt them. Also, software may be installed in order to exercise other special powers such as device tapping (therefore including the possibility of real-time surveillance).[53]

The provision allowing interference via a device of a third technically related party, who is not a target, is new and has received considerable political attention. The explanatory memorandum states that this provision allows services to commence by gaining access to a third-party device, in order to gain access to the targeted device only afterwards. The legislator argues in its explanatory memorandum that interference by third party devices is often technically crucial, that its prohibition would render the special power to access target devices meaningless, and that interference via third party devices is currently already the method used in the vast majority of cases.[54] A parliamentary amendment to the bill proposed by the government, aimed at enhancing subsidiarity and proportionality, was rejected.[55] Nonetheless, during the parliamentary debate the government confirmed that a third party hack can only be applied if a direct one is not possible.

52 'Confidence is the Future', Coalition Agreement 2017 – 2021, VVD, CDA, D66 and Christen Unie, 10 October 2017, pg. 4; confirmed and more detailed in a letter to parliament (*Parliamentary Papers* II, 2017/2018, 34588, 69). For English see https://www.government.nl/documents/publications/2017/10/10/coalition-agreement-confidence-in-the-future (accessed 21 February 2018).

53 Art. 45.

54 *Parliamentary Papers* II, 2016/2017, 34588, 3, pg. 102 onwards, and pg. 304 onwards.

55 *Parliamentary Papers* II, 2016/2017, 34588, 48.

This is in line with the opinions of the CTIVD in one of its reports.[56] Another aspect, the use of these third-party hacks for surveillance purposes, is already excluded in the law.[57]

Various internet consultation respondents are concerned that there is no need for interference in devices, despite existing risks. The use of malware and the exploitation of zero days (undisclosed software vulnerabilities) arguably have unforeseeable and far-reaching effects. NGOs, professional organizations, private companies and the CTIVD are especially worried about the implications for the integrity and trustworthiness of the internet generally and connected ICT systems.[58] Risks to critical infrastructures, such as power stations or the Delta Works which protect the country against flood, should be minimized to the greatest extent possible. As a safeguard, the new provision requires that a request for authorization of this special power includes a description of the technical risks involved. Also, a codified duty of commitment requires the services to attempt a removal of auxiliary tools.[59] The explanatory memorandum further concedes that the government will generally inform interested parties of significant software vulnerabilities. Yet simultaneously, the explanatory memorandum argues that legal arguments (including the protection of sources or maintaining a certain level of know-how) or operational reasons may exist which will inhibit public disclosure.[60]

2.8 Cooperation by third parties

Providers of communications services have an obligation to assist the intelligence and security services.[61] This obligation is linked to the executing of the (special) powers defined in the ISS Act 2017. Compliance with the obligations by, for example, tech or social media companies exempts them from further liability. No specific remedies are provided when these third parties have objections against the requested cooperation or when they have doubts about the underlying legitimacy of the imposed measures. Costs linked to the cooperation are covered by the State and regulated via a special ordonnance. The compensation excludes the costs of ordinary wiretapping of public telecommunications networks as these costs are covered by the Telecommunications Act.

56 CTIVD (2017) (3).
57 Art. 45, par. 5.
58 *Parliamentary Papers* II, 2016/2017, 34588, 3, pg. 305 onwards.
59 Art. 45.
60 *Parliamentary Papers* II, 2016/2017, 34588, 3, pg. 306 onwards.
61 Arts. 51-57. Also see par 2.2.3.

The controversy about the 'iPhone case' in the United States resulted in an amendment modifying the provision on cooperation to decrypt communications.[62] In the 'iPhone case', law enforcement services tried to force Apple engineers to break the encryption of a particular iPhone. In the new act, if a third party has knowledge about the encryption or has the decryption key, they are obliged to provide this knowledge/key to the intelligence services. However - and this is due to the amendment no. 13 - the cooperation cannot include the weakening of the encryption or the manufacturing of access to systems to gain access to encrypted data.

62 Art. 57.

3. Political and internal accountability

3.1 Introduction

Because the ISS Act 2017 is mainly about the use of powers by the security and intelligence services, accountability for the executive is crucial. Both the responsible ministers as well as the AIVD Director General and the MIVD director and the civil or military servants bear responsibility. Even though accountability is broader than working on the basis of the law, it is sometimes difficult for outsiders to understand why people working within the intelligence and security system perceive external accountability as challenging. For them, internal accountability - the relationship with their superiors higher-ups, legal and ethics training and internal procedures - are probably the most important form of accountability. It is equally difficult that the outside world does not understand that "this is very time-consuming" and "we are just doing our job". Henceforth, being accountable to members of parliament, politicians, oversight bodies, NGOs or journalists may necessitate a response to questions from non-national security experts. Yet, these "outsiders" often have less faith in the legitimacy of (secret) practices of security and intelligence services. Because even though information gathering is based on law, outsiders simply do not trust that secret agents who are more directly controlled by the involved service, or online or offline informants are (always) prone to do the 'right thing' and thereby defend democracy. The Dutch context is no exception to this dilemma and this is reflected in how political and internal accountability mechanisms are structured.

3.2 Accountability of the intelligence services

3.2.1 Organization of the intelligence services

As mentioned before, the AIVD and MIVD are not individual organizations that stand alone but rather are a part of the two ministries involved (par. 2.1). Considering their position within umbrella organizations, internal oversight is primarily provided by the Minister of the Interior and Kingdom Relations and the Minister of Defence. On paper, the Secretary-General[63] of the Ministry of General Affairs also plays an important role. As the highest civil servant in Dutch government, he or she presides over the so-called Intelligence and

63 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.

Security Services Committee, which consists of assigned high-ranking civil servants from various other ministries.[64] Both services are under a legal obligation to cooperate as much as possible.[65]

3.2.2 Executive authorization

As the intelligence and security services operate under the direct authority of the two responsible ministers, all their actions take place under full ministerial responsibility (see section 3.3). Therefore, the ISS Act 2017 requires prior ministerial approval for many special powers. However, the law offers extensive options to delegate responsibilities. Nonetheless, the application of many of these special powers not only needs prior consent of the minister, but also requires an additional prior consent from the District Court of The Hague or the new Review Board TIB (see chapter 4).

3.2.3 Duty of care

The intelligence and security services are subjected to various duties of care. The general duty of care on the processing of data bears some similarities to the data protection law, but is special within the intelligence context because it requires an appropriateness review to be conducted by the services themselves, rather than by oversight bodies or the legislator.[66] The question remains who should maintain oversight over this normative review. One parliamentary amendment that was rejected proposed to grant such authority to the CTIVD as it has been argued that they already have an extensive oversight power.[67] Indeed, the CTIVD is conceivably the appropriate body to take up such responsibility, because this external oversight body has permission to view all internal documents of the AIVD and the MIVD as part of its oversight capacity.

The PIA on the bill had recommended a provision on data privacy by design and by default: the inclusion of technical requirements on design, user (in) capabilities, default settings and transparency when data processing systems are procured and installed.[68] The legislator deemed that such a provision would be too extensive because the act already has provisions that include tailored privacy safeguards, making a general privacy by design and by default superfluous.[69] Alternatively, the act now includes a general duty of care borne by the heads of the security and intelligence services. As senior civil or military

64 Arts. 1-5.
65 Art. 86.
66 Art. 24.
67 *Parliamentary Papers* II, 2016/2017, 34588, 30.
68 Koops *et al.* (2016), pg. 151.
69 *Parliamentary Papers* II, 2016/2017, 34588, 3, pg. 48.

servants at the Ministry of the Interior and Kingdom Relations and the Ministry of Defence, the Director General of the AIVD and the Director of the MIVD must ensure that the technical, organizational and personnel-related measures taken when processing data are in accordance with the act.[70] Compliance with this requirement falls within the scope of the regulated oversight and in a letter to parliament, the government has committed itself to providing oversight with an "adequate set of instruments".

The duties of care include various sub-duties. One such sub-duty requires the heads of the intelligence and security services to take sufficient technical and organizational measures to avoid data breaches. Another sub-duty is that the Director General of the AIVD and the Director of the MIVD must ensure the correctness and completeness of processed data, and should take sufficient measures to safeguard the quality of data processing, including the algorithms and (behavioural) models used. By covering algorithms and models, the legislator intends to take a technology-neutral approach (see section 2.5). This sub-duty nicely complements obligations such as the requirement to include a description of the technical risks involved when applying for special power authorization (see section 2.7 on hacking). Together, such obligations will ensure that the heads of the AIVD and MIVD regularly consider the nature of technology involved and allow the CTIVD to oversee the accurate implementation of these obligations.

3.3 Ministerial/executive responsibility

3.3.1 Lawfulness versus appropriateness

The Netherlands attaches great value to the separation of powers more or less in line with the Montesquieu model. The executive powers are in the hands of the King and the government, while the legislative power rests with the government and parliament (both can propose legislation, only parliament can adopt it), and the independence of the judicial powers is reflected in a multi-layered civil and administrative court system. Nevertheless, this governance system has been challenged several times and the Netherlands was forced to make changes. The changes also affect the work of intelligence services. In the ECtHR 2010 Sanoma case, it became clear that the public prosecutor is part of the executive and not of the judiciary. Therefore, a search of the offices of a publisher needed the prior approval of an independent judge.[71] Similarly, the executive cannot order the secret surveillance of a journalist to find a source within the intelligence service, without the interference of the judiciary.[72] The

70 Art. 24.
71 Sanoma Uitgevers B.V. v The Netherlands.
72 Telegraaf and Others v. the Netherlands.

two cases are the consequence of a problematic Dutch doctrine on "ministerial independence". How can the executive take responsibility if it requires the prior consent of a judge? Why can the executive not decide independently of the legislator and judiciary regarding whose conversations should be listened into? The answers, as we can also learn from the Court in Strasbourg, are relatively simple: the protection of fundamental rights cannot be bypassed by the executive nor can the executive have uncontrolled powers. To stick with surveillance: it's the government and its services that decide on who to surveil, it's up to the courts to decide - *ex ante* or sometimes ex *post* - whether it's justified.

But even if courts have this role to play, the Dutch model attaches great value to the difference between assessing the lawfulness of a decision or measure and the its appropriateness. According to some, the courts can only deal with the lawfulness and have no authority over the appropriateness.[73] In the case of (communications) surveillance, this would mean that courts can only assess whether an interference meets the (formal) requirements of the law. Here again, the Strasbourg jurisprudence makes clear that courts must also consider the appropriateness when looking at the proportionality of a measure.[74] The ISS Act 2017 struggles with this and the parliamentary process shows that the government had mixed feelings about it. Nevertheless, the law does have several provisions that directly or indirectly require testing the appropriateness. See, for example, the duty of care for the services (see section 3.2.3), while article 26 contains a proportionality test. Various amendments were introduced to deal with the relationship between lawfulness and appropriateness. All of them were rejected. However, Parliament did adopt an important motion stating that the principles in the law of necessity, proportionality and subsidiarity also apply and need to be used as requirements for for maximum focus on the use of powers.[75] It will now be up to the courts and the oversight committees to apply this proportionality test.

3.3.2 Relationship between the executive and the intelligence services

A second consequence of the services' symbiosis with the other ministries is that the MIVD and AIVD are held politically accountable via the individual ministerial responsibility. The Dutch parliament may question the responsible minister on the conduct of the intelligence and security services. If dissatisfied with a minister's response, parliamentarians may hold a vote of no-confidence as an ultimate measure, requiring that the minister resign. In 2014, the responsible

73 On this issue: Konijnenbelt & van Male (2014), pg. 522.

74 See for example Zakharov v. Russia. In this case, the Court brings together large parts of its previous jurisprudence on secret surveillance.

75 *Parliamentary Papers* II, 2016/2017, 34588, 66.

Minister for the Interior and Kingdom Relations survived such a vote of confidence related to him allegedly misinforming parliament about a matter of national security. In practice, the Secretaries-General of the two ministries and the Director General of the AIVD and Director of the MIVD bear much of the political ministerial responsibility. Because of their proximity to the ministers, they fulfil a vital role in briefing on relevant matters.

3.4. International cooperation

The structural exchange of processed and unprocessed data is one of the most far-reaching forms of cooperation between the Dutch services and services in other countries. If no adequate safeguards exist, intelligence and security services risk circumventing domestic surveillance procedures through weaker foreign counterparts. The CTIVD has paid increasing attention to the international cooperation of Dutch intelligence services, not least because of the Snowden revelations. International cooperation involving the general and military intelligence and security services has also been an issue in Dutch parliament. Consequentially, the ISS Act 2017 codifies and slightly expands a previously existing procedure that ascertains whether foreign intelligence services are adequate cooperation partners. Furthermore, the act provides additional safeguards for the transfer of both processed and unprocessed data with foreign intelligence and security services.

3.4.1 Adequacy procedure

The establishment of cooperative relationships between the AIVD and MIVD and foreign intelligence services has become subject to an adequacy procedure. The responsible minister must authorize cooperation before this takes place. Authorization is contingent on a balancing exercise of five criteria: a) the "democratic embedding" of the intelligence and security services in the country concerned; b) the respect for human rights in the country concerned; c) the professionality and reliability of the service concerned; d) the legal powers and possibilities of the service in the country concerned; and e) the level of data protection maintained by the service concerned. The Director General of the Dutch intelligence and security service is obliged to re-evaluate the cooperative relationship with the foreign intelligence services if changing circumstances require such a re-evaluation. The procedure already existed under the ISS Act 2002, although limited to the first three criteria, and without an explicit legal basis. Notable in this regard is a CTIVD investigative report from 2016, indicating that the (previously informal) balancing exercise received little attention until 2015.[76] Furthermore, the CTIVD concluded that in balancing acts performed

76 CTIVD (2016) (3).

since 2015, information of fundamental importance was missing and that the information used was often superficial and insufficient.

In light of the Snowden revelations, the CTIVD had previously already advised the government to reconsider its relationship with the most trusted foreign intelligence and security services. The inclusion of the two added criteria (the legal powers and possibilities of the foreign intelligence service and the level of data protection maintained by the service) in the act provides a higher standard for such re-evaluation. The installation of the procedure is subject to a two-year transitional period during which no formal requirements will be in place for existing international cooperation. No apparent grounds exist to justify such a transitional period, which is probably why the new government has committed itself to have necessary assessments made of the most trusted foreign partners when the law enters into force.

3.4.2 Requests from foreign services

Another explicit legal basis that was missing under the previous act is for requests for (operational) support from Dutch services to foreign intelligence and security services. If Dutch services request support when applying special powers for which permission has already been granted, the services must request additional permission. If the Dutch intelligence and security services make a request that foreign services apply special powers or certain other powers, the Dutch services must first request permission as if they would apply the powers themselves. Granted permission then makes exercise of the special powers abroad as covered by Dutch law. In such cases, the permission granted may never exceed the powers granted to Dutch services. A general safeguard applicable to all requests is that permission must always be granted by the responsible minister if the request exceeds the nature and intensity of the cooperative relationship. However, these requests cannot include offering support to foreign services to independently collect information on Dutch soil. An amendment by Parliament explicitly excludes this option.[77]

3.4.3 Cross-border data transfer

For the Dutch intelligence and security services to fulfil their tasks, both evaluated and unevaluated (raw) data may be transferred to foreign services with whom a cooperative relationship exists. The responsible minister should authorize such transfer – in case of transfer of unevaluated data and in case no formal cooperation exists - and the CTIVD must be notified about the transfer of unevaluated data collected through bulk communications interception.

77 *Parliamentary Papers* II, 2016/2017, 34588, 31.

Furthermore, such transfer is only allowed under the "third party principle": the foreign secret service must consent to withhold any further transfer. In the fulfilment of the Dutch secret service's tasks, data may be transferred by Dutch services to any foreign intelligence service, with whom no cooperative relationship exists. In that case, the transfer remains subject to authorization from the responsible minister, requires an urgent and important reason and must be reported to the CTIVD if the data has been obtained through untargeted interception of communications (see section 2.6). Regardless of whether a cooperative relationship exists, if data is processed more than ten years previously, or its correctness cannot reasonably be assessed, the transfer must be accompanied by a comment on the data's reliability. Also, transfer must always be registered.

Dutch intelligence and security services may also transfer processed data through a cooperative relationship to serve interests of foreign services. In such a case, the requirements of registration and commenting on the data's reliability are applicable. Two additional requirements exist. Cross-border data transfer to foreign services may only occur if the interests served by the foreign service is not irreconcilable with the interests served by the Dutch service, and the transfer does not detract from a proper performance of the tasks of the Dutch service. Dutch services may similarly transfer raw (unevaluated) data, for no longer than twelve months after authorization. We note that interception of bulk data is subject to prior authorization by the TIB, but the transfer of these data to other countries falls outside the scope of prior independent oversight (see section 5.4).

4. Oversight and access to justice

4.1 Introduction

Existing accountability mechanisms have, to a great extent, been preserved or somewhat amended in the ISS Act 2017. As appears in more detail below, the recent reforms have blurred the boundaries between oversight and authorization. The section below discusses both authorization and oversight mechanisms separately, while showing how they increasingly interact.

Furthermore, external judicial review has also been strengthened. This is an interesting and welcome development in light of previous incidents involving journalists and lawyers in the Netherlands. Journalists of the Dutch national daily newspaper De Telegraaf brought proceedings before the ECtHR after being ordered to surrender secret documents in their possession. Previously the journalists had published articles suggesting that highly secret information had been leaked from the AIVD to the criminal circuit, and more precisely to the drugs mafia. Allegedly, the two journalists subsequently became subject to special powers (telephone tapping and observation) by AIVD agents, which were directed specifically at uncovering their journalistic sources. In its 2012 judgment, the Court concluded that Dutch law had failed to provide ex ante judicial review, therefore violating the journalists' right to privacy and freedom of expression.[78]

4.2 Prior judicial consent: district court of The Hague

If deployment of the special power might compromise the attorney-client privilege or is directed at a journalist and may reveal a journalist's source, the minister granting the permission must request additional permission from The Hague District Court. The latter safeguard is most welcome in light of ECtHR cases such as the previously mentioned case De Telegraaf v. The Netherlands and has been confirmed by Dutch Courts: It was the District Court of The Hague that ordered the Dutch State to implement a provisional independent oversight procedure because the ISS Act 2002 Act failed to provide for it.[79] In order to comply with the court's decision, a ministerial order appointed the chair of the CTIVD as the person responsible for giving prior consent.

78 Telegraaf Media v. The Netherlands, par. 102.

79 District Court of The Hague 1 July 2015, ECLI:NL:RBDHA:2015:7436.

Under the ISS Act 2017, the responsible minister must now submit a motivated request to the court, detailing, for example, what aims are to be achieved and why deployment of the special power is necessary. He or she must also indicate whether the target is a lawyer or a journalist.

There is a third category of surveillance requiring the prior consent of the court. Article 13 of the Dutch Constitution only allows opening letters based on a court order. This also includes opening letters by the intelligence and security services. A proposal is pending to change this provision in the constitution by a more generic article extending the scope of communications secrecy to all types of communications. However, limitations no longer exclusively require the prior consent of a judge but may - in the context of national security - also be transferred to 'those appointed by law'. Although this proposal dates to 2013 - before the Strasbourg court decision - the text has not been changed and seems therefore in conflict with this jurisprudence as it does not offer the necessary guarantees on oversight and due process.

4.3 Prior judicial consent: the Review Board for the Use of Powers

Another considerable improvement in authorization that contains elements of judicial review has been made with regard to the employment of special powers generally. The reforms have introduced an additional legally binding prior review to be made by an independent and specialized judicial commission, the Review Board for the Use of Powers (TIB). In the initial version of the act in 2015, the prior consent for the deployment of the special powers was limited to the pre-existent regular executive decision. Despite some extra safeguards, a considerable number of persons and organizations complained during the public consultation about the lack of prior judicial consent.[80] In response, the legislative proposal was amended. The use of special powers was already subject to ministerial authorization, but now also requires an additional assessment focussing on lawfulness and motivation by the TIB.

Because the TIB can refuse authorization to the intelligence and security services, and no appeal procedure exists, a heavy responsibility rests on the shoulders of the TIB members. Although at least two TIB members are required to have considerable experience as a judge, are appointed by the government at the Parliament's recommendation and have authority to revoke an executive decision, there is some debate whether or not this review should be classified as prior judicial consent from a fundamental rights perspective.[81] Furthermore, the Council of State has observed that it is uncertain whether or not the

80 *Parliamentary Papers* II, 2016/2017, 34588, 3, pg. 49.

81 Netherlands Institute for Human Rights 2015, pg. 40; ISS Act 2017, arts. 29-36.

TIB will have enough technical expertise to fulfil its duties.[82] Although the explanatory memorandum mentions that the third appointed TIB member could have sufficient technical insights,[83] no such codified requirement exists, and a parliamentary amendment allowing TIB members to consult experts was rejected.[84] On top of the expertise issue, the TIB does not have the power to autonomously examine existing files of the intelligence services despite being in the position to request more information and the services having to provide that information.

The combination of all these problems will determine much of the TIB's future practice. Experience can be drawn from the United States Foreign Intelligence Surveillance court (FISC), which is authorized to oversee requests for surveillance warrants against foreign spies inside the United States by federal law enforcement and intelligence services. Problems relating to a lack of expertise have previously led critics to argue that the FISC is simply a rubber-stamping mechanism.[85] Strasbourg jurisprudence has made clear that rubber-stamping cannot suffice. If essential facilities are withheld from the TIB, it may have no choice but to refuse permission in many cases.

4.4 Parliamentary oversight

As the security and intelligence services are organs within ministries, and responsible ministers can be held accountable before parliament (see section 3.3 on ministerial responsibility), parliament functions as an oversight mechanism. Two parliamentary commissions primarily focus on general issues. The first is the Committee on Home Affairs, the second is the Defence Committee. Furthermore, parliament has a special Committee for Intelligence and Security Services (Commissie voor de Inlichtingen en Veiligheidsdiensten, CIVD (publicly known as 'the Secret Commission') and is composed of the leaders of the five largest political parties in the House of Representatives. As a rule, all information is made available to the Committee on Home Affairs regarding the AIVD and to the Defence Committee regarding the MIVD. Information that is classified above the "restricted" level is shared only with the CIVD.

Although the existence of the CIVD inhibits disclosure to the whole parliament, its existence has ensured that information requested by parliament has never been withheld on state secrecy grounds, a right formally granted to ministers under the Dutch Constitution.[86] Effective oversight is therefore not hindered by

82 Advice Council of State, *Parliamentary Papers* II, 2016/2017, 34588, 4.

83 *Parliamentary Papers* II, 2016/2017, 34588, 3, pg. 67.

84 *Parliamentary Papers* II, 2016/2017, 34588, 36.

85 Mears & Abdullah (17 January 2014).

86 Art. 68 Dutch Constitution, and ISS Act 2017, *Parliamentary Papers* II, 2016/2017, 34588, 3, pg. 229.

a lack of information. Still, the CIVD might not be fully equipped for effective oversight because the Commission is relatively small and composed of members who are under time pressure and who are usually not experts in this field. Furthermore, members are under the obligation to maintain the confidentiality of such information, even towards their own political parties, which means that they cannot entrust others with oversight work.

4.5 External oversight: the Review Committee for the Intelligence and Security Services

The Review Committee for the Intelligence and Security Services (CTIVD, Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten) has become an influential external oversight committee since 2002, relatively stronger than parliamentary and, perhaps also judicial oversight.[87] Since its introduction, it has reviewed Dutch intelligence and security services' compliance with the law, but not their effectiveness or efficiency, through instruments including oversight review reports, solicited and unsolicited advice and annual reports. To conduct their assessment, the oversight department of the CTIVD has direct (digital) access to classified information kept by the AIVD and MIVD. Intelligence service employees are required to cooperate. The review reports may have confidential and public sections, and assess topics including operations, administration, policies and both national and international cooperation. In follow-up, the responsible minister is required to either endorse the findings and recommendations of the CTIVD or to put them aside. The CTIVD is also backed by an external knowledge network, which provides critical advice on contentious matters.

The ISS Act 2017 has extended the powers of the CTIVD and increased its budget.[88] The CTIVD had previously called for more effective oversight of automated data processing and analysis phases.[89] In response, the legislator has now provided resources for the CTIVD to install an IT expertise unit, with the aim of improving oversight and system review in this regard.[90] Another substantial increase in power involves the establishment of a second CTIVD branch, separate from the oversight department, which will function as a quasi-judicial body to provide a binding remedy for a (suspected) grievance.[91] Whereas previously the CTIVD advised the minister concerned on how to handle complaints, it now deals with such complaints itself.

87 CTIVD 2012; Art. 95 and 110-111.
88 *Parliamentary Papers* II, 2016/2017, 34588, 57.
89 CTIVD (2016); CTIVD (2017) (1).
90 CTIVD (2016) (2), pg. 36. See also Explanatory Memorandum, pg. 176.
91 Arts. 95 and 112-122.

The role of the Ombudsman as an independent mechanism between complainants and the government thereby ceases to exist.

4.6 Netherlands Court of Audit

With regard to judicial oversight, ordinary civil, administrative and criminal courts also play a role. For example, administrative courts may review decisions made about individuals' requests for access to data.[92] The Netherlands Court of Audit holds the services accountable for expenditure. It not only monitors the costs of public expenditure, but also has the authority to examine the effectiveness of such expenditure. Accordingly, the Netherlands Court of Audit is also in the ideal position to assess whether sufficient funds are provided for oversight purposes.[93]

4.7 Binding complaints procedure

A binding complaints procedure is the new remedy for addressing a (suspected) grievance against individuals or specific networks/organisations. Complaints can be lodged by both individuals and organisations ("action popularis", the latter being made clear in parliament during the discussions on the law).[94] In the past, most complainants relied on the CTIVD procedure, who advised the responsible minister on what to do. Also, in the new act, the Ombudsman will no longer play a role. The newly established second CTIVD branch, the Complaints Department, separate from the oversight department, will provide for the binding complaints procedure.[95] In order to do so, this quasi-judicial body must be able to hear the complainant, examine the files of the involved intelligence and security service and hear its civil or military servants. The written complaint must meet several criteria. The most relevant are a description of the (alleged) personal infringement, whom it concerns, the conduct of the civil or military servant in question and the person whom it affects, as well as the grounds for filling the complaint.

Subsequently, the complaint is handled by three members of the CTIVD complaints department. After hearing the complainant, examining the files of the involved intelligence and security service and hearing its employees, the members assess whether it is founded. The basis used is whether the conduct of the AIVD or the MIVD was proper, which includes lawfulness.

92 *Parliamentary Papers* II, 2016/2017, 34588, 3, pg. 223.

93 The national budget of 2018 shows that the intelligence and security services receive up to 353 million Euro. (AIVD approximately 250 million Euro and MIVD 103 million Euro), whereas oversight bodies receive 3.2 million Euro, National budget 2018. See also letter to parliament (*Parliamentary Papers* II, 2016/17, 34588, 67).

94 *Parliamentary Papers* I, 34588, E.

95 Arts. 97 and 114-124. See also General Administrative Act 1992, art. 9:28, 9:29 and 9:30. The complaint procedure is based on that.

By focusing on lawfulness, the complaints procedure is comparable with other Dutch complaint procedures. If the complaint is either partly or fully founded, the responsible minister can be ordered to remedy the infringement by stopping an ongoing investigation, ending the use of a special power or deleting and destroying processed data. However, the complaints department remedial powers do not include the allocation of damages. A complainant will need to initiate civil action for damages against the state.[96]

4.8 Whistle-blower procedure

Furthermore, the ISS Act 2017 now has a dedicated whistle-blower procedure. Public officials of the intelligence and security services and other persons, who have been involved in implementing the act or a security screening, can report (alleged) abuse to the CTIVD complaints department.[97] These other persons may include for example the personnel of internet or telecommunications companies. Although whistle-blowers are expected to start by addressing the issue internally, if there are reasonable grounds for not doing so, the CTIVD complaints department can address the alleged abuse directly. The CTIVD complaints department assesses whether the written complaint is admissible and whether the allegations are reasonable. In such an investigation, the CTIVD has permission to view all internal documents of the intelligence services and hear those involved. The whistle-blower and the responsible minister may then respond to the draft report about the investigation. However, the report is only available to the whistle-blower at the CTIVD office. The final report determines whether the reported abuse is wholly, partially or not founded, and the outcome is communicated to both parties. It is sent to the responsible minister, who is required to respond to the CTIVD as well as the whistle-blower within two weeks. He or she is under no obligation to remedy the situation or comply with possible CTIVD recommendations.[98] Ministers can however be held accountable before parliament.

4.9 Transparency

In the law, transparency regarding the activities of the intelligence and security services is rather limited. Amendments to enhance transparency were rejected. Each year, the responsible ministers send a public report to parliament about the activities of both the AIVD and MIVD. By law, this report cannot contain information on the specific application of powers, secret sources or the knowledge level of the services or provision on transparency. Such information

96 *Parliamentary Papers* II, 2016/2017, 34588, 3, pg. 239.
97 Art. 125-131.
98 ibid.

may be provided in confidence.[99] The CTIVD and TIB are also under obligation to report about their activities on an annual basis.

Requests for information can be made based on special provisions in chapter 5 of the act. Most provisions relate to personal data, but requests can also be made to gain access to other information. Virtually identical provisions were part of the previous ISS Act 2002 and have resulted in both granting and refusing access. When 'other' information is requested, one of the important reasons for refusal is the national security exception. In a December 2017 case, the Council of State decided that this exception needs to be substantiated.[100] NGO Bits of Freedom was refused information about so-called 'tap statistics' based on the exception. Therefore, the Council of State has obliged the responsible ministers to take a new decision taking into account, for example, the fact that this kind of information is being made available in many other countries. Since then, the Minister of the Interior and Kingdom Relations and the Minister of Defence have decided that the 'tap statistics' will be published annually.

The Dutch Freedom of Information Act (WOB, 'Wet Openbaarheid van Bestuur') has also been used as a basis to gain information on national security matters. However, as is the case with most of these laws, it has national security as an exception. This exception has been used to refuse access to information in many cases. Several of them have been tested in court with varying success.

It does not address circumstances under which third parties can make public statements about their involvement with the intelligence services. On the contrary, chapter 8 of the ISS Act 2017 makes clear that such involvements must be kept secret. Consent is required from the responsible minister before secret information can be made available to third parties, including courts. In earlier responses to questions of parliament, the government has made clear that it sees every publication by third parties without its consent as a potential infringement of the law. Companies and individuals therefore have very few incentives to become involved in so-called 'transparency reporting'.

99 Art. 12.

100 Council of State 20 December 2017, ECLI:NL:RVS:2017:3508.

5. Bottlenecks

5.1 Introduction

In this final chapter, the authors wish to reflect on a number of bottlenecks in relation to the ISS Act 2017. Although the authors take full responsibility for the analyses, most of them are shared by other parties. Secondly, our comments focus primarily on the system of checks and balances of the law. Although the lawmakers maintain that the law is human rights proof,[101] from a legal perspective one can raise questions about this. Furthermore, where the law meets certain minimum requirements, additional optimization can and should be considered.[102] In our view, these bottlenecks should be included in the announced assessment of the law and result in improvements to the law.

In paragraphs 5.2 - 5.7, we address concerns related to oversight and access to justice. The final two paragraphs, 5.8 - 5.9, discuss bottlenecks in relation to the general and special powers.

5.2 Struggles with the concept of independent oversight

Although the accountability mechanisms have been strengthened, there appears to be some shortcomings. As concluded by the Dessens Committee, extended (special) powers should go hand-in-hand with increased checks and balances. More precisely, although the previous powers were insufficient for the security and intelligence services to fulfil their assigned tasks, the new and strengthened powers require a new balance to be sought versus the statutorily defined safeguards and transparency mechanisms. Some stakeholders have argued that the legislator has not always provided such concession.

As part of the issue of lawfulness versus appropriateness, the Dutch have also struggled with the concept of independent oversight. The Strasbourg jurisprudence is quite clear about independent oversight. Meaningful oversight needs to be in place both *ex ante* and *ex post*. While preferably exercised by courts, other comparable institutions may also be assigned these tasks. Under the previous national security act, courts needed to give permission for opening letters because of the requirement to do so in the Dutch Constitution (article 13). However, all other types of surveillance could be authorized by the executive, only being subjected to *ex post* oversight. This oversight could be considered to be independent, but not to be sufficiently meaningful as it lacked the authority to intervene.
Pushed by the ECtHR's jurisprudence and by decisions of national courts, the

101 *Parliamentary Papers* II, 2016/2017, 34588, 3, pg. 224-225 and 303-304.
102 Eskens *et al.* (2016); Loof *et al*. (2015).

new act now has a complicated system of *ex ante* and *ex post* oversight. Prior court approval is required in three cases: a) opening letters (because of the constitutional requirement), b) when a lawyer is involved and c) to discover the source of a journalist. The *ex ante* authorization of a new review board, the TIB, is obligatory for many other measures. This includes a) access to types of communications other than letters b) communication by journalists not related to discovering a source. If within the context of an authorisation granted by the TIB, the communication with a lawyer is identified, this information cannot be processed unless the court gives permission. As it is very likely that the communication by a journalist will include information about a source, it can be assumed that in practice all surveillance measures directed towards journalists are made subject to authorizations granted by the court.

It is clear that such a division of tasks is highly complicated, impractical and confusing. The overall oversight system has thus become increasingly complex and therefore difficult to understand for the general public unfamiliar with the ISS Act 2017.

Two final notes on this issue: a) as far as the separate Court and TIB procedures is motivated by the argument that the court procedure offers a higher level of protection, the question can be raised why other parties in a similar critical position based on professional confidentiality or role in a democratic society (religious professionals, member of parliament, judges) have not been offered the same level of protection (as is to some extent the case in some other countries);[103] b) more attention should be given to the question whether the TIB sufficiently meets the necessary requirements in order to be considered a Strasbourg-proof alternative for oversight by a court.

Another issue is the new complaints role of the complaints department of the CTIVD in addition to its oversight responsibilities.[104] This was extensively discussed in Parliament and although an arrangement has been made to have separate persons involved in the oversight and the complaints department, citizens may still perceive the CTIVD as a single body. Considering the context of secrecy in which the relevant services perform their tasks, this may sometimes create the impression that the CTIVD is marking its own papers.[105] Previously, the risk of partiality did not exist because complaints were handled by the ombudsman. But with the introduction of the ISS Act 2017, his role ceases to exist.

This is partly compensated by the fact that the complaints procedure now

103 Van Eijk (2017).
104 Eijkman (2018).
105 Ombudsman (2015), pg. 2 and 3.

includes the possibility to impose remedies. However, the practical application of both roles will have to demonstrate whether the concerns can be addressed. One of the upsides might be that the complaints department has full access to all information.

5.3 No binding oversight for special powers

In contrast to the recommendations of influential stakeholders including the Ombudsman, the lawmaker refused to grant binding oversight for the use of special powers during, *ex nunc*, and after, *ex post*, the execution of these powers (with the exception of the complaints procedure, see section 4.7).[106] The existence of remedies would have been desirable when considering the enlarged codified powers, yet the concern expressed by stakeholders has been largely ignored. Amendments to improve the law were rejected. This does leave intact the fact that the CTIVD has broad investigatory and reporting powers. Its recommendations are in general respected and implemented.

Interestingly, the complaints procedure allows the complaints department of the CTIVD to order a) the termination of an investigation, b) the termination of the exercise of a power and c) the destruction or removal of processed data by the intelligence services. In theory, this offers interesting opportunities. As a 'consequential effect', the reports of the CTIVD might become the basis for complaints to its complaints department, thus indirectly offering remedies for the non-binding conclusions or recommendations in the report.

5.4 International exchange of data

In light of the Snowden revelations, it should be questioned whether ministerial approval and *ex post* oversight alone are adequate and effective guarantees in the context of the international exchange of data. For example, interception of bulk data is subject to prior authorization by the TIB, but the transfer of these data to other countries may not have been foreseen at the time of authorization. Separate *ex ante* oversight, such as independent and impartial full review before data is transferred abroad, is desirable and is in keeping with the system of checks and balances as envisaged when the law was put together.

106 Dessens Committee (2013), pg. 12; Ombudsman (2015); Loof *et al.* (2015), pg. 7; CTIVD (2016); Koops *et al.* (2016), pg. 40.

5.5 Review Committee for the Intelligence and Security Services vs. the Review Board for the Use of Powers

A specific point of concern is the relationship between the CTIVD and the TIB. The explanatory memorandum indicates that the CTIVD must recognize the lawfulness of TIB's decisions regarding authorizations. Simultaneously however, the CTIVD must maintain its oversight concerning the services. Tension might be especially prevalent between the TIB's *ex ante* decisions, which must occur with short notice and without the consultation of external experts, and *ex nunc/ex* post investigation by the CTIVD, which will evidentially be under less time constraints (in particular the *ex post* investigations). If the CTIVD finds retrospectively that the information used by TIB was incorrect or insufficient, the CTIVD might need to draw conclusions questioning the legitimacy of the TIB decision. The same might apply to the *ex ante* decisions by the district court of The Hague.

5.6 Legal uncertainty

A lack of legal uniformity may cause legal uncertainty: the legal norms which have been codified will need to be regularly interpreted by multiple bodies, which will each form their own interpretation. Bodies such as the CTIVD and the TIB are under no obligation to maintain legal uniformity, although parliament has stressed the need for it. Likewise, the division of special powers authorization between the TIB and The Hague District Court will cause diverging interpretations. These questions of legal uniformity will be especially prevalent when setting standards of subsidiarity or proportionality. A few examples: the (in)direct tapping or surveillance of a lawyer or journalist can result in two procedures. Will the court and the committee sync their activities and use the same criteria? Another ambiguity concerns the decisions taken by the TIB and the complaints department of the CTIVD. We assume that their decisions can be challenged in civil or administrative court.

5.7 Effectiveness of complaints and whistle-blower remedies

Despite the improved thoroughness of the complaints procedure and new whistleblower arrangement, one cannot help wondering how effective filling a complaint will be? Although the fact that a binding remedy has been provided is a huge step forward, from an access to justice perspective, the question remains how far the CTIVD complaints department is willing to go in practice. For example, we assume the subject of third party hacking can file a complaint. Additionally, the lawmaker appears to have taken ECtHR jurisprudence seriously in relation to proper safeguards for secret surveillance. Yet, the checks and

balances for group complaints are less evident.[107] For instance, what about remedying the bulk communications interception by the intelligence and security services. What to do about the fact that lawyers and journalists are excluded from the complaints procedure if the court has decided on the legality of a special power? These issues largely reflect the existence of unexplored territory and could result in opportunities to establish a new view on the use of the complaints procedure.

The whistle-blower procedure is new and its effectiveness will be proven in practice. Yet the broader context of whistle-blowing in the Netherlands shows that complexity (procedures, maintaining confidentiality) can easily frustrate adequate and effective protection of whistle-blowers. The Dutch House for Whistle-blowers was opened in 2016, seeking to both conduct investigations on alleged misconduct, as well as provide advice for individuals attempting to blow the whistle. The House has received many notifications of alleged misconduct, but it has until today failed to complete a single investigation, due to various issues. In the case of the ISS Act 2017, an employee of an involved telecom company risks losing all the provided protection if he or she fails to meet the criteria set in the act. In such a worst-case scenario, procedures will be more of a burden than a safeguard.

5.8 Open source information as intelligence?

One important question is the changing nature of open source information and open source intelligence. The security and intelligence services have always gathered information from open sources, such as newspapers, the social network sites or blogs. The ability to collect large amounts of such data, or to combine such large datasets in innovative ways, for example with algorithm-driven computer software, has significantly increased the capabilities of communications surveillance. Data can by themselves be sensitive, but the context in which they are placed has an especially large impact. A GPS location might be uninteresting in itself, but combined with a large dataset (including for example some tweets and information submitted in an app), may have far-reaching implications.

In this regard, the introduction of open source information collection as a power - albeit a regular one - is welcome, but only a first step. Because of the increased effectiveness of open source intelligence, one might consider applying safeguards from other fields of law, such as general data protection law. One possibly relevant principle is that of purpose limitation: the requirement that processing must be for a specified, explicit and legitimate purpose; and the

107 Eijkman (2018).

requirement that any further processing must be compatible with the original purpose for which the personal data were collected. The tasks currently entrusted to the security and intelligence services are very broad, and so further limitation of open source intelligence's purpose or a better understanding of duties of care in this context could ensure a more proportionate interference with civil liberties.[108] In our view, it will not be possible to deviate from generally excepted privacy and data protection principles, as jurisprudence has shown that these also apply in the context of intelligence and security services. As the services are bound to a duty of care (see subsection 3.2.3), respecting these principles is all part of the game. The CTIVD addresses several of these topics in its report on the acquisition of bulk data sets offered by third parties on the internet.[109]

5.9 Distinction between regular and special powers

The ISS Act 2017 is still built on a traditional separation of regular and special powers. Regular, general powers have less safeguards than special powers. The collection and processing of publicly available data or data gathered via informants (both general powers without prior oversight) can have similar effects on fundamental rights as the exercise of special powers. Or, as another example, informants may be asked to provide data from computerized systems, which they are able to access. This saves the services from employing other powers such as open source intelligence ("OSINT"), but the way informants operate can equally impact the citizens involved, and the data obtained is the same. The use of multiple such means to achieve the same goal is especially relevant in light of technological developments, because the scale and type of data provided would previously not have been gathered by informants without access to computerized systems. In combination with the technology-neutral approach of the law (see section 2.5), this can result in new challenges to meet the standards as set out in the underlying normative framework and as interpreted through jurisprudence. For instance, are all open data truly open data, even if this relates to large databases stolen via hacks or as the result of data leaks and to what extent are informants responsible for privacy or data protection? Despite the fact that the issue of intrusion of regular powers was addressed during the debate about the bill in the Dutch Senate, and that responsible ministers gave additional guarantees about the exceptions of systematically collecting data or certain other informant activity that required

108 Eijkman & Weggemans (2012).
109 CTIVD (2017) (2).

the equivalent level of safeguard, it is unclear what this will mean in practice.[110] Although the new government recognized that guarantees given during the parliamentary debate about the ISS Act 2017 would be respected, it remains the question whether or not this is a short-term or a long-term guarantee.

In the latter case, it should ultimately become part of the act. This is an issue that should at least be addressed as part of the assessment of the law.

110 Senate, Regels met Betrekking tot de Inlichtingen- en Veiligheidsdiensten alsmede Wijziging van Enkele Wetten, Wet op de Inlichtingen- en veiligheidsdiensten, Toezegging Reikwijdte artikel 39 [Rules in Relation to the Intelligence & Security Services and Amending Several Acts, Intelligence and Security Services Act 2017, Promise about the scope of article 39], T02468, 11 July 2017, *Parliamentary Papers* I, T02468, 35, pg. 6; letter to parliament (*Parliamentary Papers* II, 2017/18, 34588, 69).

References

This list of references includes both literature cited in the report and (indicative) material that was used as background information.

CTIVD (2014). *TOEZICHTSRAPPORT inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD.*
Available at https://www.ctivd.nl/documenten

CTIVD (2015). *Reactie CTIVD op het concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX (consultatieversie juni 2015).*
Available at https://www.ctivd.nl/documenten/publicaties/2015/08/26/reactie-ctivd-conceptwetsvoorstel

CTIVD (2016) (1). *Zienswijze van de CTIVD op het wetsvoorstel WIV 20…*
Available at https://www.ctivd.nl/binaries/ctivd/documenten/publicaties/2016/11/09/zienswijze/Zienswijze+van+de+CTIVD_november+2016.pdf

CTIVD (2016) (2). *Annual Report 2016.* Available at https://english.ctivd.nl/documents/annual-reports/2017/07/24/index

CTIVD (2016) (3). *Review Report on the implementation of cooperation criteria by the AIVD and the MIVD; investigation into the execution of Dutch House of Representatives motion no. 89 (by members Schouw and Segers) No. 48.*
Available at: https://english.ctivd.nl/binaries/ctivd-eng/documents/review-reports/2016/12/22/index48/CTIVD_Rapport_Tweede+Kamermotie+89_NR48_ENG_LR.pdf

CTIVD (2017) (1). *Letter to the Senate about the Draft-Bill Intelligence and Security Services Bill Wiv 20XX.* Available at https://www.ctivd.nl/binaries/ctivd/documenten/brieven/2017/03/28/brief-ek-wiv-20/Brief+CTIVD+aan+EK+Commissie+Biza+t.b.v.+informeel+gesprek_22+maart+2017.pdf

CTIVD (2017) (2). *Toezichtsrapport: Over het verwerven van door derden op internet aangeboden bulkdatasets door de AIVD en de MIVD, No.55.*
Available at https://www.ctivd.nl/documenten/rapporten/2018/02/13/index

CTIVD (2017) (3). *Toezichtsrapport: Over de inzet van de hackbevoegheid door de AIVD en de MIVD, No.53.* Available at https://www.ctivd.nl/actueel/nieuws/2017/04/25/index

Dessens Committee (2013). *Evaluatie Wet op de Inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen.* Available at https://www.rijksoverheid.nl/documenten/rapporten/2013/12/02/rapport-evaluatie-wiv-2002

Eijkman, Q.A.M. (2018). 'Access to Justice for Communications Surveillance and Interception: Scrutinising Intelligence Gathering Reform Legislation'. Utrecht Law Review, vol 14, 2018/1, pp. 116-127.

Eijkman, Q.A.M. & Weggemans, D. (2012). 'Open source intelligence and privacy dilemmas: Is it time to reassess state accountability?', *Security and Human Rights,* 4., pp. 285-296.

Eskens, S., van Daalen, O. & van Eijk, N.A.N.M. (2016). '10 standards for oversight and transparency for surveillance by intelligence services', Journal of National Security Law & Policy, 8, 3, pp. 553-594.

Fundamental Rights Agency (2017). *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU, Volume II: Field Perspectives and Legal Update.* Available at http://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega

Jacobs, B. (2016). 'Select while you collect. Over de voorgestelde interceptiebevoegdheden voor inlichtingen- en veiligheidsdiensten', NJB, 4, pp. 256-261.

Konijnenbelt, W. & van Male, R.M. (2014). *Hoofdstukken van Bestuursrecht.* Alphen aan den Rijn: Wolters Kluwer.

Koops, B-J, Roosendaal, A., Kosta, E., van Lieshout, M. & Oldhoff, E. (2016), *Privacy Impact Assessment Wet op de inlichtingen- en veiligheidsdiensten 20XX: Privacy impact assessment.* Available at: https://zoek.officielebekendmakingen.nl/blg-742355

Loof, J.P., Uzman, J., Barkhuysen, T., Buyse, A., Gerards, J.H. & Lawson. R. (2015). *Het Mensenrechtenkader voor het Nederlandse Stelsel van Toezicht op de Inlichtingen- en Veiligheidsdiensten,* Leiden University. Available at https://dspace.library.uu.nl/handle/1874/323665.

Ombudsman (2015). Letter to the Minister of the Interior and Kingdom Relations Draft-Bill WIV, the Hague: Ombudsman's Office. Avialable at: https://www.nationaleombudsman.nl/nieuws/2015/klachtbehandeling-aivd-en-mivd-moet-wel-onafhankelijk-blijven

Taylor, L., van der Sloot, B. & Floridi, L. eds. (2017). Group Privacy: Challenges of Data Technologies. Dordrecht: Springer.

Van Eijk, N.A.N.M. (2017), 'Standards for Independent Oversight: The European Perspective', *Bulk Collection: Systematic Government Access to Private-Sector Data*, ed. F.H. Cate & J.X. Dempsey, Oxford University Press, pp. 381-393.

ECtHR Jurisprudence

ECtHR 4 May 2000, Application no. 28341/95 (Rotaru v. Romania) .
ECtHR 4 December 2008, Applications nos. 30562/04 and 30566/04 (S. and Marper v. the United Kingdom).

ECtHR 18 May 2010, Application no. 26839/05 (Kennedy v. the United Kingdom).

ECtHR 14 September 2010, Application no. 38224/03 (Sanoma Uitgevers B.V. v The Netherlands) ECLI:NL:XX:2010:BO7625.

ECtHR 22 November 2012, Application no. 39315/06 (Telegraaf and Others v. the Netherlands) ECLI:NL:XX:2012:BY6026.

ECtHR 4 December 2015, Application no. 47143/06 (Zakharov v. Russia) ECLI:CE:ECHR:2015:1204JUD004714306.

Dutch Jurisprudence

Council of State (Raad van State), 20 December 2017, ECLI:NL:RVS:2017:3508.

District Court of The Hague (Rechtbank Den Haag), 1 July 2015, ECLI:NL:RBDHA:2015:7436.

Newspaper articles

Lichtblau, E. & Benner, K. (17 February 2016). Apple Fights Order to Unlock San Bernardino Gunman's iPhone. *The New York Times*. Available at https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html.

Mears, B. & Abdullah, H. (17 January 2014). What is the FISA court? *CNN*. Available at http://edition.cnn.com/2014/01/17/politics/surveillance-court/index.html.

List of terms/abbreviations

AIVD: General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst)

CTIVD: Review Committee for the Intelligence and Security Services (Commissie van Toezicht op de Inlichtingen en Veiligheidsdiensten)

CTIVD complaints department: Complaints Department of the Review Committee for the Intelligence and Security Services (Commissie van Toezicht op de Inlichtingen en Veiligheidsdiensten, Afdeling Klachtenbehandeling')

CIVD: Parliamentary Committee on Intelligence and Security Services (Commissie voor de Inlichtingen- en Veiligheidsdiensten). Publicly known as 'the Commission Secretly' ('Commissie stiekem')

'Eerste Kamer': Senate (Dutch Parliament)

ISS Act 2002: Intelligence and Security Services Act 2017 (Wet op de Inlichtingen- en veiligheidsdiensten 2017, Wiv. Predecessor of the ISS Act 2017)

ISS Act 2017: Intelligence and Security Services Act 2017 (Wet op de Inlichtingen- en veiligheidsdiensten 2017, Wiv 2017)

MIVD: Military Intelligence and Security Service (Militaire Inlichtingen- en Veiligheidsdienst)

TIB: Review Board for the Use of powers (Toetsingscommissie Inzet Bevoegdheden)

House of Representatives: (Dutch Parliament) (Tweede Kamer)

Senate: Senate (Dutch Parliament) (Eerste Kamer)

WOB: Dutch Freedom of Information Act (Wet openbaarheid van Bestuur)

About the Authors

Quirine Eijkman

Quirine Eijkman Phd. is the Chair of the Research Group Access2Justice at the Centre for Social Innovation (KSI) of the HU University of Applied Sciences Utrecht and the Deputy President of the Netherlands Institute for Human Rights. This publication was writtten in her personal capacity.

For more information, see: https://www.research.hu.nl/Onderzoekers/Quirine-Eijkman?_ga=2.708 66963.283121025.1519249268-855081637.1495967599.

Nico van Eijk

Nico van Eijk is Professor of Media and Telecommunications Law and Director of the Institute for Information Law (IViR, Faculty of Law, University of Amsterdam). Among other things, he is the Chairman of the Dutch Federation for Media and Communications Law (Vereniging voor Media- en Communicatierecht, VMC), member of the 'knowledge network' of the Dutch Review Committee on the Intelligence and Security Services (CTIVD) and member of the Royal Holland Society of Sciences and Humanities (KHMW).

For more information, see: https://www.ivir.nl/employee/eijk/ and http://www.uva.nl/profiel/e/i/ n.a.n.m.vaneijk/ n.a.n.m.van-eijk.html

Robert van Schaik

Robert van Schaik is a Project Researcher at the Institute for Information Law, University of Amsterdam.

For contact details, see: https://www.ivir.nl/employee/robert-vanschaik/

IViR (Institute for Information Law, University of Amsterdam)
www.ivir.nl