The Wiv 2017

A critical contemplation of the Act in an international context.

Lotte Houwing, s1850164

Supervisors: Oskar J. Gstrein (RUG) and Nico A. N. M. van Eijk (UvA).

Table of contents:

List of abbreviations:

BND Act	*Gesetz über den Bundesnachrichtendienst* - Federal Intelligence Service Act.
BPD	Bulk Personal Data.
CTG	Counter Terrorism Group.
CTIVD	*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten* - Review Committee on the Intelligence and Security Services.
DPA	Data Protection Authority.
ECHR	European Convention of Human Rights.
ECtHR	European Court of Human Rights.
G10 Act	*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses* - Act on Restrictions on the Secrecy of Mail, Post and Telecommunications.
GA	*Geïntegreerde Aanwijzing Inlichtingen- en Veiligheidsdiensten* – Integrated Intelligence and Security Services Order.
IPA 2016	Investigatory Powers Act 2016.
IPC	Investigatory Powers Commissioner's Office.
JSCU	Joint Sigint Cyber Unit.
PILP	Public Interest Litigation Project.
SRP	Special Rapporteur on the right to Privacy of the United Nations.
TIB	*Toetsingscommissie Inzet Bevoegdheden* - Review Board on the Use of Powers.
UG	*Unabhängiges Gremium* Independent Committee.
Wiv 2017	*Wet op de Inlichtingen- en Veiligheidsdiensten 2017* – Intelligence and Security Services Act 2017.

1. Introduction.

The surveillance industry has been rapidly growing and developing. This has been caused in part by technological developments. Technologies to gather, process and analyze large amounts of data are constantly improved upon, new communication technologies are used, and storage of large amounts of data has never been so cheap. On the political end, there is a lot of change as well. The attack on the 11th of September 2001 in the United States was the start of the 'War on Terror', and ever since, policies have been revised to fight terrorism and radicalisation in the United States and Europe.[1] Digital surveillance methods are increasingly used for this purpose.[2] These perceived new threats, and the development of new technologies to react, have triggered law reforms in the field of intelligence- and security services in many countries. Especially France, Germany, The Netherlands, The United Kingdom and Finland have been reforming their respective surveillance legislations extensively.[3]

Furthermore, the Snowden revelations of 2013 made clear that the United States, together with several European countries, participated in "mass-surveillance", leading to widespread criticism in terms of interferences with fundamental rights, concerning privacy in particular.[4] It is new and probably unique to have an ongoing debate on the secrecy of the work of the services in question. Considering these developments together results in the question how far states can go in their measures to protect citizens and national security. As the European Court of Human Rights (hereafter: ECtHR) in Strasbourg stated: "It would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives."[5]

The above question will form the decor of this research. More specifically, this research focuses on the relevant legal reform in the Netherlands, as manifested by the introduction of the Intelligence and Security Services Act 2017 ('*Wet op de Inlichtingen- en Veiligheidsdiensten 2017',* hereafter: Wiv 2017). The research will form a critical contemplation of this Act and its introduction process. Research question will be:

> "*How does the Dutch Intelligence and Security Services Act 2017 relate to European and international developments within the field of government surveillance?*"

To answer this question the Wiv 2017 will be placed in an European and international legal framework and compared to reforms brought about by intelligence Acts in Germany and the UK. Since these are all ongoing processes and the scope of this research is limited, I will only take developments into account until the entry into force of the Wiv 2017 on the 1st of May 2018. Unfortunately, this means that relevant developments past this date will fall

1 A. Kundnani and B. Hayes, *The globalisation of CVE policy: Undermining human rights, instrumentalising civil society.* Amsterdam: Transnational Institute, 6 March 2018, p. 6.

2 FRA, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Updates*, Luxembourg: Publications Office of the European Union 2017, p. 17.

3 FRA, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Updates*, Luxembourg: Publications Office of the European Union 2017, p. 9.

4 https://www.theguardian.com/us-news/the-nsa-files accessed 17 March 2018; HRC Report of the Special Rapporteur on the right to Privacy Joseph A. Cannataci, *Un Doc*. A/HRC/34/60, p. 6.

5 ECtHR 12 January 2016 App No 37138/14 (*Szabó and Vissy v Hungary)*, para. 68.

outside of this scope and will not be taken into account.

The Wiv 2017 and the Dutch debate surrounding it are exemplary of this development and can function as a model. First, because the arguments given for the need of this new law are the aforementioned perceived threats of terrorist attacks and the need for modernisation to keep up with the technological developments of society, specifically those in communications technology. Secondly, because the law reform unchained a discussion in Dutch society on the aforementioned question: To what extent are we willing to allow intelligence services to infringe on our fundamental rights in order to protect national security? Thirdly, because in the Netherlands an open debate is enabled by a sufficient level of free speech and transparency of the functioning of the Dutch services and government. Fourthly, it is possible to have a well-informed debate on the content of the law, since there is not one obvious flaw in the system which is blocking a broader discussion. And fifthly, because of a referendum started by five students from Amsterdam, the debate has been held throughout society. This has given the topic momentum, causing more transparency, debate, and information, and giving citizens a voice in the national security policies of their country.

Besides the fact that the Netherlands is not the only country implementing a law reform regulating the powers of the intelligence and security services, it is also not the only country where this law reform has been criticised. In the UK the Investigatory Powers Act 2016 was nicknamed “The Snooper’s Charter”, and the human rights group Liberty started a lawsuit against the untargeted surveillance powers of the Act.[6] The UK government is currently carrying out a review on their Act in which careful consideration is being given to the *Tele2 Sverige/Watson* judgment of the CJEU. The government found some aspects of the regime which do not meet the requirements of the CJEU judgment and therefore proposes to amend the IPA 2016.[7] Most recently, the appeal court judges ruled parts of this Act’s surveillance regime unlawful.[8] In Germany, Reporters Without Borders won a case on metadata collection and telephony data, and the Constitutional Court will rule on the legality of the entire BND law on a number of grounds.[9] In the Netherlands, a broad coalition coordinated by the Public Interest Litigation Project (hereafter: PILP) has announced to start a court case as soon as the Wiv 2017 enters into force.[10] This shows the developments in the Netherlands are part of, and therefore relevant for, a larger international debate. In this research I will elaborate on the capabilities of the Dutch Act as well as the criticisms voiced in the debate. To place this in an international context I will make comparative remarks with the law reforms in Germany and the UK.

The initiative to start a referendum and court cases against the (introduction of the) new Act, the campaign, and the lively debate on the topic show there is a lot of criticism towards the expansion of powers of the services. The core of the criticism is directed at the untargeted effects of surveillance powers, and the perceived lack of safeguards to protect civilians against unlawful infringements of their rights. This research addresses the

6 https://www.liberty-human-rights.org.uk/news/press-releases-and-statements/people-vs-snoopers%E2%80%99-charter-liberty-launches-crowdfunded-legal, accessed 22 January 2018.

7 Home Office, *Investigatory Powers Act 2016: Consultation on the Government’s proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data.* November 2017, p. 2 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/663668/November_2017_IPA_Consultation_-_consultation_document.pdf>.

8 https://www.theguardian.com/uk-news/2018/jan/30/uk-mass-digital-surveillance-regime-ruled-unlawful-appeal-ruling-snoopers-charter, accessed 31 January 2018.

9 https://rsf.org/en/news/germany-landmark-ruling-against-bnd, accessed 19 March 2018.

10 https://pilpnjcm.nl/dossiers/wet-op-de-inlichtingen-en-veiligheidsdiensten-wiv/, accessed 19 March 2018.

capabilities that are the most prominent within the debate; those which incorporate untargeted effects. This list includes but is not limited to: bulk interception, the capability to hack through third parties, real-time access to databases, and the exchange of data with foreign services. Apart from the surveillance powers, the oversight and control mechanisms contained in the Act will be addressed.

European law, including case-law, is providing the parameters within which national law reforms can be formulated. The debates on the law reforms are being held against this background and eventually it will be the (European) courts who have the final verdict on the legality of the reforms. For this reason I will start with a sketch of this framework so far, before continuing with an elaboration on the capabilities of the Act. I will take matters at the level of the United Nations in regard as well, as far as these influence developments in Europe.

2. Methodology.

The intent of this research is to give a critical contemplation of the Dutch Intelligence- and Security Services Act 2017 in an international context. This will be done by an elaboration of the most recurring aspects of the Act. These are bulk interception, the hacking capability, real-time access to databases, the provision of data to foreign services, as well as authorisation, oversight, and control mechanisms. In a comparison with the law reforms on intelligence services of Germany and the UK, these capabilities will be placed in an European and international legal framework. The conclusions of these elaborations together will form the conclusion of the research, wherein they will form an answer to the research question: “How does the Dutch Intelligence and Security Services Act 2017 relate to international developments within the field of government surveillance?” The nature of this research is partly a legal analysis of the national law and debate, and partly a comparative research.

Surveillance is a broad term, often used to cover many things. For the purpose of this research, the best definition of the term comes from David Lyon: ”The monitoring of behavior, activities, or other changing information for the purpose of influencing, managing, directing, or protecting people.”[11] Furthermore, within the scope of this research the meaning will be limited to surveillance for government purposes.

Because of the limited scope of the research it is not possible to include many countries in the comparison. In an attempt to create continuity, the comparison is limited to the United Kingdom and Germany. Several aspects led to this selection: Both countries have seen recent law reforms that are quite detailed. In both countries a debate is ongoing concerning the desirability and constitutionality of the expanded surveillance powers. Within the Anglo-Saxon orientation the Netherlands belongs to, the UK plays a leading role regarding far-reaching surveillance capabilities, and is known for it. Furthermore, the UK heavily influences one of the main legal systems in the world: the common law system. Finally, there is also quite a lot of relevant case-law within this field coming from cases in the UK. Germany however, has a leading role within the European Union, and it is interesting to consider German developments because the perception and cultural tradition of privacy is different. Germany heavily influences the other main legal system of the world; the civil law system. Hence, this selection will enable the inclusion of as many factors as possible within this limited scope.

The subject of this research is very much actual. Developments regarding the legal framework, as well as the law reforms and debate are not finished. It is tempting to keep updating this research, and include all new interesting developments. Unfortunately, this research can only be of limited scope, and I have limited time. Therefore, this study is demarcated to include the relevant developments until the moment the Dutch Act enters into force on the 1st of May 2018. This means that some relevant developments such as the finishing of the modernisation process of Convention 108, the accession of Mexico to this Convention and the judgment of the ECtHR in the case of *Centrum för Rättvisa v Sweden* will not be taken into account.

Since the debate mostly focuses on the infringements of the surveillance measures on civil liberties, the focus within this research will be on civil intelligence services and exclude surveillance for military purposes. Also, the different countries all have different traditions and systems regarding (the embedding of) their intelligence and security services. Unfortunately, due to the limited scope of this research I will not be able to provide such

11 D. Lyon, *Surveillance Studies: An Overview,* Cambridge: Polity Press 2007.

context and will focus purely on the most notable capabilities regulated in the law reforms. I will start with substantively describing the Dutch capabilities according to the new Act, and subsequently provide a critical reflection. When appropriate, I will make comparative remarks to the Acts of the United Kingdom and Germany, and to the European legal framework, mostly distilled from relevant case-law.

In an attempt to be consistent with English terminology, and due to the lack of an official and complete translation, I will use the translation that has been composed in the context of the EU notification.[12]

12 http://ec.europa.eu/growth/tools-databases/tris/en/search/trisaction=search.detail&year=2016&num=188, accessed 19 March 2018.

3. European and international framework

The many developments and discussions in the field of surveillance have found their way into the judicial institutions as well. The United Nations called upon all states "to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law".[13] Regional Human Rights Courts such as the European Court of Human Rights (hereafter: ECtHR) already had pretty detailed case-law on related subjects like privacy and data protection, but more recently have started handing down judgments that will establish a clear and binding framework of requirements regarding governmental surveillance.[14] And many more cases on the use of untargeted state surveillance will be adjudicated.[15] Moreover, the Court of Justice of the European Union (hereafter: CJEU) has been pulling the subject towards its jurisdiction since it struck down the Data Retention Directive which obligated communication service providers to undertake mass retention of their customer's metadata in 2014.[16] In 2016, the Court delivered the *Tele2 Sverige/Watson* judgment which was interpreted as reminding European Union Member States of their obligations regarding the human right to privacy and the equal applicability thereof in the digital age.[17]

When it comes to surveillance, it is not only the right to privacy that is at stake. The rights to correspondence, freedom of expression, freedom of assembly and association, protection of journalistic sources and data protection, among others, are (potentially) infringed upon as well.[18] In general, article 52 of the Charter of Fundamental Rights of the European Union (hereafter: CFREU) states that fundamental rights that are recognised in the Charter can be limited in so far as the limitation is prescribed by law and respects the substantial content of the rights. These limitations are subject to the principle of proportionality, need to be necessary, and are required to genuinely meet objectives of general interest recognised by the European Union. The article also refers to the European Convention on Human Rights (hereafter: ECHR) in case the rights guaranteed in the Charter correspond with rights guaranteed in the Convention. Limitations to the rights guaranteed under the ECHR can be justified if they are in accordance with the law, in pursuit of one or more of the legitimate aims, and are necessary in a democratic society in order to achieve the aim.[19]

For a measure to be 'in accordance with the law' it needs to have a basis in domestic law and to be compatible with the rule of law, which means that this domestic law must meet some specific quality requirements: It must be accessible to the person(s) concerned and foreseeable as to its effects.[20] Since the *Sanoma* judgment, domestic law needs to afford a measure of legal protection against arbitrary interferences by public authorities, with the

13 United Nations General Assembly Resolution, *The right to privacy in the digital age*, 18 December 2014, UN Doc. A/RES/69/166, p. 3.

14 ECtHR 4 December 2015 App No 47143/06 (*Roman Zakharov v Russia*).

15 ECtHR App No 25252/08 (*Centrum För Rättvisa v Sweden)*; ECtHR App No 3599/10 (*Tretter and Others v Austria*); ECtHR *App* No 58170/13 (*Big Brother Watch and Others v UK)*; ECtHR App No 62322/14 (*Bureau of Investigative Journalism and Alice Ross v UK)*; ECtHR App No 24960/15 (*10 Human Rights Organizations and Others v UK)*, ECtHR App No 49526/15 (*Association Confraternelle de la Presse Judiciaire v France).*

16 CJEU 8 April 2014 Joined Cases C-293/12 and C-594/12 (*Digital Rights Ireland and Seitlinger).*

17 HRC Report of the Special Rapporteur on the right to Privacy Joseph A. Cannataci, *UN Doc*. A/HRC/34/60, p. 7, referring to: CJEU 21 December 2016 Joined Cases C-203/15 and C-698/15 (*Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others).*

18 Artt. 8 and 10 ECHR, artt 7, 8 and 11 CFREU.

19 ECtHR 18 May 2010 App No 26839/05 (*Kennedy v UK*), para. 130.

rights safeguarded in the Convention as well.[21] National security is accepted by the Court as a legitimate aim, and is described in the second paragraph of article 8 ECHR as such. The Court tends to accept without question that a state is pursuing to protect national security and/or to prevent crime with the implementation of secret surveillance measures.[22] To meet the requirement of 'necessary in a democratic society' there must be a 'pressing social need' that is proportional to the achieved aim. Grounds argued for the necessity of the measures should be relevant and sufficient.

According to case-law of the ECtHR, the mere existence of a law permitting surveillance can constitute an interference with article 8 if the scope of the legislation is such that the individual can be affected by it.[23] Whether the mere existence of a law permitting surveillance is sufficient to constitute an interference depends on the availability of effective remedies.[24] In practice, ECtHR and CJEU take the stance that as soon as intelligence services intercept signals and collect data there is an interference with the right to a private life, articulated in article 8 of the ECHR.[25] Furthermore, an interference does not only take place when data is collected, but every time the data is accessed by a government authority for further processing.[26]

In its seminal judgment in the case *Roman Zakharov v Russia* the ECtHR elaborates on and summarises the current state of ECHR case-law, specifically regarding measures of secret surveillance. The Strasbourg based Court acknowledges that, given the secrecy of the measure, the foreseeability requirement needs to be adjusted. The level of clarity must be sufficient "to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measure". Since the application of measures of secret surveillance is not open to scrutiny by the individual or the public and it would be contrary to the rule of law to grant unfettered powers to the executive, "the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference".[27] In order to avoid abuses of power in this respect, the Court has developed the following minimum safeguards that should be clear in the law: The nature of offenses which may give rise to an interception order; a definition of the categories of people liable to have their communications tapped; a limit on the duration of the interception; the procedure to be

20 ECtHR 4 May 2010 App No 28341/95 (*Rotaru v Romania)*, para. 52; ECtHR 4 December 2008 App No 30562/04 and 30566/04 (*S and Marper v UK)*, para. 95.

21 ECtHR 14 September 2010 App No 38224/03 (*Sanoma v The Netherlands)*, para. 82.

22 S. J. Eskens, 'Ongerichte interceptie, of het verwerven van bulk-communicatie, en waarom de Grondwet en het EVRM onvoldoende tegenwicht bieden', in: *Computerrecht* 2015, nr. 3, p. 129.

23 ECtHR 6 September 1978 App No 5029/71 (*Klass and Others v Germany*), para. 34-36 and 41; ECtHR 18 May 2010 App No 26839/05 (*Kennedy v UK*), para. 119 and 124.

24 ECtHR 6 September 1978 App No 5029/71 (*Klass and Others v UK*), para. 41, 50 and 55; ECtHR 2 August 1984 App No 8691/79 (*Malone v UK*), para. 64; ECtHR 18 May 2010 App No 26839/05 (*Kennedy v UK*), para. 153.

25 ECtHR 4 December 2015 App No 47143/06 (*Roman Zakharov v Russia*), para. 229-231; ECtHR 18 May 2010 App No 26839/05 (*Kennedy v UK)*, para. 118-129; FRA, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Updates*, Luxembourg: Publications Office of the European Union 2017, p. 33-34; CJEU 8 April 2014 Joined cases C-293/12 and C-594/12 (*Digital Rights Ireland and Seitlinger);* CJEU 21 December 2016 Joined Cases C-203/15 and C-698/15 *(Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others)*, para. 100.

26 CJEU 6 October 2015 C-362/14 (*Maximillian Schrems v Data Protection Commissioner)*, para. 95; ECtHR 2 September 2010 App No 35623/05 *(Uzun v Germany)*, para. 63.

27 ECtHR 4 December 2015 App No 47143/06 (*Roman Zakharov v Russia)*, para. 229-234; ECtHR 29 June 2006 App No 54934/00 (*Weber and Saravia)*, para. 95.

followed for examining, using and storing the gathered data; the precautions to be taken when communicating the data to other parties, and the circumstances in which intercepted data may or must be destroyed.[28] These requirements are developed within the context of targeted surveillance, but in *Weber and Saravia* the Court rules their implicit applicability to untargeted surveillance measures. In *Liberty and Others v UK* this ruling is reiterated.[29]

With regard to the requirement 'necessary in a democratic society' in pursuit of a legitimate aim, the Court determined that national authorities enjoy a certain "margin of appreciation" in the balancing between the interest of the State in protecting its national security against the interference with the applicants' right to privacy. This means that the State has some space to manoeuvre when it comes to the manner in which it chooses to fulfill its obligations under the ECHR. However, this goes hand in hand with European supervision over the national legislation and decisions concerning the application thereof.[30] The Court acknowledges the risk that a system of secret surveillance, set up to protect national security, may undermine or even destroy democracy under the cloak of defending it.[31] To prevent this from happening, adequate and effective guarantees against abuse need to be in place. To determine whether the safeguards are strong enough to keep the interference at a level which is necessary in a democratic society, the Court takes all circumstances of the case into account. Particularly the nature, scope, and duration of the possible measures; the grounds required for ordering them; the authorities competent to authorise, carry out and supervise them; and the kind of remedy provided by the national law.[32] From this case-law of the ECtHR, the CJEU derives a need for clear and precise rules laid down in EU legislation, governing the scope and application of the measure and imposing minimum safeguards so that the persons whose data have been retained have sufficient guarantees to protect their personal data against the risk of abuse and against any unlawful access to, and use of, that data.[33] The Court states that where data is processed automatically, the need for such safeguards is even greater.[34]

Principal topic within the debate on the law reforms is the shift from targeted to untargeted effects of surveillance measures. Targeted effects are those which are directed at a specific person or group (target), of interest. Untargeted effects come along with, for example, interception in bulk, whereby large amounts of data of people that are not targets are intercepted (as well). In the case *Liberty and Others v UK* the ECtHR states that it does not consider there to be "any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications on the one hand, and more general programs of surveillance on the other."[35] In *M.M. v UK* the ECtHR states that the greater the scope of the recording system, resulting in a greater amount and sensitivity of data concerned, the more important the safeguards regarding the processing of data become.[36] In terms of

28 ECtHR 12 January 2016 App No 37138/14 (*Szabó and Vissy v Hungary)*, para. 56; ECtHR 4 December 2015 App No 47143//06 (*Roman Zakharov v Russia)*, para. 231, ECtHR 29 June 2006 App No 54934/00 (*Weber and Saravia)*, para. 93.

29 S. J. Eskens, 'Ongerichte interceptie, of het verwerven van bulk-communicatie, en waarom de Grondwet en het EVRM onvoldoende tegenwicht bieden', in: *Computerrecht*, nr. 3, p. 129; ECtHR 29 June 2006 App No 54934/00 *(Weber and Saravia)*, para. 95-100; ECtHR 1 July 2008 App No 58243/00 (*Liberty and Others v UK)*, para. 63.

30 ECtHR 4 December 2015 App No 47143/06 (*Roman Zakharov v Russia*), para. 232.

31 ECtHR 4 December 2015 App No 47143/06 (*Roman Zakharov v Russia*), para. 232.

32 ECtHR 29 June 2006 App No 54934/00 *(Weber and Saravia)*, para. 95.

33 CJEU 8 April 2014 Joined Cases C-293/12 and C-594/12 (*Digital Rights Ireland and Seitlinger)*, para. 54.

34 CJEU 8 April 2014 Joined Cases C-293/12 and C-594/12 (*Digital Rights Ireland and Seitlinger)*, para. 55.

35 ECtHR 1 July 2008 App No 58243/00 (*Liberty and Others v UK)*, para. 63.

36 ECtHR 13 November 2012, App No 24029/07 (*M. M. v UK*), para. 200.

proportionality this shift might be an issue since *Zakharov* as well as S*zabó* indicate that to perform a proper necessity-assessment regarding the application of surveillance powers there has to be a reasonable suspicion regarding the target person.[37] It remains up to the judge to point out what this means regarding the proportionality assessment for the application of bulk powers. Some scholars criticize the application of the necessity-assessment of the ECtHR for placing too much focus on the procedural embedding such as the manner in which the authorisation is granted, control on the execution of it, and the presence of independent oversight, instead of focusing on proportionality.[38]

Important and recent case-law of the CJEU regarding untargeted measures of surveillance shows that the Court is fairly critical. In 2014 the Court struck down the Data Retention Directive in the case *Digital Rights Ireland.* The Directive which was laid before the judges in that case did not meet the necessity requirement for three reasons. First, the comprehensive scope of the measure that "covers in a generalised manner all persons, all means of communication as well as traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime".[39] Secondly, because it did not determine the limits of the access of the competent national authorities to the data and their subsequent use by imposing substantive and procedural conditions in terms of a prior review by a court or independent administrative body.[40] And thirdly, the period of data retention was not deemed proportionate because there was no distinction being made between the categories of data based on possible usefulness or persons concerned, and the determination of the period must be based on objective criteria in order to ensure that it is limited to what is strictly necessary.[41]

The invalidation of the Directive led to questions whether national data retention measures can be adopted, whether EU law applies to them and if so, what safeguards are needed to be compliant with *Digital Rights Ireland*.[42] These questions were laid before the Court in *Tele2 Sverige/Watson.*[43] In this judgment the Court states that national legislation on the retention of traffic and location data and access to that data by the national authorities, for the purpose of combating crime, falls within the scope of Directive 2002/58/EC, the e-Privacy Directive.[44] Quintessential of this Directive is to guarantee the right to confidential communication.[45] Article 15 formulates the possibility for member states to implement limitations when this is necessary to guarantee national security. However, in *Tele2 Sverige/Watson* the Court states that it follows from the text of the article itself that it has to be interpreted in the light of the fundamental rights guaranteed by the Charter.[46] From this follows that the e-Privacy Directive precludes national legislation which "for the purpose of

37 ECtHR 4 December 2015 App No 47143/06 (*Roman Zakharov v Russia)*, para. 260; ECtHR 12 January 2016 App No 37138/14 (*Szabó and Vissy v Hungary)*, para. 71.

38 S. J. Eskens, 'Ongerichte interceptie, of het verwerven van bulk-communicatie, en waarom de Grondwet en het EVRM onvoldoende tegenwicht bieden', in: *Computerrecht*, nr. 3, p. 130.

39 CJEU 8 April 2014 Joined Cases C-293/12 and C-594/12 (*Digital Rights Ireland and Seitlinger)*, para. 57.

40 CJEU 8 April 2014 Joined Cases C-293/12 and C-594/12 (*Digital Rights Ireland and Seitlinger)*, para. 60-62.

41 CJEU 8 April 2014 Joined Cases C-293/12 and C-594/12 (*Digital Rights Ireland and Seitlinger)*, para. 63-64.

42 M. Tzanou, '*The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance'*, Oxford and Portland: Oregon 2017, p. 104.

43 CJEU 21 December 2016 Joined Cases C-203/15 and C-698/15 (*Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others)*, para. 59.

44 CJEU 21 December 2016 Joined Cases C-203/15 and C-698/15 (*Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others)*, para. 65-81.

45 Art. 5 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.

46 CJEU 21 December 2016 Joined Cases C-203/15 and C-698/15 (*Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others)*, para. 91.

fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication".[47] As well as national legislation "governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union."[48]

With a reference to *Zakharov*, the CJEU states that general access to all retained data cannot be regarded as limited to what is strictly necessary. National legislation needs to be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data of subscribers or registered users. As a general rule, the Court states, access can be granted in relation to the objective of fighting crime, but only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime. The Court continues with stating that only "in particular situations, for example when vital national or public security interests are threatened by terrorist activities, access to data of other persons might be granted in case of objective evidence showing that that data might, in a specific case make an effective contribution to combating such activities."[49]

The Court allows member states to adopt national legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited to what is strictly necessary, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted.[50] Article 4 of the Treaty on European Union prescribes that the EU shall respect the essential state functions, leaving in particular national security to remain the sole responsibility of each member state.[51] Whether EU law is applicable to activities, regarding national security, of the intelligence and security services specifically, is now laid in front of the Court in the form of a preliminary ruling.[52]

This possible lack of jurisdiction of the CJEU regarding national security does not occur with regard to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe (hereafter: Convention 108). It is the first legally binding international instrument in the field of data protection.[53] Convention 108 applies to all data processing, including data processing by intelligence and security

47 CJEU 21 December 2016 Joined Cases C-203/15 and C-698/15 (*Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others)*, para. 112.

48 CJEU 21 December 2016 Joined Cases C-203/15 and C-698/15 (*Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others)*, para. 125.

49 CJEU 21 December 2016 Joined Cases C-203/15 and C-698/15 (*Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others)*, para. 119.

50 CJEU 21 December 2016 Joined Cases C-203/15 and C-698/15 (*Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others)*, para. 108.

51 Art. 4 para. 2 Consolidated Version of the Treaty on European Union.

52 CJEU *(*Reference for Preliminary Ruling) C-623/17 (*Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others)*.

53 FRA, *Handbook on European Data Protection Law* Luxembourg, Luxembourg: Publications Office of the European Union 2014, p. 16; G. Greenleaf, *Balancing globalisation's benefits and commitments: Accession to Data Protection Convention 108 by countries outside Europe*, Strasbourg: Council of Europe Convention 108 Globalisation Conference 17 June 2016, p. 3.

services. It aims to protect the individual against abuse in the context of the collection and processing of data, and to regulate the transnational flow of personal data.[54] Foremost principles laid down in the Convention constitute the fair and lawful collection and automatic processing of data, the storage thereof being contingent on being used for specified legitimate purposes and not for use for ends that are incompatible with these purposes, and that the data may not be kept longer than strictly necessary.[55] It also aims to assure the quality of data; in particular the adequacy, relevancy, proportionality, and accuracy.[56]

The Convention aims to bring cross-border data protection that does not solely rely on the ECHR, since the latter is a 'closed document' which does not permit non-European and non-member states to participate.[57] To include these countries, representatives of Australia, Japan, Canada and the United States took part in the process of drafting the document. However, none of these countries have signed up (so far).[58] All EU member states have ratified the Convention, and in 2013 Uruguay was the first non-European country to accede.[59] This might have been the start of the globalisation process of the document, with Mauritius being the second country to accede, and Cape Verde, Morocco, Senegal and Tunisia currently at different stages of accession.[60] The globalisation of the document makes more sense as more countries, especially outside of Europe, are in the process of implementing national data protection laws. Since 2015 the majority of these laws are from outside of Europe.[61] With this globalisation and increase of national laws, the need for a global, universal standard increases. The general and technologically neutral nature, the coherence and compatibility with other relevant legal frameworks and the open character of the Convention gives it a unique potential of a universal standard, and a basis for promoting data protection at a global level.[62]

In 2010 the need was expressed to modernise the Convention to reinforce the protection of privacy in the digital area against challenges accompanying the use of new information - and communication technologies, and to strengthen the Convention's follow-up mechanism.[63] This modernisation however brings along a re-thinking of the document, and with the ongoing globalisation process, more countries with different views and standards

54 FRA, *Handbook on European Data Protection Law*, Luxembourg: Publications Office of the European Union 2014, p. 16.

55 FRA, *Handbook on European Data Protection Law*, Luxembourg: Publications Office of the European Union 2014, p. 16.

56 FRA, *Handbook on European Data Protection Law*, Luxembourg: Publications Office of the European Union 2014, p. 16.

57 Council of Europe, *Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, Strasbourg: Council of Europe, 28 January 1981, p. 5.

58 J. Polakiewicz, *Convention 108 as a global privacy standard?*, Budapest: International Data Protection Conference 17 June 2011, p. 4.

59 FRA, *Handbook on European Data Protection Law*, Luxembourg: Publications Office of the European Union 2014, p. 16.

60 G. Greenleaf, *Balancing globalisation's benefits and commitments: Accession to Data Protection Convention 108 by countries outside Europe*, Strasbourg: Council of Europe Convention 108 Globalisation Conference 17 June 2016, p. 1; See for current list https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures.

61 G. Greenleaf, *Balancing globalisation's benefits and commitments: Accession to Data Protection Convention 108 by countries outside Europe*, Strasbourg: Council of Europe Convention 108 Globalisation Conference 17 June 2016, p. 1.

62 https://www.coe.int/en/web/data-protection/convention108/modernisation, accessed 19 March 2018.

63 https://www.coe.int/en/web/data-protection/convention108/modernisation, accessed 19 March 2018; FRA, *Handbook on European Data Protection Law*, Luxembourg: Publications Office of the European Union 2014, p. 17.

regarding privacy and data protection have a say in what the standards in the modernised Convention should look like. Therefore it remains to be seen what the exact implementation of the principles within the document will look like when this process is finished.

The UN Special Rapporteur on the right to privacy (hereafter: SRP) Joseph Cannataci invested considerable efforts in the organisation of the annual International Intelligence Oversight Forum since 2016.[64] The aim of this event is to start an open debate on the adequacy of oversight mechanisms, existing and future surveillance measures that might impact the right to privacy, the distinction between targeted and untargeted surveillance, and the proportionality, cost-effectiveness and overall efficacy of surveillance measures.[65]

Apart from that, the SRP believes in the importance to achieve synergy between national security interests and the right to privacy to maintain “cyberpeace”. Therefore, he pleads for measures that limit surveillance and other privacy-infringing measures in the avoidance of cyberwar, and explored options for a “draft legal instrument on government-led surveillance and privacy” to strengthen existing standards and create more detailed guidance and protection mechanisms that are able to address large-scale infringements of the human right to privacy of people around the world.[66] This document has been drafted as a result of several research projects and the meetings of and exchanges between several parties involved in shaping the development and use of digital technologies; such as global technology companies, experts from civil society, law enforcement agencies, intelligence services, and academics. The provisions of the text are based on international human rights law and aim at providing guidance for government surveillance using electronic means. This is deemed necessary for both human rights and the responsible and dignified conduct of state authority and powers.[67]

64 HRC Report of the Special Rapporteur on the right to Privacy Joseph A. Cannataci, *UN Doc*. A/HRC/34/60, p. 3-4.

65 HRC Report of the Special Rapporteur on the right to Privacy Joseph A. Cannataci, *UN Doc*. A/HRC/34/60, p. 3.

66 HRC Report of the Special Rapporteur on the right to Privacy Joseph A. Cannataci, *UN Doc*. A/HRC/37/62, p. 5.

67 HRC Report of the Special Rapporteur on the right to Privacy Joseph A. Cannataci, *UN Doc*. A/HRC/37/62, Appendix 7, p. 3.

4. Capabilities.

4.1 Bulk interception.

Paragraph 3.2.5.6.3 of the Wiv 2017 describes the capability of case-specific investigation of communications (‘*onderzoeksopdrachtgerichte interceptie’,* hereafter: bulk interception). Arguably, this capability is the most notorious within the Dutch debate, and it is the capability which led to the name ‘*sleepwet’*, a portmanteau word of the Dutch word for dragnet (‘*sleepnet’*) and the Dutch word for law (‘*wet’*). The total capability consists of a subset of provisions. The essence is the capability to collect, which is described as ‘to use technical supports for case-specific interception, receipt, recording and tapping of any form of telecommunication or data transfer by means of an automated information system, regardless of the locations involved’.[68] Apart from collecting, the subset includes the capability to decrypt telecommunication or data, as well as to conduct technical analysis on the data to optimise the exercise of the power.[69] Furthermore, it includes the power to filter, select and store metadata and content, and entails several obligations for telecommunication providers to cooperate.[70]

Particularly concerning seems the envisaged scope of such bulk interception. At the outset, it is determined by the ‘research order’ (‘*onderzoeksopdracht’).* The Prime Minister, the Minister for the Interior and Kingdom Relations and the Minister for Defense will lay down the Integrated Intelligence and Security Services Order (‘*Geïntegreerde Aanwijzing Inlichtingen- en Veiligheidsdiensten’,* hereafter: GA) pursuant to article 6 of the Intelligence and Security Services Act, within the prescribed tasks of the services. These are for the general services: Investigating targets that form a threat to the democratic rule of law, national security or other important interests of the state and investigating other countries.[71] The GA, which has a validity of four years, includes specific research orders. Acute research orders can be added by the Minister of Interior Affairs and/or the Minister of Defense.[72] This gives some insight in how research orders are formulated and by whom. However, it does not entail any information about the scope of the research orders, and thus of how large-scaled the effect of the bulk interception will be.

Apart from concerns about the unclarity of the exact scope, there is criticism regarding the necessity assessment of bulk interception. As follows from European case-law, the application as well as the introduction of new capabilities need to meet the necessity requirement.[73] As Lenaerts and van Nuffel describe, this assessment should include, apart from a subsidiarity test, a fact-based assessment of the effectiveness of the measure for the objective pursued.[74] Critics in the debate address that the Dutch legislator did not address this necessity requirement sufficiently. The NJCM, the Dutch section of the International Commission of Jurists, states in its reaction to the Bill that the explanatory report fails to give sufficient argumentation for why present capabilities do not suffice and which (serious) problems the new capabilities will be solving. The Commission states that

68 Art. 48 para. 1 Intelligence and Security Services Act 2017.

69 Art. 48 para. 1 Intelligence and Security Services Act 2017.

70 Artt. 48-50 Intelligence and Security Services Act 2017.

71 Art. 6 para. 1 jo. art. 8 para. 2 sub a and d Intelligence and Security Services Act 2017.

72 *Parliamentary Papers II* 2016/17, 34588, 3, p. 30-33.

73 ECtHR 4 December 2015 App No 47143/06 (*Roman Zakharov v Russia)*, para. 232; ECtHR 6 September 1978 App No 5029/71 (*Klass and Others v Germany*), para. 34-36 and 41; ECtHR 18 May 2010 App No 26839/05 (*Kennedy v UK*), para. 119 and 124.

74 G. Vermeulen and E. Lievers (eds.), ‘Surveillance for public security purposes: Four pillars of acceptable interference with the fundamental right to privacy’, in: *Data Protection and Privacy under Pressure: Transatlantic tensions, EU surveillance and big data*, Antwerp, Apeldoorn, Portland: Maklu 2017, p. 179.

because of the lack of this information it is not possible to assess to what extent the infringements on fundamental rights are justified.[75]

It is remarkable that the bulk interception capabilities in the law reforms in the UK as well as in Germany make a difference between foreign and domestic communication, where this division is not made in the Netherlands. Discussing this aspect in detail, there is a distinction between three kinds of communication: Purely national communication referred to as domestic; national-foreign communication where either the sender or the receiver is foreign, referred to as international; and purely foreign communication referred to as foreign. In both the UK and Germany, bulk interception of communications data is not allowed when it comes to purely domestic communication.[76] De-jure this appears to be a great difference from the Dutch Act. However, it is unclear whether the difference is as relevant when considering the technological context and de-facto circumstances. For example, if two persons within the British Islands are communicating with each other via a platform of which the server is located in a foreign country, the communication will fall in the category of international communication. Hence, the category sounds more encompassing than it appears to be in practice. Also, it is extremely hard to know in what category your data falls, since you need to have information on the location of the servers of the services you are using, which most of the time is not the case.

The German system even makes a more specified distinction as international communication falls within the stricter regime of the Act on Restrictions on the Secrecy of Mail, Post and Telecommunications (‘*Gesetz zur Beschränking des Brief-, Post- und Fernmeldegeheimnisses’,* hereafter: G10 Act) derogated from article 10 of the German Constitution. To filter the data and process it according to the correct regime the services use an automatic filtering system called DAFIS. The system has three filters to remove all communication protected by the G10 regime before the BND can process the data. Federal Data Protection Commissioner Andrea Voßhoff is critical, stating in a secret report that the system has substantial systemic deficits: “The DAFIS filter does not completely detect and filter data from individuals protected by article 10 of the Constitution. Hence, the BND has – contrary to legal obligations resulting from the G10 law – processed personal data of these individuals and has unlawfully intervened in communication that is protected by article 10 of the Constitution.”[77]

The SRP reflects negatively on this distinction, calling it an expression of the xenophobic fallacy some governments promote that “it’s only nasty foreigners which are out to get us… and therefore they don’t deserve their fundamental human rights to be respected by our laws”.[78] The SRP argues that, since the vast majority of terrorist attacks in Europe were carried out by EU citizens it is a fallacy that it makes sense to discriminate against people whose citizenship lies not within the lawmakers’ jurisdiction.[79] Unfortunately, the idea of the threat being foreign, and the infringements being less problematic when they happen to non-Dutch citizens, plays a part in the Dutch discourse as well. In the letter describing the proposed changes after the referendum, the Dutch government states it is

75 NJCM, Reactie op concept-wetsvoorstel, Leiden: 31 August 2015, p. 2 <https://njcm.nl/wp-content/uploads/2016/12/Reactie-consultatie-WIV-NJCM.pdf>.

76 Art. 136 para. 1-3 Investigatory Powers Act 2016; Art. 5 Act on Restrictions on the Secrecy of Mail, Post and Telecommunications and artt 6 and 7 Federal Intelligence Service Act.

77 https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/#Sachstandsbericht, accessed 20 March 2018.

78 HRC Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, *UN Doc*. A/HRC/34/60, 24 February 2017, p. 36.

79 HRC Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, *UN Doc*. A/HRC/34/60, 24 February 2017, p. 36.

practically ruled out that bulk interception of domestic communication on the cable will be implemented in the coming years (except for research of cyberdefence).[80] From case-law of the ECtHR it follows that infringements on an individual's right to privacy made within the territory of a state also falls within the jurisdiction of this state. According to the Court it is irrelevant whether said individual is located within this territory as well.[81] This means that states are equally responsible for infringements made on the right to privacy of individuals involved in domestic communication as in international or foreign communication, and thus renders the distinction irrelevant.

Since the law itself does not entail any information about the scope, this has been raising questions from the beginning of the debate. In the parliamentary debate and the explanatory memorandum, Minister Ronald Plasterk gives the examples of intercepting the Internet traffic between Syria and the Netherlands to gather all metadata.[82] He states the capability will not be used to intercept all communications within a city like The Hague for a month.[83] However, outside of the public debate, in confidential communication with Internet providers that have been leaked through the platform Publeaks, other examples are given: An interception of all Internet traffic between a city of 400.000 inhabitants and a certain communication service like WhatsApp is mentioned. Another example makes clear that data of individuals connected with a public WiFi hotspot and visiting a website hosted in a specific foreign country can be intercepted. And also, where Minister Plasterk mentions the term of one month in the public debates, he mentions a year in the confidential documents.[84] The distress caused by this unclarity led to some commitments in the coalition agreement stating that "random and massively collecting data of citizens in the Netherlands or abroad can, must and will not be the case".[85] Critics question the added value of this sentence, since random data collection is already contrary to the legal abilities of the services by law. The second extra-legal safeguard in the coalition agreement is the acceleration of the evaluation from five to two years.[86]

After the referendum one of the proposed changes by the government is to formulate a policy rule that special powers have to be applied in an as targeted manner as possible. The infringement on fundamental rights of third parties is explicitly taken into account and the scope of the application will be assessed within the legal requirement of proportionality.[87] This policy rule should be incorporated into the law as soon as possible.[88] Critics state that since the services already have the obligation to take infringements of fundamental rights into account, and to assess the application of powers to the legal requirements of proportionality and subsidiarity, the added value of the proposal again remains unclear.

When implementing the capability, the services will consult telecommunication providers to

80 *Parliamentary Papers II* 2017/18, 34588, 70, p. 3-4.

81 N. A. N. M. van Eijk and C. M. J. Ryngaert, 'Deskundigenbericht: Juridische grondslag multilaterale informatie-uitwisseling', bijlage IV in: CTIVD, '*Toezichtsrapport over de multilaterale gegevensuitwisseling door de AIVD over (vermeende) jihadisten*', nr. 56, 28 March 2018, p. 4.

82 *Parliamentary Papers II* 2016/17, 34588, 50, p. 86.

83 *Parliamentary Papers II* 2016/17, 34588, 3, p. 125.

84 https://nos.nl/artikel/2100411-plasterk-denkt-na-over-aftappen-chat-apps-en-wifi-hotspots.html, accessed 20 March 2018.

85 VVD, CDA, D66 en ChristenUnie, *Vertrouwen in de toekomst, regeerakkoord 2017-2021*, 10 Oktober 2017, p. 4.

86 VVD, CDA, D66 en ChristenUnie, *Vertrouwen in de toekomst, regeerakkoord 2017-2021*, 10 Oktober 2017, p. 4.

87 *Parliamentary Papers II* 2017/18, 34588, 70, p. 3.

88 *Parliamentary Papers II* 2017/18, 34588, 70, p. 5.

select which specific fibers are to be intercepted.[89] During the interception, the data will be technically analyzed to judge whether the right fiber is being intercepted.[90] Intercepted data can be saved up to three years after collection, awaiting to be processed.[91] In case data is encrypted this three year term can be prolonged each time with another three years, without a fixed maximum term, and starts again after decryption.[92] Critics state that this 3 year term is too long, and the motivation for it is weak. The motivation given in the explanatory memorandum is that the one-year storage term in the old Act was experienced as a bottleneck and had to be prolonged to enable the services to work with historical data.[93] In the letter on adjustments to the Act after the referendum, the government proposed to change the maximum term to one year, which can be prolonged yearly with the permission of the Minister to a maximum of three years.[94]

In the UK there is no explicit storage term, storage of data needs to be necessary and proportionate. Within the German G10 regime the necessity of the gathered data for the purposes of the services will be reviewed every six months, and data should be deleted when not deemed necessary any longer.[95] However, a recent case of Reporters Without Borders made clear that once data is collected, it is never deleted entirely.[96] Data acquired through bulk interception within the BNDG regime is divided into metadata, which can be retained for six months, and content data, which can be saved up to 10 years.[97]

The processing of the intercepted data starts with filtering. First, a negative filter deflects data which is irrelevant due to its format. The Minister states that at this point, 98% of the intercepted data is expected to be deleted.[98] This number sounds like a lot, giving the impression that 2% cannot be that bad. However, 2% is still an incredibly huge amount of data in absolute numbers, since the entire amount of the data stream is enormous. Also, examples given by the Minister of the kind of data that will be deflected due to its format are associated with services like Netflix, Spotify, Bittorrent and Youtube.[99] These examples all entail services that use large amounts of bandwidth, and none entail communications data. Hence, in terms of percentage of the amounts of data volume this adds up, but in terms of sensitive data in connection with the infringement of privacy or data protection, such data is practically not relevant. The interception of personal and communications data is potentially much more sensitive, while the format of this information is smaller in terms of overall data volume, and therefore accounts for a smaller percentage of the total amount of data in the data stream.

Another aspect of the processing is investigating the intercepted data to determine the characteristics and the nature of the telecommunication, to determine the identity of the person or organisation involved in the telecommunication, to determine and verify selection criteria related to targets, and to identify persons or organisations eligible for

89 *Parliamentary Papers II* 2017/18, 34588, 69, attachment, p. 3.

90 Art. 48 para. 1 Intelligence and Security Services Act 2017.

91 Art. 48 para. 5 Intelligence and Security Services Act 2017.

92 Art. 48 para. 6 Intelligence and Security Services Act 2017.

93 *Parliamentary Papers II* 2016/17, 34588, 3, p. 131.

94 *Parliamentary Papers II* 2017/18, 34588, 70, p. 3.

95 Art. 4 Act on Restrictions on the Secrecy of Mail, Post and Telecommunications.

96 https://www.juris.de/jportal/portal/page/homerl.psml?nid=jnachr-JUNA171206018&cmsuri=%2Fjuris%2Fde%2Fnachrichten%2Fzeigenachricht.jsp, accessed 11 january 2018. Judgment is not published yet, accessed 9 January 2018.

97 https://lawfareblog.com/new-rules-sigint-collection-germany-look-recent-reform, accessed 9 January 2018.

98 *Parliamentary Papers II* 2017/18, 34588, 69, attachment, p. 3.

99 *Parliamentary Papers II* 2017/18, 34588, 69, attachment, p. 3.

investigation by the service within the context of ongoing investigations.[100]

Thereafter, a distinction will be made between metadata and content. Content data will pass through a positive filter consisting of selectors. Examples of selectors are telephone numbers or IP-addresses. In a letter, the Minister states that content data that is deemed irrelevant will not be saved and is made irretrievable.[101] However, in the explanatory memorandum it is explained that based on article 48, information will be available for processing for a maximum of three years. If relevant, content data leads to new knowledge and insights, and the services might want to filter data again with new selectors based on the updated knowledge.[102] It is unclear how the irretrievability of data which is deemed irrelevant, and the refiltering of this same data based on updated knowledge relate to each other, or how this will turn out in practice. After all, irretrievable data cannot be (re)filtered. Content that is deemed relevant will be involved in the research and will also be available for other investigations.[103] Metadata will be used for automated data analysis. The law gives a non-exhaustive list of possible conduct that falls within 'automated data-analysis': To compare data with each other and in combination to each other in an automated manner, to search on the basis of profiles, and to compare in order to find specific patterns.[104]

Authorisation has to be granted by the Minister at several points: To start the interception, to do the technical analysis, to determine and verify selection criteria, to identify persons or organisations eligible for investigation, to select content data, and to perform automated data analysis on the metadata.[105] And, as aforementioned, in case the proposed adjustments will be integrated in the law, to prolong the storage of data. The Review Board on the Use of Powers ('*Toetsingscommissie Inzet Bevoegdheden',* hereafter: TIB) will conduct a lawfulness-assessment on this authorisation.[106] In comparison, to apply the capability of bulk interception in the UK the Minister has to grant authorisation, of which the Judicial Commissioner has to approve.[107] In Germany, bulk interception within the G10 regime can start after authorisation of the G10 Commission which will then conduct monthly supervision.[108] Within the BNDG regime of foreign communication data, authorisation of the Chancellery is requested and oversight is performed by the Independent Committee (hereafter: UG).[109] I will elaborate further on this point in the paragraph on oversight and control mechanisms.

To be able to collect data, the services require cooperation of providers of telecommunication networks and services. The Act entails several obligations to cooperate with and inform the services, as pertaining to the collection of data based on the case-specific investigation of communications capability.

This obligations entail:

- Provision of the relevant information to map the communication landscape.[110]

100 Art. 49 para. 1 and 2 Intelligence and Security Services Act 2017.
101 *Parliamentary Papers II* 2017/18, 34588, 69, attachment, p. 3.
102 *Parliamentary Papers II* 2016/17, 34588, 3, p. 142.
103 *Parliamentary Papers II* 2016/17, 34588, 3, p. 142.
104 Art. 60 para. 2 Intelligence and Security Services Act 2017.
105 Artt. 48-50 Intelligence and Security Services Act 2017.
106 Art. 32 para. 2 and art. 36 para. 1 Intelligence and Security Services Act 2017.
107 Art. 138 Investigatory Powers Act 2016.
108 Art. 10 para. 5 Act on Restrictions on the Secrecy of Mail, Post and Telecommunications.
109 https://lawfareblog.com/new-rules-sigint-collection-germany-look-recent-reform, accessed 9 January 2018.
110 Art. 52 Intelligence and Security Services Act 2017.

- The technical execution of the capability itself.[111]
- The provision of information regarding telecommunication of customers.[112]
- The provision of information regarding a customer and its communication traffic.[113]
- The provision of personal information of customers.[114]
- The provision of all necessary cooperation in decrypting data. This obligation applies to everyone who can be reasonably expected to have knowledge about the manner of encryption.[115] This obligation can apply to legal persons and corporations, but it can also apply to individuals.

Refusing to comply with any of these obligations is prosecutable.[116]

The collection of data in bulk poses a big challenge in terms of guaranteeing professional secrecy. According to the Wiv 2017 this data has to be destroyed immediately, unless processing of the data is necessary in terms of the investigation in which context the data has been collected and there is approval of the Court in The Hague.[117] The problem is, however, that it is inherent to bulk collection of communication data to initially gather this data despite the above restriction. Without a special system with, for example, number recognition that marks and automatically excludes this data, the services do have access to this privileged communication.[118] Safeguards only come into play when the services want to use this information in their investigations. In the explanatory memorandum it is stated that, with regard to the interest of national security, it is deemed undesirable to categorically exclude certain communication from the use in investigations of the services on forehand.[119]

111 Art. 53 Intelligence and Security Services Act 2017.
112 Art. 54 Intelligence and Security Services Act 2017.
113 Art. 55 Intelligence and Security Services Act 2017.
114 Art. 56 Intelligence and Security Services Act 2017.
115 Art. 57 Intelligence and Security Services Act 2017.
116 Art. 143 Intelligence and Security Services Act 2017.
117 Art. 27 para 2 Intelligence and Security Services Act 2017.
118 *Parliamentary Papers II* 2016/17, 34588, 3, p. 56.
119 *Parliamentary Papers II* 2016/17, 34588, 3, p. 56.

4.2 Hacking capability.

The hacking capability might be the most important capability of the new law, since some say that bulk interception of communications data is already an outdated practice. Huib Modderkolk, a Dutch research journalist specialised in the conduct of the services, explains in the Dutch podcast '*Volkskrantgeluid*' that the hacking capability is a more efficient and workable capability for the services. With bulk interception it is only possible to intercept information that is transferred at that moment. With the hacking capability it is possible to hack into servers, where the services could also get to emails that have already been sent, and are now stored on the server.[120] David Anderson, Independent Reviewer of Terrorism Legislation in the UK, agrees, writing in his *'Operational Case for Bulk Powers'* report that the growing use of encryption has made the acquisition of data through interception more difficult, and that hacking might be the only option to obtain this information.[121] Encryption is mostly used for communications data during the transmission thereof. After transmission the data is stored on a device, however, and the hacking capability provides for the possibility to access the data once it is stored.

In the old Act (Wiv 2002) the services already had the capability to 'enter automated works (for the meaning of this term see next indention) with the use of technical tools, false signals, false keys or false representation and to break security, apply technical equipment to decrypt data processed or stored in the automated work, and copy the data stored or processed in the automated work'.[122] In short, this means that under the old Act the services were able to hack into the devices of a target, decrypt data that is stored on the device or sent/received by it, and copy this data. In the new Act four capabilities are added in this respect:

- To explore technical characteristics of automated works that are connected to a communication network.
- To enter an automated work through the automated work of a third party.
- Once the services have entered an automated work they can install malware to observe or implement a targeted tap.[123]
- Another notable aspect of this capability is the decryption order the services can file to everyone who has the information needed to decrypt information that is processed in or stored on the automated works. There is an obligation to cooperate with this order and it is a criminal act to refuse.[124]

Since the scope of the capability is based on the term 'automated work' it seems useful to briefly reflect on the meaning and scope of this term. The definition of automated work is broad, and is probably going to be broadened with a new definition in Dutch criminal law. This new definition will include every device or group of connected devices of which one or more automatically process data based on a program.[125] The government deemed restrictions undesirable since one of the aims of the Act is to make regulations which are ready for the future. Especially in the light of the 'Internet of Things', the scope of this capability will be substantial. The Internet of Things is a global infrastructure enabling more

120 https://soundcloud.com/volkskrantgeluid/sleepwetpodcast1?in=volkskrantgeluid/sets/special-de-sleepwet, accessed 20 March 2018.

121 D. Anderson, *Operational Case for Bulk Powers*, March 2016, p. 6, <https://www.gov.uk/government/publications/investigatory-powers-bill-overarching-documents>.

122 Art. 24 Intelligence and Security Services Act 2002.

123 Art. 45 para. 1 sub a and para. 2 sub c jo. art. 40 para. 1 and art. 47 para. 1 Intelligence and Secret Services Act 2017.

124 Art. 45 para. 9 jo. 12 jo. art. 143 Intelligence and Security Services Act 2017.

125 Art. 80 sexies Cybercrime Act 3, *Parliamentary Papers II* 2015/16, 34 372.

and more devices, vehicles and home appliances to be connected to the Internet and to exchange data. For example, this development enables a fridge to fall within the category, since it will be considered a device that is connected to the Internet and which automatically processes data based on a program. This data can be of importance to the execution of the task of the services[126] as it could, for example, provide information on when someone is at home.

The exploration of technical characteristics serves a supportive purpose to the entering of an automated work, which means that it will be used mostly to create the possibility to enter. The capability entails the use of technical equipment like IP- and port scanning software and registration tools to gain knowledge on the technical features of automated works on a communication network. These technical features will mostly be information that is openly available, like IP-addresses or the function of a specific automated work within a network. Based on these features, the services decide whether an automated work is relevant or not. Since networks are dynamic, and these features will change continuously, the services will be applying this capability semi-continuously.[127]

In case the services are not able to enter the automated work of a target because of well-functioning security systems, the services might be able to get to the information or device by hacking third parties. There is no definition of third parties in the Act, but in the explanatory memorandum it is explained that this refers to parties which are technically related to the target. Nevertheless, this seems like a very broad description, potentially including anybody from the party which installs a network or delivers a service or software to an individual civilian.[128] Regarding the hacking of third parties there are a few safeguards: There has to be separate authorisation from the Minister to hack into the automated work of the third party.[129] The interference with the privacy of the third party should be as little as possible, and the third party should not be more than a corridor to the automated work of the target.[130] In case there is any malware the services have an obligation of effort to remove it, otherwise it needs to be reported.[131]

The last new capability is the application of technical equipment in an automated network as a supportive measure of the capabilities to observe and to tap targets.[132] This means that the services can place malware on devices to activate the camera and/or microphone in it from a distance in order to observe or record conversations.[133] In case these capabilities get combined, separate authorisation for all conduct is required.

The scope of the hacking capability has expanded from being exclusively targeted to including third parties, which clearly has a greater scope when these are, for example, telecommunication providers. Like bulk interception, the hacking capability is a surveillance measure that has (potential) untargeted effects. Under the IPA 2016 in the UK there is, next to targeted equipment interference warrants, the term for the hacking capability under the IPA 2016, the bulk equipment interference warrant.[134] Again, where the Dutch Act does not make this distinction, the IPA 2016 requires that the main purpose of

126 *Parliamentary Papers II* 2016/17, 34588, 3, p. 100.
127 *Parliamentary Papers II* 2016/17, 34588, 3, p. 101.
128 *Parliamentary Papers II* 2016/17, 34588, 3, p. 102.
129 Art. 45 para. 5 Intelligence and Security Services Act 2017.
130 *Parliamentary Papers II* 2016/17, 34588, 3, p. 104.
131 Art. 45 para. 7 Intelligence and Security Services Act 2017.
132 Art. 45 para. 2 sub c jo. art. 40 para. 1 and art. 47 para. 1 Intelligence and Security Services Act 2017.
133 *Parliamentary Papers II* 2016/17, 34588, 3, p. 104-105.
134 Chapter 3 Investigatory Powers Act 2016.

bulk equipment interference must be to obtain overseas-related data.[135] The provisions on bulk equipment interference warrants do not give an exhaustive list of possible conduct. Warrants authorise any conduct that is necessary to undertake, in order to do what is expressly authorised or required by the warrant.[136] The scope of the capability is even extended to "any conduct of any person which is conduct in pursuance of a requirement by or on behalf of the person to whom the warrant is addressed to be provided with assistance in giving effect to the warrant."[137] The Code of Practice does describe some capabilities that fall within the warrant. This enumeration is comparable with the Dutch capabilities.[138] The IPA 2016 does exclude application of equipment interference in relation to communication data in transmission, since this requires an interception warrant.[139] However, it is possible to obtain communication information by monitoring, observing or listening in to a person's communications or activities and store this information under a targeted equipment interference warrant when expressly mentioned and authorised.[140]

In Germany, the capability of telecommunication surveillance ('*Quellen-Telekommunikationsüberwachung'*, hereafter: Quellen-TKÜ) entails the capability to infiltrate devices in order to monitor and record communication between targets with the use of monitoring software.[141] This capability was explicitly introduced to circumvent encryption, since electronic content in encrypted form could not be evaluated by the classical form of telecommunication surveillance.[142] The interception of communication in this manner enables the services to record the data directly from the user's device, as opposed to intercepting encrypted data from telecommunication networks. Authorisation regarding the collection of data in the application of Quellen-TKÜ is limited to such data which before was collected by tapping the network. This however leads to a contradictory situation de-jure and de-facto, since in implementation of Quellen-TKÜ the services need to install software like keyloggers to collect the data before transmission. The installation of software, however, falls outside the authorisation, since installing software requires access to the storage of a device.[143]

Comparable with the targeted hacking capability is the German capability of online search ('*Online-Durchsuchung',* hereafter: ODS) that allows for the access of foreign information technology systems via communication networks by means of monitoring software.[144] This capability is supposed to be applied in a targeted manner, but in case it is necessary for a proper execution of the task or in case of a suspicion that the target is using devices of other people, it can also be applied to third parties.

It is remarkable that both the German Act as well as the Act in the UK do make distinctions between foreign and domestic communication data; the same distinction that is made in the application of bulk interception. Regarding the hacking capability, the Dutch Act, again,

135 Art. 176 para. 1 sub c Investigatory Powers Act 2016.

136 Art. 176 para. 5 sub a Investigatory Powers Act 2016.

137 Art. 176 para. 5 sub b Investigatory Powers Act 2016.

138 Home Office, *Equipment Interference DRAFT Code of Practice*, December 2017, p. 9, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/668940/Draft_code_-_Equipment_Interference.pdf>.

139 Art. 176 para 5, 6 and 7 Investigatory Powers Act 2016.

140 Art. 99 para. 4 Investigatory Powers Act 2016.

141 Art. 4a jo. 20l Bundeskriminalamtgesetz.

142 https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html, accessed 21 March 2018.

143 https://netzpolitik.org/2014/geheimes-dokument-bundeskriminalamt-darf-finfisherfinspy-nicht-einsetzen-versucht-einfach-neue-version-nochmal/, accessed 21 March 2018.

144 Art. 20k Federal Criminal Law Act.

does not make this difference. Note, however, that it remains unclear what the meaning of this differentiation is de-facto and particularly considering the technological context. Another distinction that has been made in the hacking capabilities of the Acts of Germany and the UK is the difference between communication data in transmission, and stored information. Despite the obvious practical differences between access through interception and access through hacking, the Dutch Act does not legally exclude the option, or make the difference.

A request for authorisation of the hacking capability under the Wiv 2017 needs to entail a description of the technical risks of executing the capability.[145] This description is important for the balancing of interests and the proportionality assessment in the authorisation. The use of vulnerabilities, instead of disclosing them, and the installation of malware can bring along severe consequences for the general safety of the Internet. After all, if the services can enter a system because of a vulnerability in its security, others can as well. Targets are not the only ones using this software, so failure to report such vulnerabilities can have widespread consequences. Also, services themselves can get hacked. This happened in 2016 to the NSA by the Shadow Brokers who published all the unknown vulnerabilities, so-called *zerodays*, the NSA had. Several infectious bugs have been created by hacking groups based on these published vulnerabilities, for example “EternalRocks” and “WannaCry”.[146] This led, among other things, to the malfunctioning of the computer systems in British hospitals, and Dutch parking systems.[147]

Therefore, the services have to inform the National Cyber Security Center if they come across significant vulnerabilities that can have consequences for general Internet users. However, this obligation is not without exceptions, for example the protection of intelligence sources and the information position of the services.[148] The Review Committee on the Intelligence and Security Services (‘*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten’,* hereafter: CTIVD) writes that between the 17th of March 2016 and the 10th of March 2017 only one instance of a vulnerability was reported, and before their investigation none were reported.[149]

This policy is being criticized on the ground that if the victims do not know their problems are caused by abuse, they cannot file a complaint and their access to effective remedies is blocked. Another problematic aspect in this regard is that the consideration whether or not to report these vulnerabilities is made by the Joint Sigint Cyber Unit (hereafter: JSCU), the hacking team of the services, itself. In coming to a conclusion, the JSCU is weighing different interests against each other. There is no codified regulation of this procedure, and no reporting of the considerations made. This leads to a situation in which oversight and control bodies do not have any instruments to apply. The CTIVD described and criticised this situation under the old Act, calling it careless.[150] However, the new Act does not entail any new regulation in this respect.

145 Art. 45 para. 4 Intelligence and Security Services Act 2017.

146 https://www.cnet.com/news/doomsday-worm-eternalrocks-seven-nsa-exploits-wannacry-ransomware/, accessed 20 March 2018.

147 https://www.rtlnieuws.nl/buitenland/computerstoringen-in-britse-ziekenhuizen-door-cyberaanval; https://www.rtlnieuws.nl/nederland/parkeergarages-in-nederland-getroffen-door-wereldwijde-cyberaanval, accessed 20 March 2018.

148 *Parliamentary Papers II* 2016/17, 34588, 3, p. 106.

149 CTIVD, *Toezichtsrapport over de inzet van de hackbevoegdheid door de AIVD en MIVD in 2015*, nr. 53, 25 April 2017, p. 26.

150 CTIVD, *Toezichtsrapport over de inzet van de hackbevoegdheid door de AIVD en MIVD in 2015*, nr. 53, 25 April 2017, p. 26.

All capabilities of this subset can only be implemented after the Minister has granted authorisation, and the TIB has done an assessment in terms of lawfulness on this authorisation.[151] The authorisation is not bound to the device but to the target, meaning that if the target starts using another device, this device will be within the scope of the authorisation as well.[152] This 'extended authorisation' also applies to the aforementioned third parties.[153] This differs especially from the authorisation under the IPA 2016, where authorisation for bulk equipment interference includes all conduct necessary to undertake what is expressly authorised in the warrant, except for the interception of communication in transmission. This is called 'incidental conduct'. When incidental conduct is foreseen, it should be mentioned in the authorisation request, although unforeseen incidental conduct is regarded as lawful as well.[154]

151 Art. 36 para. 1 Intelligence and Security Service Act 2017.

152 Art. 45 para. 8 Intelligence and Secret Services Act 2017.

153 *Parliamentary Papers II* 2016/18, 34588, 3, p. 107.

154 Home Office, *Equipment Interference DRAFT Code of Practice*, December 2017, p. 12, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/668940/Draft_code_-_Equipment_Interference.pdf>.

4.3 Real-time access to databases.

This capability is a new extension of the already existing capability to consult informants (‘*informanten’*). The services can approach anybody who is supposed to have the information they need, including administrative bodies, telecommunication providers and civil servants, with a voluntary information request.[155] New in the Wiv 2017 is the possibility to answer this request in an automated manner. There are two ways to do this: Firstly, by granting the services direct automated access (hereafter: real-time access) to databases. Secondly, by providing the services with the automated data itself.[156] The latter option includes the acquisition of bulk data sets online.

The need for this capability, as argued in the explanatory memorandum, lies in the foreseeability of the need for the services to do structural information requests to the same informant. The example mentioned here is the “ContraTerrorism Infobox” (hereafter: CT Infobox).[157] This is a joint-venture between several parties of the intelligence, security and investigation domain. Most often, the capability will be combined with the capability of automated data analysis, which enables the services to search on profiles or patterns.[158]

There are great concerns about this capability. The Act states that services can approach anybody (‘*een ieder*’) and does not state that the services have to approach, for example, the head of a company or institution.[159] This leaves open the possibility to approach a system administrator or any other employee. The request is secret, meaning that if somebody answers it, the head, nor anyone else is informed of the data provision. The fact that the provision is a voluntary answer to a request creates the impression that the capability is less intrusive. However, the voluntary aspect applies to the provision by the informant, but this does not count regarding the data subject whose information is in the database.

Once real-time access has been granted, human intervention on the side of the informant will no longer be needed. In the Act and the explanatory memorandum is explained that provision of data will go on a so-called ‘hit/no hit basis’. This is explained as a comparison of the gathered data with data that is already in the system, and in case there is a so called ‘hit’, which is a connection between the compared data, information will be provided.[160] Further regulation on the functioning of this system is announced in the Act, but is not published so far.

The other application of the capability to consult informants is the acquisition of bulk data that third parties offer on the Internet. The availability of such data sets is the result of, for example, hacks or data leaks of companies or institutions.[161] The CTIVD describes in its report that the services acquired four bulk data sets between the 1st of January 2016 and the 11th of July 2017. Two of these consisted of names, email addresses and passwords of over 100 million persons, mainly persons that are not and will never be subject of an investigation.[162] The Review Committee writes that the acquisition of these data sets served a clear intelligence interest, existing in the necessity of the data for the

155 Art. 39 para. 1 Intelligence and Security Services Act 2017.

156 Art. 39 para. 3 Intelligence and Security Services Act 2017.

157 *Parliamentary Papers II* 2016/17, 34588, 3, p. 76.

158 *Parliamentary Papers II* 2016/17, 34588, 3, p. 77.

159 Art. 39 para. 1 Intelligence and Security Services Act 2017.

160 Art. 39 para. 4 Intelligence and Security Services Act 2017; *Parliamentary Papers II* 2016/18, 34588, 3, p. 76.

161 CTIVD, *Toezichtsrapport over het verwerven van door derden op internet aangeboden bulk data sets door de AIVD en de MIVD,* nr. 55, 28 December 2017, p. 3.

identification of targets and the use of the data within the implementation of the hacking capability.[163] Furthermore, the CTIVD writes that the bulk personal dataset which was of a general nature and contained personal data of a lot of Dutch citizens needed permission on a higher level because of these characteristics. This permission was not given, and thus the acquirement of this data was unlawful.[164]

The services in the UK are allowed to acquire bulk data as well. In the IPA 2016 this is defined as bulk personal data (hereafter: BPD) sets. These are large amounts of data that consists of personal information of a number of individuals of whom the majority are not, and are unlikely to become, of interest to the services. The services can keep these data sets after initial examination for the purpose of the exercise of its functions. The data set is held electronically for analysis in this context.[165] There are two kinds of warrants in this respect under the IPA 2016, a class BPD warrant that authorises the retention and examination of a certain class of databases and a specific BPD warrant authorising retention and examination of the specific database mentioned in the warrant.[166] This distinction enables the application of a more strict regime to databases that contain separable identifying data and/or health records or consists for a substantial part of sensitive personal data, and hence require a specific BPD warrant.[167] It is remarkable that in the Dutch Act the oversight body classifies the level on which permission is needed according to this difference, but the Dutch Act does not itself account for this difference. Therefore, it might be a valid suggestion to include this difference in the Dutch Act as well.

In Germany, the services do not have a capability that gives the services real-time access to databases. The BND does want to use information from social media like Facebook and Twitter.[168] Because of the amount of information shared on these platforms they can be interpreted as collective databases. However, since this entails research in open sources, where the information is added voluntarily by the data subjects themselves, knowing that this information is openly accessible, it is clearly distinguishable from the capability to get automated access to databases via informants. A comparison with the capability of systematic data gathering in open sources is more accurate.[169]

The classification of this capability as a regular power instead of a special power is a source of concern. There will be further elaboration on this distinction in the paragraph on oversight and control. For now, it suffices to state that regular powers do not require authorisation from the Minister, and thus are withdrawn from the control of the TIB. From the report of the Review Committee it becomes clear that the JSCU, who executes the capability, took the initiative to formulate internal policy.[170] This policy requires authorisation from the Minister before acquisition of data sets that contain personal information of a

162 CTIVD, *Toezichtsrapport over het verwerven van door derden op internet aangeboden bulk data sets door de AIVD en de MIVD*, nr. 55, 28 December 2017, p. 3-5.

163 CTIVD, *Toezichtsrapport over het verwerven van door derden op internet aangeboden bulk data sets door de AIVD en de MIVD*, nr. 55, 28 December 2017, p. 4.

164 CTIVD, *Toezichtsrapport over het verwerven van door derden op internet aangeboden bulk data sets door de AIVD en de MIVD*, nr. 55, 28 December 2017, p. 4.

165 Art. 199 Investigatory Powers Act 2016.

166 Art. 200 Investigatory Powers Act 2016.

167 Art. 202 para. 1 and 2, and art. 203 Investigatory Powers Act 2016.

168 https://www.stern.de/digital/online/projekt-des-bnd-ueberwachung-von-facebook-und-co—kein-grundrechtseingriff-3944568.html, accessed 22 March 2018.

169 Art. 38 Intelligence and Security Services Act 2017.

170 CTIVD, *Toezichtsrapport over het verwerven van door derden op internet aangeboden bulk data sets door de AIVD en de MIVD*, nr. 55, 28 December 2017, p. 8.

large amount of persons.[171] This is a good practice, however it remains unclear why this is not adopted as a requirement in the Act.

171 CTIVD, *Toezichtsrapport over het verwerven van door derden op internet aangeboden bulk data sets door de AIVD en de MIVD,* nr. 55, 28 December 2017, p. 4.

4.4 The provision of data to foreign services.

Since the scope and scale of surveillance measures concerned with the acquisition of data are increasing, so are the scope and scale of the exchange of data between governments.[172] This, in turn, increases the capability to provide information to foreign services, causing them to pose more far-reaching infringements upon human rights, especially the right to private life. It is hard to get a grip on what data is exactly shared, with whom, how much data and how often. The agreements that are made within these cooperative relationships are typically confidential and thus not subject to public scrutiny.[173] According to the research of the European Union Agency for Fundamental Rights, almost all EU member states (27 out of 28) have adopted the practice of international intelligence cooperation in their domestic legal frameworks, defining and regulating the competences of intelligence services in this regard. However, very few member states have explicitly articulated the modalities for establishing and implementing international cooperation within these enabling laws. Few member states, among which is Germany[174], have detailed laws describing the procedure that intelligence services must follow in order to implement international cooperation in primary legislation. Other member states, among which the United Kingdom and the Netherlands, have established internal rules which govern the international exchange of information. These internal rules are drafted by the executive or the services themselves, and are mostly secret. However, in a few member states they are publicly available.[175] In the Netherlands, the internal rules of 2013 and 2014 are classified, but an assessment of these rules by the CTIVD is published.[176]

The Dutch Act describes two scenarios within which data can be provided to foreign services. The first one is within the context of a cooperative relationship. The services are authorised to establish cooperative relationships with countries that are eligible.[177] Before the establishment of such a relationship, the services perform a balancing act to determine the eligibility of the specific country, the nature of the shared data, and the intensity of the cooperation, if any.[178] The act does not give a limitative enumeration, but the following criteria are taken into consideration in any case: The democratic embedding of the service within the relevant country, the respect for human rights by the relevant country, the professionality and reliability of the relevant service, the legal powers and capabilities of the services in the relevant country, and the level of data protection guaranteed by the relevant service.[179] The result of the considerations of the services are laid down in so called ‘weighing notes’, which the Minister uses in the decision whether or not to grant the required authorisation.

Remarkable is the Dutch willingness to share. This appears in the first place from the fact

172 Privacy International, *Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards*, April 2018, p. 5, <https://privacyintyqcroe.onion/sites/default/files/2018-04/Secret%20Global%20Surveillance%20Networks%20report%20web%20(200).pdf>.

173 Privacy International, *Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards*, April 2018, p. 3, <https://privacyintyqcroe.onion/sites/default/files/2018-04/Secret%20Global%20Surveillance%20Networks%20report%20web%20(200).pdf>.

174 Act for Foreign-Foreign Signals Intelligence Gathering of the Federal Intelligence Service.

175 FRA, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Updates*, Luxembourg: Publications Office of the European Union 2017, p. 50.

176 CTIVD, *Toezichtsrapport over de invulling van samenwerkingscriteria door de AIVD en de MIVD*, nr. 48, 4 Mei 2016, p. 14-17.

177 Art. 88 para. 1 Intelligence and Security Services Act 2017.

178 Art. 88 para. 2 Intelligence and Security Services Act 2017.

179 Art. 88 para. 3 Intelligence and Security Services Act 2017.

that the AIVD plays a pioneering role within multilateral cooperations such as the Counter Terrorism Group (hereafter: CTG)[180] The cooperation within this Group intensified considerably under Dutch presidency, introducing a shared database of (personal) data to which all involved services have real-time access. The server of the CTG, as well as its operational platform, is located in Dutch territory.[181] The intensification of this cooperation, as well as the aforementioned willingness to share, also appear from the text of the law. The criteria that have to be met before data can be provided to foreign services within an established cooperative relationship are formulated as follows: The services can provide data to the service of the foreign country for the benefit of interests to be represented by these bodies, as long as these interests are not contradictory to the interests to be represented by the Dutch services, or a proper discharge of their functions.[182] The provision of data within a cooperative relationship can take place under the condition of no further provision by the foreign services, the so-called 'third party rule', but this is not an obligation.[183]

The logic of these criteria appears to be based on the '*quid pro quo'* principle, which is common practice between the intelligence services in their data exchange. It means that if one service gives something to the other, the other has to give something in return. The Dutch services seem more eager to share data than appears from the policies in Germany and the UK. The formulation of the provisions seem to display a logic of 'sharing, unless...'. The rules governing this practice in the UK unfortunately are not public, but are internal regulations that are kept confidential.[184] These are made by the heads of the services with the purpose to ensure that there is no more information obtained nor disclosed as is strictly necessary for the proper discharge of its functions or for the purpose of the prevention or detection of serious crime or criminal proceedings.[185] This formulation still leaves space. However, it displays a clear logic of minimization; 'only sharing if..'. The focus of the data provision within the German capability appears to be on purpose limitation. Before establishment of the cooperative relationship, the services draft a declaration of intent ('*Absichtserklärung'*) which specifies the objectives, scope, duration and specific guarantees. The declaration requires the approval of the Federal Chancellery before the relationship can be established.[186] Data collected in the context of cooperation can only be used for the purpose of this specific collection that is agreed on beforehand. Furthermore, the German Act prescribes that cooperation will only be authorised to the extent that it would be considerably more difficult, or impossible, to achieve the purposes and objectives without such cooperation.[187]

Axel Arnbak, lawyer at *De Brauw Blackstone Westbroek* and researcher at the *Institute for Information Law* at the University of Amsterdam, explains this Dutch willingness to share

180 The Counter Terrorism Group is a cooperation between 30 security services of all EU Member States, Norway and Switzerland, founded in the aftermath of the attack of 11 September 2001 in the United States.

181 CTIVD, *Toezichtsrapport over de multilaterale gegevensuitwisseling door de AIVD over (vermeende) jihadisten'*, nr. 56, 28 March 2018, p. 11, 13 and 23.

182 Art. 89 para. 1 Intelligence and Security Services Act 2017.

183 Art. 89 para. 3 jo. art. 65 Intelligence and Security Services Act 2017.

184 FRA, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Updates*, Luxembourg: Publications Office of the European Union 2017, p. 50.

185 IPT 5 December 2014 IPT/13/77/H *(Liberty & Others v GCHQ & Others)*, para. 18 (ii), (v) and (viii) and 42.

186 Art. 13 para. 5 Federal Intelligence Service Act and art 7a para 1 Act on Restrictions on the Secrecy of Mail, Post and Telecommunications.

187 Privacy International, *Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards*, April 2018, p. 26, <https://privacyintyqcroe.onion/sites/default/files/2018-04/Secret%20Global%20Surveillance%20Networks%20report%20web%20(200).pdf>.

data as serving the purpose of strengthening the international power relations of the Netherlands. He refers to a report of Dutch investigative journalist collective *De Correspondent* which describes the Dutch services as being the only Western service that still intercepted transceivers. In exchange for this data, the Dutch services were allowed to join the Five Eyes between 2006 and 2011.[188] This is a clear demonstration of how information can be transformed into power. Nowadays it might not concern transceivers anymore, but the Netherlands nevertheless has a unique data position again, due to the trans-Atlantic Internet cables entering the European continent via the Netherlands, and the AMS-IX being the biggest Internet exchange of the world.[189] To transform the incredibly large amount of data that passes through this point every day, the services need a capability to collect it, and a capability to share it: Bulk interception and a regime that is allowing this data provision.

Cause for concern is the fact that the establishment of a cooperative relationship is dependent upon a balancing act that neither entails a limited enumeration of criteria, nor a minimum bar. Since this procedure is not formulated as a hard rule with prescribed requirements, it does not exclude any countries, regardless to what extent the criteria are met, nor does it exclude the addition of extra criteria. The Administrative Evaluation Committee of the service ('*Commissie Bestuurlijke Evaluatie AIVD'*) has written in its report that these criteria are not deemed sacred, and there can be situations in which the exchange of information is deemed to be more important than sticking to the criteria. Also, more criteria are taken into consideration than are codified in the law: The creation of an information position, the building and maintaining of a strategic network, and specific operational reasons are explicitly mentioned in this regard.[190] The CTIVD has expressed critical notes on the performance of this balancing act by the services. The Committee makes reservations on the amount and depth of information the AIVD uses in their balancing acts and on the judgment to what extent the criteria are met. It states that fundamental information is missing, and the manner in which the policy framework is implemented in deciding which nature and intensity of cooperative relationship can be established is questionable.[191]

Apart from providing data within a cooperative relationship, the Act describes the capability to provide data without such a relationship. Article 64 allows for provision of data to foreign services with whom no cooperative relationship is established, in the context of a proper discharge of the functions of the services, based on an urgent and weighty reason.[192] Before provision, the authorisation of the Minister needs to be granted.[193] This is the sole ex ante safeguard, since the TIB will not perform a lawfulness assessment on this authorisation.[194] The CTIVD writes in its latest report that the cooperative relationships of the AIVD with foreign services are intensified. However, at this point there are insufficient safeguards regarding the protection of the rights of the individual included in the provision and processing of data within these cooperative relationships.[195] The Act is unclear on the point whether the third party rule applies to the provision of data without the establishment

188 A. Arnbak, 'Machtspositie Nederland drijfveer controversiële internettap: Referendum gaat over veel meer dan balans tussen terreurdreiging en privacy' in: *Het Financieele Dagblad* 25 January 2018, p. 9.

189 https://ams-ix.net/connect-to-ams-ix/benefits-of-connecting, accessed 26 April 2018.

190 Commissie Bestuurlijke Evaluatie Algemene Inlichtingen- en Veiligheidsdienst, *De AIVD in verandering*, November 2004, p. 113, <https://www.aivd.nl/publicaties/publicaties/2004/11/16/de-aivd-in-verandering-rapport-commissie-bestuurlijke-evaluatie-over-functioneren-aivd>.

191 CTIVD, *Toezichtsrapport over de invulling van samenwerkingscriteria door de AIVD en de MIVD*', nr. 48, 4 mei 2016, p. 23.

192 Art. 64 para. 1 Intelligence and Security Services Act 2017.

193 Art. 64 para. 2 Intelligence and Security Services Act 2017.

194 Art. 32 para. 2 Intelligence and Security Services Act 2017.

of a cooperative relationship.[196]

The role of the third party rule is a double one; it is important to note its potential function as a safeguard, but unfortunately it is used in a manner that limits oversight as well. While the rule prevents the loss of control over data which is provided to foreign services, the rule can also be used to prevent oversight bodies to gain access to information related to international agreements.[197] The Commissioner for Human Rights of the Council of Europe recommended that the access to information by oversight bodies should not be restricted by, or subject to this rule and should extend to all relevant information held by security services, including information provided by foreign bodies.[198] Unfortunately, this still appears to be a recurring practice.[199]

Within both scenarios the services have the ability to share unevaluated data; data that is collected by the services but not yet analyzed nor filtered. This provision requires authorisation from the Minister. In this case the Minister can grant authorisation for a year, during which the services can perform several consecutive provisions. In case the provision of unevaluated data concerns data collected through the application of bulk interception, the CTIVD needs to be informed.[200] The sharing of unevaluated data is part of the SIGINT cooperation.[201] The SIGINT Seniors Europe is a partnership between the United States, the United Kingdom, Australia, Canada, New Zealand, Belgium, Denmark, France, Germany, Italy, the Netherlands, Norway, Spain, and Sweden within which signals intelligence are shared.[202] Signals intelligence is defined by the NSA as "intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems".[203] A special feature of this SIGINT partnership is that joint intelligence products are made.[204]

The provision of unevaluated data has some inherent problematic aspects. Firstly, it is not possible to perform a proper necessity assessment in the same way as with evaluated data, since it is not clear to which persons the data is relating. The necessity assessment is addressed in multilateral agreements within the SIGINT partnerships.[205] However, since this is laid down in agreements between parties and not in the laws, it is not clear whether

195 CTIVD, *Toezichtsrapport over de multilaterale gegevensuitwisseling door de AIVD over (vermeende) jihadisten*, nr. 56, 28 March 2018, p. 31-32.

196 Art. 62 para. 1 sub d jo. artt. 64 and 65 Intelligence and Security Services Act 2017.

197 FRA, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Updates*, Luxembourg: Publications Office of the European Union 2017, p. 104, 106.

198 Council of Europe, *Democratic and effective oversight of national security services*, Strasbourg: Council of Europe, May 2015, p. 13.

199 Privacy International, *Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards*, April 2018, p. 14, <https://privacyintyqcroe.onion/sites/default/files/2018-04/Secret%20Global%20Surveillance%20Networks%20report%20web%20(200).pdf>.

200 Art. 89 para. 2 and art. 64 para. 1 and 3 Intelligence and Security Services Act 2017.

201 CTIVD, *Toezichtsrapport over de multilaterale gegevensuitwisseling door de AIVD over (vermeende) jihadisten*, nr. 56, 28 March 2018, p. 12.

202 Privacy International, *Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards*, April 2018, p. 8, <https://privacyintyqcroe.onion/sites/default/files/2018-04/Secret%20Global%20Surveillance%20Networks%20report%20web%20(200).pdf>.

203 https://www.nsa.gov/what-we-do/signals-intelligence/, accessed 8 May 2018.

204 CTIVD, *Toezichtsrapport over de multilaterale gegevensuitwisseling door de AIVD over (vermeende) jihadisten*, nr. 56, 28 March 2018, p. 12.

205 CTIVD, *Toezichtsrapport over de multilaterale gegevensuitwisseling door de AIVD over (vermeende) jihadisten*, nr. 56, 28 March 2018, p. 31.

this practice does not exceed strict necessity as prescribed by European case-law.[206] Secondly, it is not possible to properly weigh the infringements on the rights of individuals, as well as the extent to which the provision of data serves the interest of the cooperation, for the same reason. Because of these shortcomings, extra weight is put on the required authorisation of the Minister as a safeguard. The Minister estimates whether the risks that come with the provision are acceptable, in the light of the interest of the provision. The Minister bases his assessment on the weighing notes made by the services. For this safeguard to be effective it is essential that these weighing notes are made. Unfortunately, the CTIVD found in its investigation that they were not, resulting in the provision of unevaluated data between the 30th of June 2016 and the 6th of December 2016 without approval of the Minister.[207]

The law includes a transitional period of two years wherein the services do not have to apply the requirements of the new Act regarding weighing notes and the new criteria in the balancing act to existing cooperative relationships.[208] In December 2017 the Ministers write that the weighing notes of the countries that the Dutch services are cooperating with intensively will be finished by the time the new Act enters into force, the 1st of May 2018.[209] Within this category are all countries of the CTG and countries with whom the Dutch services work together closely within SIGINT partnerships.[210] After the voting of the referendum, this topic reoccurs in proposed adjustments by the government which entail that there will be made a weighing note on every country the Dutch services are providing with data.[211] What this means for the former promise regarding the weighing notes of countries that the Dutch services are cooperating with intensively, and when they are supposed to be finished, is not entirely clear. The CTIVD writes in its report that no weighing notes have yet been made. It declares this to be problematic because of the constituting function of the weighing notes for both the legal basis of the cooperation and the provision of data, as well as the determination of the bandwidth of the possible cooperation. This is why the CTIVD has been pressing in its reports since 2009 for the composition of the weighing notes.[212]

Concerns have been expressed in the debate regarding the oversight in this capability. The ex-post oversight of the CTIVD only reaches as far as the conduct of the Dutch services.[213] This means that after provision of data to foreign services, all control and oversight over the data is lost. This concern increases when relating to unevaluated data, especially when this is provided to foreign services with whom the Netherlands does not have a cooperative relationship. The unclarity of the applicability of the third party rule as a guarantee on providing data to these parties adds to this concern. Another concern in this respect is the provision of data collected through the application of bulk interception. When bulk interception is implemented, authorisation of the Minister is required, which has to pass the lawfulness assessment of the TIB. However, this lawfulness assessment applies specifically to the authorisation of applying this capability. The provision of the collected

206 CJEU 21 December 2016 Joined Cases C-203/15 and C-698/15 (*Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others)*, para. 119.

207 CTIVD, *Toezichtsrapport over de multilaterale gegevensuitwisseling door de AIVD over (vermeende) jihadisten*, nr. 56, 28 March 2018, p. 32.

208 Art. 166 Intelligence and Security Services Act 2017.

209 *Parliamentary Papers II* 2017/18, 34588, 69, p. 4.

210 CTIVD, *Toezichtsrapport over de multilaterale gegevensuitwisseling door de AIVD over (vermeende) jihadisten*, nr. 56, 28 March 2018, p. 20.

211 *Parliamentary Papers II* 2017/18, 34588, 70, p. 2.

212 CTIVD, *Toezichtsrapport over de multilaterale gegevensuitwisseling door de AIVD over (vermeende) jihadisten*, nr. 56, 28 March 2018, p. 22.

213 Art. 97 para. 3 Intelligence and Security Services Act 2017.

data to foreign services falls outside the scope of this assessment, and the mandate of the TIB does not extend to the authorisation of data provision, evaluated nor unevaluated. There seems to be a gap in the ex ante oversight on this point.

In general, there is a lack of oversight when it comes to the international sharing of intelligence between intelligence agencies. Several judicial institutions have expressed recommendations to address this. The UN Human Rights Committee has advocated for the implementation of effective and independent oversight mechanisms over intelligence-sharing of personal data. And the Council of Europe Commissioner for Human Rights has advocated for a mandate for oversight bodies to scrutinise the human rights compliance of the cooperation between intelligence services and foreign bodies, including information exchange.[214]

It is not always clear what the shared data is used for, but the consequences of the use of this data can be grave. Therefore, NGOs like Privacy International are worried that states may share intelligence that might be used to facilitate serious human rights infringements such as unlawful arrest or detention, extra-judicial killings, or torture and other cruel, inhuman or degrading treatment. Certain groups as dissidents, journalists, human rights defenders, or minorities can be particularly vulnerable to such abuse.[215] In operation 'Ocean Shield' the Dutch military intelligence service intercepted communications data of Somalis for years and shared the metadata with the NSA. In more than 50% of the cases, the Americans based their choice of drone strike targets on this data. A lot of innocent people were killed in these attacks as 'collateral damage'. The Somalis and their lawyers of Prakken d'Oliveira hold the Netherlands co-responsible for these attacks.[216]

214 Privacy International, *Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards*, April 2018, p. 30, <https://privacyintyqcroe.onion/sites/default/files/2018-04/Secret%20Global%20Surveillance%20Networks%20report%20web%20(200).pdf>.

215 Privacy International, *Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards*, April 2018, p. 10, <https://privacyintyqcroe.onion/sites/default/files/2018-04/Secret%20Global%20Surveillance%20Networks%20report%20web%20(200).pdf>.

216 https://beta.volkskrant.nl/nieuws-achtergrond/somali-victims-of-us-drone-strike-take-legal-action-against-the-netherlands~bb62e8d8/, accessed 8 May 2018.

4.5 Authorisation, oversight and control mechanisms.

The Council of Europe Commissioner for Human Rights stated “Security services have a number of characteristics that create the potential for human rights abuses if these services are not subjected to effective oversight and underpinned by effective laws. These characteristics include recourse to very invasive powers that can be used in a highly discretionary manner, undertaken largely in secret and, in some countries, viewed as an instrument of the incumbent government that can be used for political purposes.”[217] This quote emphasizes how important effective oversight and control mechanisms are. In the following section, I will elaborate on different aspects of authorisation, oversight and control mechanisms. These mechanisms are very complex and often integrated with the political and judicial system of a country. Since the scope of this research is limited I will focus on the elaboration of this theme to the six topics with the most importance to the Dutch Act and debate in this regard. This are extra safeguards on privileged communication, authorisation, oversight ex ante, oversight ex post, transparency and data protection.

Before turning to the detailed elaboration, it should be noted that the Dutch Act distinguishes between regular and special powers. Regular powers can be applied after authorisation by the Director-General of the AIVD, and in the fulfillment of any of the statutorily defined tasks of the service, as long as it is necessary, proportional and passes the subsidiarity test. Special powers are deemed to exert stronger infringements on civil rights, and can only be applied in the performance of certain tasks. For the execution of special powers, the services need to request authorisation of the Minister.[218]

Privileged data recognised in the Wiv 2017 concerns the confidential communication between a lawyer and his client, and information about the source of a journalist, where ‘source’ is defined in the Act as “persons that have provided data to a journalist for publication”.[219] Note that the protection is limited to this specific information, and does not cover the total scope of professional secrecy. The protection entails the obligation to acquire approval of the Court of The Hague before application of special powers towards lawyers or journalists, where this application can lead to the acquisition of this privileged data.[220] The reach of the protection of confidential lawyer-client communication goes beyond that of the protection of sources of journalists in two ways: In case of acquisition of privileged lawyer-client communication by application of a special power towards a third party, this data needs to be destroyed immediately, unless further processing is necessary in the context of the investigation in which they are acquired. In that case approval of the Court in The Hague is needed before further processing.[221] Secondly, in case of transmission to the Public Prosecutor, confidential lawyer-client communication is protected, and before transmission approval of the Court in The Hague is needed.[222]

Under the Wiv 2017, the protection of journalistic sources is only guaranteed in case of application of a special power towards the journalist, in so far as this application leads to information about the source.[223] However, the ECHR requires any interference with the

217 Council of Europe Commissioner for Human Rights, *Democratic and effective oversight of national security services, Strasbourg*, May 2015, p. 19, <https://rm.coe.int/1680487770>.

218 Art. 30 para. 1 Intelligence and Security Services Act 2017.

219 Art. 30 para. 2 Intelligence and Security Services Act 2017.

220 Art. 30 para. 2 and 3 Intelligence and Security Services Act 2017.

221 Art. 27 para. 2 Intelligence and Security Act 2017.

222 Art. 66 para. 3 Intelligence and Security Services Act 2017.

223 Art. 30 para. 2 Intelligence and Security Services Act 2017

right to protection of journalistic sources that could lead to their identification to be backed up by effective legal procedural safeguards. First and foremost among these safeguards is the guarantee of review by an independent and impartial body to prevent unnecessary access to information that might lead to disclosure of the sources' identity.[224] The ECtHR has criticised the Dutch government for not meeting these requirements before.[225] According to researchers of the Institute for Information Law of the University of Amsterdam this is the consequence of the Dutch doctrine on 'ministerial independence'. This doctrine requires the Minister to be accountable. In this regard, it might be problematic when prior consent of a judge is required. According to the research we can learn the following lesson regarding the division of tasks from the cases before the ECtHR: "The government and its services decide on who to surveil, it is up to the courts to decide whether it is justified".[226]

The scope of privileged communication under the IPA 2016 is broader than recognised in the Wiv 2017 since it entails the communication of journalists, lawyers and members of parliament. However, the safeguard in the Dutch Act is stronger, since in the IPA 2016 the application of powers towards privileged communication only calls for a stricter weighing of interests, where the Dutch Act requires prior judicial consent. In Germany, there are almost no safeguards respecting the professional secrecy of foreign communication in the BND regime. The civil society organization Reporters Without Borders took this as a reason to file a lawsuit.[227] The G10 regime, detailing domestic communications, does entail professional secrecy.

Regarding authorisation, the ECtHR emphasised this should not be done haphazardly, irregularly, or without due and proper consideration. In the assessment whether authorisation procedures are capable of protecting people against surveillance measures implemented in such a manner, the Court takes several factors into account; the authority competent to authorise the surveillance, the scope of review and the content of the interception authorisation.[228] In the Wiv 2017 authorisation is needed before application of special powers, and is granted by the Minister at request of the head of the relevant service. Authorisation is valid for a maximum period of three months and can be prolonged at request.[229]

In the UK it is also the Minister who grants the authorisation.[230] In Germany, a distinction is made between international communication data and foreign communication data. In case of international communication data, requests for authorisation are done by the BND through the Interior Ministry under the G10 Act. Regarding strategic surveillance of foreign communication, the 2016 law reform applies, introducing distinctive authorisation procedures for four different target groups. Regarding the content data of German citizens,

224 Council of Europe Platform to Promote the Protection of Journalism and Safety of Journalists, *The Protection of Journalistic Sources, a Cornerstone of the Freedom of the Press,* May 2017, p. 1, <https://rm.coe.int/factsheet-on-the-protection-of-journalistic-sources-may2017/16807178d7>.

225 ECtHR 22 November 2007 App No 64752/01 (*Voskuil v The Netherlands)*; ECtHR 14 September 2010 App No 38224/03 (*Sanoma v The Netherlands)*; ECtHR 22 November 2012 App No 39315/06 (*Telegraaf v The Netherlands).*

226 Q. Eijkman, N. A. N. M. van Eijk and R. van Schaik, *Dutch National Security Reform under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?,* University of Amsterdam: Amsterdam/Utrecht March 2018, p. 30.

227 https://rsf.org/en/news/bnd-law-german-bundestag-ignores-criticism-civil-society-and-breaches-constitution, accessed 9 February 2018.

228 ECtHR 6 December 2015 App No 47143/06 *(Roman Zakharov v Russia)*, para. 257.

229 Art. 29 para. 1 Intelligence and Security Services Act 2017.

230 Art. 138 para. 2 Investigatory Powers Act 2016.

ex ante authorisation needs to be provided by the G10 Commission, and provision of the search terms is obliged. Regarding the content data of public institutions of EU bodies and member states the UG needs to provide ex ante authorisation, and provision of the search terms is obliged. Regarding content data of EU citizens and the rest of the world, ex ante authorisation needs to be provided by the UG, and search term provision is not obligatory.[231]

Recurring remarks in the Internet consultations, the reaction of the CTIVD on the draft Bill, the conclusion of a study on the Dutch human rights framework of oversight on intelligence and security agencies, and the development of case-law of the ECtHR led to the introduction of a new commission for prior consent; the TIB.[232] The TIB consists of three members of which two are required to have at least six years of experience as a judge. The procedure to appoint the members is as follows: The appointment Committee proposes at least three persons for each role in the Committee, then the Parliament selects at least three members to recite to the Ministers who appoints the members.[233] Members of the TIB should be independent and cannot be members of the CTIVD at the same time.[234] There are no codified requirements of technical expertise within the TIB, although in the selection process the appointment Committee became convinced of the need for a technical expert, and thus the third member was appointed to fulfill this role specifically.[235] Noteworthy in this respect, is that the appointment Committee was not able to meet the legal requirement to propose three persons for this role.[236] Critics have been pointing to this process as well as the final appointment of Ronald Prins, the co-founder of the controversial company Fox-IT, as technical expert in the Commission.[237]

The TIB will perform a lawfulness assessment on the authorisation of the Minister to apply certain special powers. The exact intensity of this test, especially regarding the question whether it will include efficiency, is yet unclear, since the Act does not elaborate on this point.[238] The Minister provides the TIB with all the information it deems necessary. The application of the power will not start before the TIB has given a verdict. The judgment of the TIB is binding, and if the TIB states the authorisation is unlawful it will be canceled by law.[239] In case of expedition, the agencies can start when the Minister has authorised the application of the powers. Then the TIB forms a judgment on the authorisation as well as the expedient procedure. In case the TIB states the authorisation has been granted unlawfully, the data which has been acquired needs to be destroyed. In case the TIB states that authorisation has been granted lawfully, but the application of the expedient procedure is unlawful, the TIB decides what happens with the collected data.[240]

Although the TIB is often described as a form of prior judicial consent, it is not, since the TIB itself is not part of the judiciary. This means the Commission is functioning outside the reach of the Council for the Judiciary (*Raad voor de Rechtspraak).* However, it probably

231 https://www.lawfareblog.com/new-rules-sigint-collection-germany-look-recent-reform, accessed 22 March 2018.

232 *Parliamentary Papers II* 2016/17, 34588, 3, p. 66-67.

233 Art. 33 para. 4 jo. art. 99 para. 1 Intelligence and Security Services Act 2017.

234 Art. 33 Intelligence and Security Service Act 2017.

235 *Parliamentary Papers II* 2017/18, 34862, 1, p. 2.

236 *Parliamentary Papers II* 2017/18, 34862, 1, p. 2.

237 https://www.vn.nl/de-geheimen-van-een-supertapper-2/; https://www.bof.nl/2018/01/23/de-spelregels-van-de-sleepwet-worden-nu-al-overtreden/, accessed 22 March 2018.

238 Art. 32 para. 2 Intelligence and Security Services Act 2017.

239 Art. 36 Intelligence and Security Services Act 2017.

240 Art. 37 Intelligence and Security Services Act 2017.

does satisfy the requirements of the ECtHR concerning independency and sufficient powers. A non-judicial Commission also has benefits. Powers that are applied towards foreign countries and non-Dutch citizens might fall outside the jurisdiction of the Dutch judge.[241] However, this application might fall within the mandate of a Commission. Secondly, this enables the appointment of members based on their technical expertise, which might be of more added value than having solely judges. This need for technical expertise in supervisory bodies to be able to adapt to contemporary circumstances is recognised by the European Union Agency for Fundamental Rights as well.[242] A lack of technical expertise has been feared by the Council of State, among others, since there is no codified requirement for a technical expert. To fill this gap a parliamentary amendment was filed to allow TIB members to consult external experts. However, this amendment was rejected.[243] With the acknowledgement of the importance of this expertise in the first formation process this might set the tone for the interpretation of the tasks of the third member being a technical expert, although this has to be proven in practice.

In *Zakharov* the ECtHR recognised that supervision exercised by a non-judicial organ can be compatible with the ECHR, provided that the oversight body is independent from the authorities carrying out the surveillance, and is equipped with sufficient powers and competence to exercise effective and continuous control.[244] A clear explanation of the assessment of independency by the Court has been given in *Campbell and Fell v UK.* Herein is stated that in determining the independency of a body, from the executive as well as from the parties to the case, the Court takes into account the manner of appointment of its members and the duration of their term of office, the existence of guarantees against outside pressures, and the question whether the body presents an appearance of independence.[245] Only a legal obligation addressing the institution to act independently and impartially is insufficient to pass this test. To meet the minimum standard, independency from the executive must be ensured functionally as well as institutionally.[246] Blending of functions within one office, where requests for interceptions are authorised as well as supervision of the implementation is taking place, may raise doubts.[247] The requirement of sufficient powers and competence can take many forms, but mostly refers to the oversight body's expertise, the ability to intervene at various stages in the surveillance process by issuing binding decisions, and its access to (classified) information concerning the activities of the services.[248] Examples are to be found in *Klass & others* and *Kennedy* where the supervisory body was able to stop the interception when found to be illegal or unnecessary, respectively to order to destroy the intercepted data when the interception was found to be unlawful.[249]

In the UK, as well as in The Netherlands, the ex-ante oversight body is newly introduced

241 *Parliamentary Papers II* 2016/17, 34588, 3, p. 67.

242 FRA, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Updates,* Luxembourg: Publications Office of the European Union 2017, p. 85.

243 *Parliamentary Papers II* 2016/17, 34588, 36.

244 ECtHR 4 December 2015 App No 74143/06 (*Roman Zakharov v Russia)*, para. 62 and 273.

245 ECtHR 28 June 1984 App No 7819/77 and 7878/77 (*Campbell and Fell v UK)*, para. 78.

246 ECtHR 28 June 1984 App No 7819/77 and 7878/77 (*Campbell and Fell v UK)*, para. 77.

247 ECtHR 4 December 2015 App No 74143/06 (*Roman Zakharov v Russia)*, para. 278.

248 FRA, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Updates,* Luxembourg: Publications Office of the European Union 2017, p. 75.

249 ECtHR 4 December 2015 App No 74143/06 (*Roman Zakharov v Russia)*, para. 281-282; ECtHR 6 September 1978 App No 5029/71 (*Klass & Others v UK)*, para. 53; ECtHR 18 May 2010 App No 26839/05 (*Kennedy v UK)*, para. 168.

by the current law reform, and tests the granted authorisation of the more intrusive bulk powers. The authorisation of the Minister regarding the application of such powers has to be approved by a Judicial Commissioner.[250] In Germany, the division is not made on the intrusiveness of the capability, but on the kind of communication collected by the applied power. In case of domestic and international communication it is the G10 Commission reviewing the authorisation, and in case of foreign communication it is the UG. The G10 Commission is a quasi-judicial body performing judicial oversight, and the UG is an administrative body performing restricted judicial oversight.[251]

During the application of powers and ex post, oversight is performed by the CTIVD, which already existed under the former Act. In the new Act this Review Committee will be divided in two departments. The department for oversight oversees the lawfulness of the execution of the powers based on the Act, and provides the Minister with information and advice. The other department investigates and assesses complaints and reports of abuses.[252] The Committee exists of four members, supported by a secretariat. Regarding appointment of the members, the same procedure applies as for appointing members of the TIB. Three members are appointed for the department for oversight, and one member for the department on the handling of complaints.[253]

To fulfill its tasks the CTIVD gets access to all information and cooperation they request, including classified information.[254] In contrast to the TIB, the CTIVD can consult external experts. In the context of the oversight task, the CTIVD can investigate the execution of powers based on the Act at their own initiative. The CTIVD writes monitoring reports on their findings which are publicly accessible as much as possible.[255] Only the department handling complaints is able to issue binding decisions.[256] The possibility to file a complaint is open for everybody, and if done correctly, the CTIVD is obliged to handle the complaint.[257] This probably leaves open the possibility for human rights advocates and NGOs to file complaints, as long as the complaint addresses conduct of one of the enumerated actors, regarding an individual or corporation. When the CTIVD finds unlawful conduct during the investigation of a complaint, it has the ability to stop an ongoing investigation, and/or the application of powers, and/or demand that acquired data will be destroyed.[258]

Ex-post oversight in the UK is performed by the Investigatory Powers Commissioner's Office (hereafter: IPC). The IPC consists in total of around 70 people, 15 Judicial Commissioners, (ex) High Court judges, Court of Appeal- and Supreme Court judges, a technical advisory panel and around 50 staff consisting of legal and technical expertise.[259] Like in the Dutch Act the IPC has to be provided with all the documents, information and

250 Artt. 108, 140, 159, 179, and 208 Investigatory Powers Act 2016.

251 https://www.lawfareblog.com/new-rules-sigint-collection-germany-look-recent-reform, accessed 22 March 2018.

252 Art. 97 Intelligence and Security Services Act 2017.

253 Art. 98 Intelligence and Security Services Act 2017.

254 Art. 107 Intelligence and Security Services Act 2017.

255 Artt. 112 and 113 Intelligence and Security Services 2017.

256 Art. 124 Intelligence and Security Services Act 2017.

257 Art. 114 Intelligence and Security Services Act 2017.

258 Art. 124 Intelligence and Security Services Act 2017.

259 FRA, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Updates,* Luxembourg: Publications Office of the European Union 2017, p. 67.

assistance they need to carry out their function.[260] Also, they can consult external experts for all the advice they need.[261] As opposed to The Netherlands, ex post oversight and complaints are divided over two different bodies in the UK. Complaints can be filed to the Investigatory Powers Tribunal (hereafter: IPT). Another difference with the Dutch Act is that the IPA 2016 gives the possibility to appeal the decision either at the Court of Appeal in England and Wales, or at the Court of Session in Scotland. The IPT is not a non-judicial body, but does not classify as an ordinary court either.[262] In Germany, the G10 Commission is the oversight body regarding the implementation of targeted surveillance and bulk powers within the G10 regime. Just like in The Netherlands and the UK, the law reform in Germany introduced a new oversight body as well. The UG is attributed with the control over the implementation of surveillance measures on foreign communication.[263]

Transparency, or public scrutiny in terms of the ECtHR, formed a recurring topic in the Internet consultations, especially regarding the authorisation and implementation of special powers. For example, the public availability of statistics on the amount of interception, or the allowing of telecommunication companies to publish transparency reports. The Dutch NGO Bits of Freedom started a court case against the refusal to publish relevantstatistics in an information request, leading to the result that the statistics will be published on an annual basis.[264] In this context it is interesting to consider that the ECtHR places emphasis on the public availability of the reports written by the oversight bodies.[265] The Wiv 2017 is providing for cited transparency: The Minister annually reports to the Parliament describing the focus of the investigations of the past and coming year. However, information on what powers were and will be applied in concrete matters, classified information about sources, and everything about the knowledge position of the services will be left out.[266] The CTIVD writes investigation reports on specific topics, and annually a general report on all of its tasks. However, the same limitations apply before publication, meaning all classified information must be left out.[267]

Under the IPA 2016 it is the IPC that provides for annual reports. The IPA 2016 contains requirements regarding the content of this report. The IPC is obliged to include: Statistics on the use of investigatory powers; information about the results or impact of such use; information about the operation of safeguards contained in the Act in relation to items subject to legal privilege, confidential journalistic material and sources of journalistic material; and information about the use of specific categories of warrant. The report will be laid before Parliament and will be publicly available, but only after it has been subject to redactions. In Germany, it is the G10 Commission that publishes reports that include numbers on the amount of individuals that are under surveillance.[268]

260 Section 235 IPA 2016.

261 FRA, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Updates*, Luxembourg: Publications Office of the European Union 2017, p. 67.

262 FRA, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Updates*, Luxembourg: Publications Office of the European Union 2017, p. 112.

263 Art. 16 Federal Intelligence Service Act.

264 https://www.rijksoverheid.nl/actueel/nieuws/2018/01/30/tapstatistieken-aivd-en-mivd-voortaan-openbaar, accessed 2 February 2018.

265 ECtHR 18 May 2010 App No 36839/05 (*Kennedy v UK)*, para. 166; ECtHR 12 January 2016 App No 37138/14 (*Szabó and Vissy v Hungary)*, para. 82; ECtHR 4 December 2015 App No 47143/06 (*Roman Zakharov v Russia)*, para. 281.

266 Art. 12 Intelligence and Security Services Act 2017.

267 Art. 113 para. 1 and art. 132 jo. art. 12 para. 3 Intelligence and Security Services Act 2017.

Supervision by Data Protection Authorities (hereafter: DPAs) is an essential component of the right to personal data protection, according to the CJEU.[269] However, since national security falls within the national sovereignty of the member states, there is no obligation to assign powers to the DPA within the field of intelligence and security services.[270] The Netherlands is one of 11 states in the EU which did not assign any powers over the intelligence services to its DPA.[271] In the Wiv 2017, general data protection legislation is explicitly not applicable to the conduct of the services, but is replaced by a general duty of care regarding the processing of data. This means that the services themselves will be reviewing their own data processing for appropriateness.[272] Within the Dutch debate several options were mentioned to include external oversight at this point. A parliamentary amendment proposing to lay down this task with the CTIVD was rejected.[273] The Privacy Impact Assessment performed on the Bill proposed to include measures of privacy by design and privacy by default.[274] However, the legislator did not deem this necessary, stating the Act contained other privacy safeguards already.[275]

The UK and Germany both did assign powers to their DPA, however limited. In the UK this comes down to a competence for the Information Commissioner Officer to control how data is retained, without having access to all of what is retained, since the services can rely on the exception of national security.[276] The control entails an assessment on compliance with data retention requirements in terms of integrity, security, or destruction of data by the services. In Germany the new law attributes the power to file non-binding complaints against intelligence services in case a data breach is detected. The Federal Commissioner for Data Protection and Freedom of Information is handling these complaints.[277]

268 FRA, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Updates*, Luxembourg: Publications Office of the European Union 2017, p. 88-89.

269 CJEU 8 April 2014 Joined cases C-293/12 and C-594/12 (*Digital Rights Ireland and Seitlinger)*, para. 68; CJEU 6 October 2015 C-362/14 (*Maximillian Schrems v Data Protection Commissioner)*, para. 41 and 66.

270 Art. 4 par. 2, par. 3 Treaty on the European Union.

271 FRA, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Updates*, Luxembourg: Publications Office of the European Union 2017, p. 56.

272 Art. 24 Intelligence and Security Services Act 2017.

273 *Parliamentary Papers II* 2016/17, 34588, 30, under I.

274 B. J. Koops e.a., *Privacy Impact Assessment on the Wiv 20xx*, TNO 12 February 2016, p. 142-144, <https://zoek.officielebekendmakingen.nl/blg-742355.pdf>.

275 *Parliamentary Papers II* 2016/17, 34588, 3, p. 48-49.

276 Section 28(1) Data Protection Act 1998.

277 Section 16(2) Federal Data Protection Act, enters into force 25 May 2018.

5. Conclusion: A critical contemplation of the Wiv 2017 in a broader international perspective.

Comprehensively considering the reforms of the laws on intelligence services in the Netherlands, the United Kingdom and Germany, it is possible to identify a general trend. All countries experience a development from capabilities with targeted effects to surveillance measures with untargeted effects, caused by the expansion of the collection of data from small scale to collection in bulk. Also, the cooperation between international services is intensified. The introduction of all these Acts has unchained a lot of societal debate, critique and legal challenges. Case-law on these new practices is continuing to grow and at this point we are waiting for some important decisions by high courts across Europe. It remains to be seen how these judgments will affect the legal framework on surveillance measures by intelligence services, while taking national security concerns into account. Furthermore, the societal debate these developments have unchained is interesting in itself. It seems unique that citizens get to have a say on the national security policies of their state, the conduct of their intelligence services, and secrecy in this respect. Personally, I am very happy to see the engagement of an increasing amount of people in this subject, caring for a national security policy that is taking their fundamental rights into account.

I found the differences between the Acts to be smaller than I expected at the start of this research project. The choice of Germany and the United Kingdom was partly based on their seemingly opposing images. However, after the research I do not think this image of opposites is justified. Still, there are definitely differences between all three of the Acts, and some aspects of the Wiv 2017 appeared remarkable when placed in an international context by this comparison:

- The Wiv 2017 does not make a difference between domestic, international and foreign communication data. In Germany as well as the UK this distinction is made. Germany even has different regimes according to this classification. However, this difference might be mostly de-jure, and it is a bit unclear what remains of it de-facto. The SRP calls it a “xenophobic fallacy” based on the idea that the threat is coming from the foreigners. Since the majority of terrorist attacks in Europe were carried out by EU citizens, I join the SRP in his opinion that it is a fallacy that it makes sense to discriminate against people whose citizenship lies not within the lawmakers’ jurisdiction.[278] Also, from case-law of the ECtHR it follows that infringements on the right to privacy that are made within the territory of a state fall within the jurisdiction of that state. Whether the individual whose rights are infringed upon is located within this territory as well is deemed irrelevant.

- The Wiv 2017 facilitates the sharing of data with foreign services in a far-reaching manner. These provisions are founded on the ‘*quid pro quo’* principle. In a comparative perspective the logic of these provisions is formulated in a sense that they appear to display a logic of ‘sharing, unless...’ by the Dutch Act as opposed to the logic of ‘only sharing if...’. Germany is one of the few EU member states that has implemented a relatively detailed procedural regulation on how to implement cooperative relationships in their primary legislation.

- Especially worrying regarding the international exchange of intelligence is the oversight gap. Data that is collected through bulk interception can be shared with foreign services before it is analysed by the Dutch services, even with services with whom the Dutch

278 HRC Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, *UN Doc*. A/HRC/34/60, 24 February 2017, p. 36.

services do not have a cooperative relationship. The ex-ante assessment on the authorisation of the Minister only accounts for the collection of the data, and its scope does not extend to the provision thereof to foreign services. Apart from that, the oversight of the CTIVD only applies to the conduct of the Dutch services. This means that there is no control nor oversight over data that is provided to foreign services, or over its use.

- The Wiv 2017 does not assign any power to the DPA. This is not a unique situation, since the Netherlands is one of the 11 states where the DPA does not have power over the intelligence services. The only safeguard in terms of data protection within the Dutch Act is the general duty of care of the services. In Germany as well as in the UK, the Acts do assign limited power to the DPA.

- Regarding the hacking capability, the expected differences between the countries are slightly visible. In comparison with the IPA 2016 it is noteworthy that the IPA 2016 gives examples of possible conduct under the hacking capability, where the Wiv 2017 provides for a limited enumeration of possible conduct. Also, the authorisation procedure within the IPA 2016 allows for all conduct that is necessary to do what is expressly mentioned in the warrant, and unforeseen conduct is assumed lawful. In the Wiv 2017, separate authorisation is required for all conduct. In this regard, the German Act is more limited regarding permitted conduct by describing only two forms. However, since this limitation of the capability is deemed technologically impossible, it is the question to what extent the total reach of the capability is more restricted.

- Noteworthy in regard of the hacking capability as well is the fact that the Wiv 2017 does not make a distinction between data in transmission and storage data. In the German Act two totally different capabilities address each type of data, and the IPA 2016 excludes data in transmission from the equipment interference warrant. In the Dutch Act, this distinction is not made, and conduct regarding both kinds of data is allowed and possible to combine within one authorisation.

- The capability to get real time access to databases is new in the Wiv 2017. The UK already has a practice in the acquirement of bulk personal datasets. The German Act does not account for this capability. The untargeted effect is mainly present within the acquisition of bulk data sets. In the IPA 2016 a distinction is made between warrants depending on the sensitivity of the nature of the data within the dataset. In case of sensitive data, a more strict regime applies. In the Netherlands, this distinction is made in practice and in internal rules, but it could be a valid suggestion to implement this in the Act. Remarkable about this capability as well is the classification as regular power instead of special power, like the other far-reaching surveillance measures with an untargeted effect within the Wiv 2017.

This leads to the conclusion that with the introduction of the Wiv 2017, the Netherlands places itself within the broader trend of the international development that is visible in the capabilities of intelligence services. Case-law of the ECtHR as well as the CJEU show that these Courts are taking a critical stance towards the shift from targeted to untargeted effects of surveillance measures as part of this development. Whether the criteria laid down in contemporary judgments also apply to the domain of intelligence and security services, in the light of the national security exception, is not clear yet. In this regard, we wait for the judgments in pending cases to be adjudicated. More specifically on the Wiv 2017, the legal battle is yet to come. As a broad coalition of IT-/tech-companies, lawyers, journalists and NGO’s have announced to start strategic litigation against the Act because of the untargeted effect of some of its surveillance measures, and the entry into force of the unchanged version of the Act before Parliament has agreed on the proposed

adjustments.[279]

In my opinion, it is a good thing that throughout several countries there are NGOs, activists, journalists, lawyers, and other people fighting this trend of wanting to collect more and more data. The 'security paradigm' appears to be very dominant. It seems that politicians want to show that they are taking the fear of citizens seriously, and that they are 'doing something'. However, we should be careful not to jump the gun. It is important to think rationally about what, and how urgent, these perceived threats are, and take appropriate measures. It is important as well to not forget what it is that needs protection.

The ECtHR acknowledges the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it.[280] Therefore, the introduction as well as the implementation of surveillance measures needs to be necessary, proportional, and subsidiary. In my opinion, this excludes surveillance powers with untargeted effects.

279 https://pilpnjcm.nl/dossiers/wet-op-de-inlichtingen-en-veiligheidsdiensten-wiv/, accessed 8 May 2018.

280 ECtHR 4 December 2015 App No 47143/06 (*Roman Zakharov v Russia*), para. 232.

6. Proposal for further research on the Wiv 2017.

6.1. Introduction/Inducement.

On the 1st of May 2018 the Intelligence and Security Services Act 2017 (hereafter: Wiv 2017) entered into force. The formulation of this Act unchained a lot of public debate. A record amount of reactions were filed in the Internet consultation, an online consultation round where citizens and legal persons can send in comments on the proposed Bill.[281] Five students from the University of Amsterdam took the initiative to start a referendum, which led to campaigns of several parties, fueling the debate. A broad coalition of IT-/tech-companies, lawyers, journalists and NGOs announced to lay the Act in front of the judge.

Main concern of the opponents of the Act is the untargeted effect of newly introduced surveillance measures. Untargeted effects come along with, for example, interception in bulk, whereby large amounts of data of people that are not targets are intercepted (as well). This will cause infringements upon fundamental rights of citizens that are not targets of the intelligence services. Critics argue that these measures do not meet the necessity requirement of the European Convention on Human Rights (hereafter: ECHR). Also, concerns are expressed about the "*chilling effect*" which might result from the application of such capabilities. This effect refers to the inhibition or discouragement of the legitimate exercise of certain fundamental rights these measures might have.

The Netherlands is by far not the only country that is modernising its intelligence law. Countries such as France, Germany, the United Kingdom and Finland are in the midst of overarching reforms as well.[282] The introduction of surveillance measures with an untargeted effect form an emerging trend within these law reforms. Argued necessity of these law reforms is of comparable nature, based on a combination of a perceived threat of terrorism and technological developments. This leads to the question to what extent society is willing to allow intelligence services to make infringements on fundamental rights to protect national security.

The Dutch Act and debate have the potential to function as an international model. Firstly, because the Dutch Act is part of this trend, and the Dutch debate is addressing this to a large extent. Secondly, because in the Netherlands an open debate is enabled by a sufficient level of free speech and transparency on the conduct of the Dutch intelligence services and government communication. Thirdly, the fact that the Act does not have one obvious flaw that is blocking a broader discussion makes it possible to have a well-informed debate on its content. And lastly, because of the referendum and the announced court case, the debate has been held throughout society, giving the topic momentum, causing more transparency and debate, and producing accessible information.

Unique about the Dutch situation is the extent of influence the debate has had on the formulation and development of the Act, giving citizens a voice in the national security policies of their country. The referendum resulted in a majority of voters taking position against the Act in its contemporary form. This led to a reaction of the Minister, announcing policy rules, safeguards regarding the practice of the intelligence services, points to address during the evaluation, and proposed adjustments to the Act. Although critics called the announced adjustments in the reaction 'cosmetic', the fact that the result led to adjustments shows the influence of a public debate on the process of this law reform.[283]

281 https://www.internetconsultatie.nl/wiv/details, accessed 14 May 2018.

282 FRA, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Updates*, Luxembourg: Publications Office of the European Union 2017, p. 9.

283 https://www.bof.nl/2018/04/12/kabinet-voert-sleepwet-per-1-mei-in/, accessed 10 May 2018.

It also means that although the Wiv 2017 entered into force, it will be an ongoing process. Apart from the Dutch law reform itself, the legal framework constructed of European case-law is not yet fully crystallised. Several cases on this subject are waiting to be adjudicated. The judgments following from these cases will be of particular relevance for the lawsuit on the Wiv 2017. Therefore I want to continue investigating the developments of the Dutch law reform within a European context.

6.2. State of the field.

As aforementioned, the Wiv 2017 entered into force on the 1st of May 2018. However, the Minister of Interior and Kingdom Relations Kajsa Ollongren send a letter containing the reaction to the result of the referendum. In this letter she announced three policy rules. The first policy rule concerns the drafting of the weighing notes on the foreign services with whom the Dutch services cooperate. The second policy rule is about the storage term of data acquired through bulk interception. The last policy rule addresses the application of special powers by the services. Furthermore, the letter contained safeguards regarding the practice of the intelligence services on bulk interception, the treatment of medical data and the protection of journalists. Lastly, the Minister addressed the continuation of the process.[284]

The Act will be evaluated after two years. On the basis of this evaluation, decisions will be made on adjusting the Act, adopting the policy rules into the primary legislation, and the Review Committee on the Intelligence and Security Services (hereafter: CTIVD) can suggest to adopt other adjustments. However, before adjustments can be made to the Act itself, the proposed changes have to pass through Parliament. During this process, Parliament can still make adjustments to the proposals.

Regarding the framework of European (case-)law, the European Court of Human Rights (hereafter: ECtHR) has already started handing down judgments that will establish a clear and binding framework on mostly targeted governmental surveillance.[285] Regarding surveillance measures with an untargeted effect several cases will be adjudicated in the coming years.[286]

The Court of Justice of the European Union (hereafter: CJEU) has created more detailed jurisprudence on surveillance since it struck down the Data Retention Directive which obliged communication service provides to undertake mass retention of their customer's metadata in 2014.[287] In 2016 the Court delivered the *Tele2 Sverige/Watson* judgment in which the Court iterated requirements regarding surveillance measures, based on EU legislation.[288] However, until now it remains unclear whether these requirements are applicable to the conduct of the intelligence services, seen in the light of the national security exception of article 4 Treaty on the European Union. This article states explicitly that national security remains the sole responsibility of each member state. It is precisely this question of applicability that is now laid in front of the Court in the form of a preliminary

284 *Parlementary Papers II* 2017/18, 34588, 70.

285 ECtHR 4 December 2015 App No 47143/06 (*Roman Zakharov v Russia*).

286 ECtHR App No 25252/08 (*Centrum För Rättvisa v Sweden)*; ECtHR App No 3599/10 (*Tretter and Others v Austria*); ECtHR *App* No 58170/13 (*Big Brother Watch and Others v UK)*; ECtHR App No 62322/14 (*Bureau of Investigative Journalism and Alice Ross v UK)*; ECtHR App No 24960/15 (*10 Human Rights Organizations and Others v UK)*, ECtHR App No 49526/15 (*Association Confraternelle de la Presse Judiciaire v France).*

287 CJEU 8 April 2014 Joined Cases C-293/12 and C-594/12, (*Digital Rights Ireland and Seitlinger).*

288 HRC Report of the Special Rapporteur on the right to Privacy Joseph A. Cannataci, *UN Doc*. A/HRC/34/60, p. 7, referring to: CJEU 21 December 2016 Joined Cases C-203/15 and C-698/15 (*Tele2 Sverige AB v Post-och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others).*

ruling.[289]

6.3. Research question and focus.

The aforementioned developments can be broadly divided into two tracks. The first track will be the Dutch developments regarding the Act and the debate. The second track will concern an analysis of the framework constructed from European (case-)law and developments at the level of the United Nations as far as these influence developments in Europe.

Regarding the first track I will closely follow the developments of the Act and the debate, starting from the day the Act entered into force. I choose this point because it is a clear demarcation Furthermore, this research can be interpreted as a continuation of the research of my thesis, which ends at that point. Of course, I will not leave it at a description of the developments, but also reflect on this development critically. The research on this track will be guided by the first subquestion: "*How is the Wiv 2017 developing after its entry into force?"*

This first chapter will be a descriptive overview of the public debate and the adjustments to the Act. This will be based on the proposed policy rules, the process in Parliament, the input of the evaluation, and possible the lawsuit of the PILP coalition. The goal of this chapter is to lay the necessary theoretical foundations and take the reader by the hand towards answering the research question.

In the second track, I will closely follow the developments of the framework constructed from European (case-)law on the subject and developments on the level of the United Nations as far as these influence developments in Europe. The research on this track will be guided by the second subquestion: "*What requirements are constructed in the European and international legal framework concerning state surveillance?"*

In the final section of the research I will bring the two tracks together. This enables me to place the Wiv 2017 within this European and international legal framework. In this final section I will explicitly address the main research question:

> *"To what extent does the Wiv 2017 meet the requirements as constructed in the European and international legal framework?"*

6.4. Methodology.

Since I am investigating different developments within my research I will make use of different research methodologies.

In the first track, on the development of the Wiv 2017 and the Dutch debate, I will conduct a document study. The formulation of the adjustments to the Act and the governmental communication on it will be laid down in Parliamentary Papers. In the document study I will focus on analyzing these documents. If necessary, I will request information through the Freedom of Information Act (*Wet Openbaarheid Bestuur).* I foresee this might be necessary regarding the documents of the evaluation.

The critical reflection on this process will be of an evaluative nature. This means that I will make an inventory on what changes will be made to the Act, and what the legislator is trying to achieve with these changes. Based on later documents on the functioning of the

289 CJEU *(*Reference for Preliminary Ruling) C-623/17 (*Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others)*.

Act I will evaluate to what extent the changes benefited the purpose.

In the second track I will conduct an investigation on the case-law of the regional, European Courts. I will analyze these judgments, and examine what they mean in the light of the already existing framework on the subject. Also, I will include documents from the level of the United Nations as far these influence the developments in Europe. This research will be of a more classical nature.

In interpreting all the data and placing it in the broader context of public debate I will conduct interviews with NGOs and experts in the field. I will be involved in the court case that lays the Act in front of the court. It is important to see the law in a broader social context. This enables a better understanding of developments in society and the manner in which these developments are reflected in the law.

6.5. Sources.

To do this research I will make use of several kinds of sources:

- Dutch law and secondary literature.
- All documents involved in the court case coordinated by the Public Interest Litigation Project (hereafter: PILP), especially the judgment and possible answer to preliminary questions. In this lawsuit, the judge will assess whether the Wiv 2017 is compliant with the European (case-)law, which is extremely relevant to my research.
- Parliamentary Papers regarding the adjustments that will be made to the Wiv 2017, the debates held in the Parliament, and governmental communication, will provide me with contextual governmental background information.
- I had personal contact with field experts of Bits of Freedom, Amnesty International, and the CTIVD. Also with Otto Volgenant, Fulco Blokhuis and Ron Lamme, the lawyers of Boekx law firm who will be representing the coalition in the court case. I am involved in the PILP myself, coordinating this case. In my research I will rely on the expertise of these parties.
- Documents on the evaluation of the Act. The evaluation will be expedited, and now will be held after two years. The evaluation will be an important moment of reflection and sharing of information. As aforementioned, this evaluation will be of great importance since it will be decided to adjust the Act or not, and in case of adjustment, in what manner. Also, the CTIVD will provide information on the functioning of the Act during the evaluation.
- Reports of the CTIVD. The CTIVD writes annual reports, providing information on their findings as an oversight body. These reports are crucial to my research, as the CTIVD is seen as an authoritative body regarding this Act and their findings will play an important role in the further development of it.
- Judgments of the ECtHR and CJEU will provide me with newly adjudicated case-law to construct the European aspect of the legal framework.
- Documents from the level of the United Nations as far as these influence developments in Europe.

6.6. Possible bottlenecks.

The first bottleneck in this research is inherent to studying a development that is happening at this very moment. It is yet unclear what turn events will take.

The second bottleneck is that the subject I will be investigating lies within the realm of national security. This means that a substantial amount of information will be classified,

and thus not accessible to me. I have to take this into account, especially in filing requests on the Freedom of Information Act. I can forestall this partly by filing this request as soon as possible, so it will not be problematic if it takes a lot of time before I receive the requested information. Also, I have to take into account that I have to object to the refusal of my request if necessary, and the amount of time this might take.

In case I do not get any information from the Freedom of Information Act request I will still be able to conduct the research, since the information that is of essential importance will be published in Parliamentary Papers.

7. Summary.

Surveillance activities using digital means have been rapidly growing and developing. Political developments started with the 'War on Terror' in the aftermath of the attack on the 11th of September 2001 in the United States. This led to new policies to fight perceived threats of terrorism and radicalisation.[290] Digital surveillance methods are increasingly used for this purpose.[291] These developments have triggered law reforms in the field of intelligence- and security services in many countries.[292]

The Snowden revelations of 2013 led to widespread criticism on the interferences with fundamental rights, made by the "mass-surveillance" projects the United States and several European countries participated in.[293] It is new and unique to have a debate on the secrecy of the work of the services. These developments taken together lead to the question how far states can go in their measures to protect their citizens and national security.

This question forms the decor of this research. More specifically, it focuses on the law reform in the Netherlands, introducing the Intelligence and Security Services Act 2017 ('*Wet op de Inlichtingen- en Veiligheidsdiensten 2017',* hereafter: Wiv 2017). This Act and the Dutch debate are exemplary of this development and therefore can function as a model. Firstly, because the arguments given for the need of this new law are the aforementioned perceived threats of terrorist attacks and the need for modernisation to keep up with the technological developments of society, more specifically in communications technology. Secondly, because the law reform unchained a discussion in Dutch society on the aforementioned question: To what extent are we willing to allow the services to make infringements on our fundamental rights in order to protect national security? Thirdly, because in the Netherlands an open debate is enabled by a sufficient level of free speech and transparency on the functioning of the Dutch services and government. Fourthly, it is possible to have a well-informed debate on the content of the law, since there is not one obvious flaw in the system which is blocking a broader discussion. And fifthly, because of a referendum started by five students from Amsterdam, the debate has been held throughout society, giving the topic momentum, causing more transparency and debate, producing publicly accessible information, and giving citizens a voice in the national security policies of their country.

The initiative to start a referendum with appurtenant campaigns, the announced court cases, and the lively debate about the Act show there is a lot of criticism on the expansion of powers of the intelligence services. The core of the criticism is directed at the untargeted effects of surveillance powers, and the perceived lack of safeguards to protect civilians against unlawful infringements on their rights. With the newly introduced bulk powers, large amounts of data of citizens that are not targets of the services will be gathered. Opponents state that the effectivity of bulk powers has not been proven, while the risks are occurrent. Data gathered by the government is not in the control of citizens anymore. Regimes can change, and in that case, so can the use of this data. Especially

290 A. Kundnani and B. Hayes, *The globalisation of CVE policy: Undermining human rights, instrumentalising civil society*, Amsterdam: Transnational Institute, 6 March 2018, p. 6.

291 FRA, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Updates*, Luxembourg: Publications Office of the European Union 2017, p. 17.

292 FRA, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Updates*, Luxembourg: Publications Office of the European Union 2017, p. 9.

293 https://www.theguardian.com/us-news/the-nsa-files. accessed 17 March 2018; HRC Report of the Special Rapporteur on the right to Privacy Joseph A. Cannataci, *Un Doc*. A/HRC/34/60, p. 6.

when unevaluated bulk data sets are provided to foreign services there is a lack of control. Also, governments get hacked, and data leaks occur. Apart from that, the bulk capabilities cause for a "*chilling effect";* the inhibition or discouragement of the legitimate exercise of certain fundamental rights these measures might have. This research addresses the capabilities in the law that are the most prominent within the debate. These are bulk interception, the hacking capability, real-time access to databases, the exchange of data with foreign services, and oversight and control mechanisms.

European law, including case-law, is providing the parameters within which the national law reforms can be formulated. The debates on the law reforms are being held against this background, and eventually it will be the judge who has the last verdict on the legality of the reforms. Therefore a sketch of the European case-law is included.

An emerging trend is visible regarding the law reforms on intelligence services in the Netherlands, the United Kingdom and Germany. It consists of a shift from surveillance measures with targeted effects to surveillance measures with untargeted effects, and an intensified international cooperation between the services. Also, all Acts unchained a lot of societal debate, critique and legal challenges.

I found the differences between the Acts to be smaller than I expected. However, some aspects of the Wiv 2017 appeared remarkable when placed in an international context:

- The Wiv 2017 does not make a difference between domestic, international and foreign communication data. In Germany as well as the UK this distinction is made. Germany even has different regimes according to this classification. However, this difference might be mostly de-jure, and it is a bit unclear what remains of it de-facto. The United Nations Special Rapporteur on the Right to Privacy (hereafter: SRP) calls it a "xenophobic fallacy" based on the idea that the threat is coming from the foreigners. Since the majority of terrorist attacks in Europe were carried out by EU citizens, I join the SRP in his opinion that it is a fallacy that it makes sense to discriminate against people whose citizenship lies not within the lawmakers' jurisdiction.[294]

- The Wiv 2017 displays a far-reaching willingness of the Dutch services to share data with foreign services. The logic of the provisions that determine in what cases data can be shared can be summarised as 'sharing, unless...' as opposed to the logic of 'only sharing if...'. Germany is one of the few EU member states that has implemented a relatively detailed procedural regulation on how to implement cooperative relationships in their primary legislation.

- Especially worrying, regarding the international exchange of intelligence, is the oversight gap. Data that is collected through bulk interception can be shared with foreign services before it is analysed by the Dutch services, even with services with whom the Dutch services do not have a cooperative relationship. The ex-ante assessment on the authorisation of the Minister only accounts for the collection of data, and its scope does not extend to the provision to foreign services. Apart from that, the oversight of the CTIVD only applies to the conduct of the Dutch services. This means that there is no control nor oversight over data that is provided to foreign services, or over its use.

- The Wiv 2017 does not assign any power to the DPA. The only safeguard in terms of data protection is the general duty of care of the services. In Germany as well as in the

294 HRC Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci, *UN Doc*. A/HRC/34/60, 24 February 2017, p. 36.

UK, the Acts do assign limited power to the DPA.

- Regarding the hacking capability the expected differences between the countries are slightly visible. In comparison, it is noteworthy that the IPA 2016 gives examples of possible conduct under the hacking capability, where the Wiv 2017 provides a limited enumeration of possible conduct. Also, the authorisation procedure within the IPA 2016 allows for all conduct necessary to do what is expressly mentioned in the warrant. Unforeseen conduct is assumed lawful. In the Wiv 2017, separate authorisation is required for all conduct. In this regard, the German Act is more limited regarding permitted conduct by describing only two forms. However, since this limitation of the capability is deemed technologically impossible, it is the question to what extent the total reach of the capability is more restricted.

- Noteworthy in regard of the hacking capability as well is the fact that the Wiv 2017 does not make a distinction between data in transmission and storage data. In the German Act two different capabilities address each type of data, and the IPA 2016 excludes data in transmission from the equipment interference warrant. In the Dutch Act, this distinction is not made, and conduct regarding both kinds of data is allowed and possibly combined.

- The capability to get real time access to databases is new in the Wiv 2017. The UK already has a practice in the acquirement of bulk personal datasets. The German Act does not account for this capability. The untargeted effect is mainly present within the acquisition of bulk data sets. In the IPA 2016, a distinction is made between warrants depending on the sensitivity of the nature of the data within the dataset. In case of sensitive data, a more strict regime applies. In the Netherlands, this distinction is made in practice and in internal rules, but it seems a valid suggestion to implement this in the Act. Remarkable about this capability as well is the classification as regular power instead of special power.

This leads to the conclusion that with the introduction of the Wiv 2017, the Netherlands places itself within the broader trend of the international development that is visible in the capabilities of intelligence services. Case-law of the ECtHR as well as the CJEU show that these Courts are taking a critical stance towards the shift from targeted to untargeted effects of surveillance measures. Whether the criteria laid down in contemporary judgments also apply to the domain of intelligence and security services, in the light of the national security exception, is not clear yet. In this regard, we wait for the judgments in pending cases to be adjudicated.

In my opinion, it is a good thing that throughout several countries there are NGOs, activists, journalists, lawyers, and other people fighting the trend of wanting to collect more and more data. The ‘security paradigm’ appears to be very dominant. It seems that politicians want to show that they are taking the fear of citizens seriously, and that they are ‘doing something’. However, we should not jump the gun. It is important to think rationally about what, and how urgent, these perceived threats are, and to take appropriate measures. It is important as well to not forget what it is that needs protection.

The ECtHR acknowledges the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it.[295] Therefore, the introduction as well as the implementation of surveillance measures needs to be necessary, proportional, and subsidiary. In my opinion, this excludes surveillance powers with untargeted effects.

295 ECtHR 4 December 2015 App No 47143/06 (*Roman Zakharov v Russia*), para 232.

References.

Literature and reports:

A. Kundnani and B. Hayes, *The globalisation of CVE policy: Undermining human rights, instrumentalising civil society,* Amsterdam: Transnational Institute, 6 March 2018.

A. Arnbak, 'Machtspositie Nederland drijfveer controversiële internettap: Referendum gaat over veel meer dan balans tussen terreurdreiging en privacy' in: *Het Financieele Dagblad* 25 January 2018.

B. J. Koops e.a., *Privacy Impact Assessment on the Wiv 20xx*, TNO 12 February 2016, <https://zoek.officielebekendmakingen.nl/blg-742355.pdf>.

Commissie Bestuurlijke Evaluatie Algemene Inlichtingen- en Veiligheidsdienst, *De AIVD in verandering,* November 2004, <https://www.aivd.nl/publicaties/publicaties/2004/11/16/de-aivd-in-verandering-rapport-commissie-bestuurlijke-evaluatie-over-functioneren-aivd>.

Council of Europe, *Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* Strasbourg 28 January 1981.

Council of Europe, *Democratic and effective oversight of national security services*, Strasbourg May 2015, <https://rm.coe.int/1680487770>.

Council of Europe Platform to Promote the Protection of Journalism and Safety of Journalists, *The Protection of Journalistic Sources, a Cornerstone of the Freedom of the Press,* May 2017, <https://rm.coe.int/factsheet-on-the-protection-of-journalistic-sources-may2017/16807178d7>.

CTIVD, *Toezichtsrapport over de inzet van de hackbevoegdheid door de AIVD en MIVD in 2015*, nr. 53, 25 April 2017.

CTIVD, *Toezichtsrapport over de invulling van samenwerkingscriteria door de AIVD en de MIVD,* nr. 48, 4 Mei 2016.

CTIVD, *Toezichtsrapport over de multilaterale gegevensuitwisseling door de AIVD over (vermeende) jihadisten*, nr. 56, 28 March 2018.

CTIVD, *Toezichtsrapport over het verwerven van door derden op internet aangeboden bulk data sets door de AIVD en de MIVD,* nr. 55, 28 December 2017.

D. Anderson, *Operational Case for Bulk Powers*, March 2016, <https://www.gov.uk/government/publications/investigatory-powers-bill-overarching-documents>.

D. Lyon, *Surveillance Studies: An Overview,* Cambridge: Polity Press 2007.

FRA, *Handbook on European Data Protection Law*, Luxembourg: Publications Office of the European Union 2014.

FRA, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Updates,* Luxembourg:

Publications Office of the European Union 2017.

G. Greenleaf, *Balancing globalisation's benefits and commitments: Accession to Data Protection Convention 108 by countries outside Europe,* Council of Europe Convention 108 Globalisation Conference, Strasbourg 17 June 2016.

G. Vermeulen and E. Lievers (eds.), 'Surveillance for public security purposes: Four pillars of acceptable interference with the fundamental right to privacy*',* in: *Data Protection and Privacy under Pressure: Transatlantic tensions, EU surveillance and big data,* Antwerp, Apeldoorn, Portland: Maklu 2017.

Home Office, *Equipment Interference DRAFT Code of Practice*, December 2017, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/668940/Draft_code_-_Equipment_Interference.pdf>.

Home Office, *Investigatory Powers Act 2016: Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data,* November 2017 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/663668/November_2017_IPA_Consultation_-_consultation_document.pdf>.

HRC Report of the Special Rapporteur on the right to Privacy Joseph A. Cannataci, *Un Doc*. A/HRC/34/60.

HRC Report of the Special Rapporteur on the right to Privacy Joseph A. Cannataci, *UN Doc*. A/HRC/37/62.

J. Polakiewicz, *Convention 108 as a global privacy standard?* Budapest: 17 June 2011.

M. Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance,* Oxford and Portland: Oregon 2017.

N. A. N. M. van Eijk and C. M. J. Ryngaert, 'Deskundigenbericht: Juridische grondslag multilaterale informatie-uitwisseling', bijlage IV in: CTIVD, *Toezichtsrapport over de multilaterale gegevensuitwisseling door de AIVD over (vermeende) jihadisten*, nr. 56, 28 March 2018.

NJCM, Reactie op concept-wetsvoorstel, Leiden: 31 August 2015 <https://njcm.nl/wp-content/uploads/2016/12/Reactie-consultatie-WIV-NJCM.pdf>

Privacy International, *Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards,* April 2018 <https://privacyintyqcroe.onion/sites/default/files/2018-04/Secret%20Global%20Surveillance%20Networks%20report%20web%20(200).pdf>.

Q. Eijkman, N. A. N. M. van Eijk and R. van Schaik, *Dutch National Security Reform under Review: Sufficient Checks and Balances in the Intelligence and Security Services Act 2017?,* University of Amsterdam: Amsterdam/Utrecht March 2018.

Resolution 69/166 of the General Assembly of the United Nations (18 December 2014), *The right to privacy in the digital age* UN Doc. A/RES/69/166.

S. J. Eskens, ‘Ongerichte interceptie, of het verwerven van bulk-communicatie, en waarom de Grondwet en het EVRM onvoldoende tegenwicht bieden’, in: *Computerrecht*, nr. 3, p. 125-131.

VVD, CDA, D66 en ChristenUnie, *Vertrouwen in de toekomst, regeerakkoord 2017-2021,* 10 Oktober 2017.

Case-law:

CJEU 8 April 2014 Joined Cases C-293/12 and C-594/12 (*Digital Rights Ireland and Seitlinger).*
CJEU 6 October 2015 C-362/14 *(Maximillian Schrems v Data Protection Commissioner).*
CJEU 21 December 2016 Joined Cases C-203/15 and C-698/15 *(Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others).*
CJEU (Reference for Preliminary Ruling) C-623/17 *(Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others).*

ECtHR 6 September 1978 App No 5029/71 *(Klass and Others v UK).*
ECtHR 2 August 1984 App No 8691/79 *(Malone v UK).*
ECtHR 29 June 2006 App No 54934/00 *(Weber and Saravia).*
ECtHR 22 November 2007 App No 64752/01 *(Voskuil v The Netherlands).*
ECtHR 1 July 2008 App No 58243/00 *(Liberty and Others v UK).*
ECtHR 4 December 2008 App No 30562/04 and 30566/04 *(S and Marper v UK).*
ECtHR 4 May 2010 App No 28341/95 *(Rotaru v Romania).*
ECtHR 18 May 2010 App No 26839/05 (*Kennedy v UK*).
ECtHR 2 September 2010 App No 35623/05 *(Uzun v Germany).*
ECtHR 14 September 2010 App No 38224/03 *(Sanoma v The Netherlands).*
ECtHR 13 November 2012 App No 24029/07 *(M. M. v UK).*
ECtHR 22 November 2012 App No 39315/06 *(Telegraaf v The Netherlands).*
ECtHR 4 December 2015 App No 47143/06 *(Roman Zakharov v Russia).*
ECtHR 19 June 2018 App No 25252/08 *(Centrum För Rättvisa v Sweden).*
ECtHR App No 3599/10 *(Tretter and Others v Austria).*
ECtHR App No 58170/13 *(Big Brother Watch and Others v UK).*
ECtHR App No 62322/14 *(Bureau of Investigative Journalism and Alice Ross v UK).*
ECtHR App No 24960/15 *(10 Human Rights Organizations and Others v UK).*
ECtHR App No 49526/15 *(Association Confraternelle de la Presse Judiciaire v France).*

IPT 5 December 2014 IPT/13/77/H *(Liberty & Others v GCHQ & Others).*

Online references:

https://beta.volkskrant.nl/nieuws-achtergrond/somali-victims-of-us-drone-strike-take-legal-action-against-the-netherlands~bb62e8d8/.

https://www.ams-ix.net/connect-to-ams-ix/benefits-of-connecting.

https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/QuellentkueOnlinedurchsuchung/quellentkueOnlinedurchsuchung_node.html.

https://www.bof.nl/2018/04/12/kabinet-voert-sleepwet-per-1-mei-in/.

https://www.bof.nl/2018/01/23/de-spelregels-van-de-sleepwet-worden-nu-al-overtreden/.

https://www.cnet.com/news/doomsday-worm-eternalrocks-seven-nsa-exploits-wannacry-ransomware/.

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures

https://www.coe.int/en/web/data-protection/convention108/modernisation.

http://www.ec.europa.eu/growth/tools-databases/tris/en/search/trisaction=search.detail&year=2016&num=188.

https://www.internetconsultatie.nl/wiv/details.

https://www.juris.de/jportal/portal/page/homerl.psml?nid=jnachr-JUNA171206018&cmsuri=%2Fjuris%2Fde%2Fnachrichten%2Fzeigenachricht.jsp.

https://lawfareblog.com/new-rules-sigint-collection-germany-look-recent-reform.

https://www.liberty-human-rights.org.uk/news/press-releases-and-statements/people-vs-snoopers%E2%80%99-charter-liberty-launches-crowdfunded-legal.

https://www.netzpolitik.org/2014/geheimes-dokument-bundeskriminalamt-darf-finfisherfinspy-nicht-einsetzen-versucht-einfach-neue-version-nochmal.

https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/#Sachstandsbericht

https://www.nos.nl/artikel/2100411-plasterk-denkt-na-over-aftappen-chat-apps-en-wifi-hotspots.html.

https://www.nsa.gov/what-we-do/signals-intelligence/.

https://www.pilpnjcm.nl/dossiers/wet-op-de-inlichtingen-en-veiligheidsdiensten-wiv/.

https://www.rijksoverheid.nl/actueel/nieuws/2018/01/30/tapstatistieken-aivd-en-mivd-voortaan-openbaar, accessed 02/02/2018.

https://rsf.org/en/news/bnd-law-german-bundestag-ignores-criticism-civil-society-and-breaches-constitution.

https://www.rsf.org/en/news/germany-landmark-ruling-against-bnd.

https://www.rtlnieuws.nl/buitenland/computerstoringen-in-britse-ziekenhuizen-door-cyberaanval.

https://www.rtlnieuws.nl/nederland/parkeergarages-in-nederland-getroffen-door-wereldwijde-cyberaanval.

https://www.soundcloud.com/volkskrantgeluid/sleepwetpodcast1?in=volkskrantgeluid/sets/special-de-sleepwet.

https://www.stern.de/digital/online/projekt-des-bnd-ueberwachung-von-facebook-und-co—kein-grundrechtseingriff-3944568.html.

https://www.theguardian.com/us-news/the-nsa-files.

https://www.theguardian.com/uk-news/2018/jan/30/uk-mass-digital-surveillance-regime-ruled-unlawful-appeal-ruling-snoopers-charter.

https://www.vn.nl/de-geheimen-van-een-supertapper-2/.