Report of Various Size

Monthly data collection on the current reform of intelligence legislation

Country: the Netherlands

Contractor's name: Art.1, Dutch knowledge centre on discrimination

Author(s) name: Eddie Nieuwenhuizen, Gregor Walz

Reviewed by: Ashley Terlouw, Jacky Nieuwboer

Period covered: December 2016 - June 2017

1. **Legislative reform(s)**
(Please, highlight the key aspect(s) of the reform, summarise any key report published in the context of the reform procedure)

On 28 October 2016[1] the government sent the bill for the Act on the Intelligence and Security Services 20.. (*Wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20..*) to the House of Representatives (*Tweede Kamer der Staten-Generaal*). [2] This bill amends the act that lays down the authorities of the General Intelligence and Security Service (*Algemene Inlichtingen en Veiligheidsdienst* or AIVD) and the Military Intelligence and Security Service *(Militaire Inlichtingen- en Veiligheidsdienst* or MIVD). The draft bill extends the powers of the services to intercept internet traffic and email and phone communications while at the same time providing additional requirements to guarantee the privacy of citizens. On 15 December 2016 the standing committee on the Interior of the House of Representatives held a round table conference at which stakeholders (oversight bodies, non-governmental organisations, companies and academia) could express theirs views on the bill. Some of these stakeholders wrote position papers for this round table conference. We have made summaries of these papers under the relevant headings below. The representative of the Dutch Data Protection Authority criticized the plans of the government for a dragnet, the hacking by third parties and the sharing of information with foreign services. He called the use of the term "investigation mandated interception" (*onderzoeksopdrachtgerichte interceptive*) for a drag net the "understatement of the year".

In response to this round table conference the House of Representatives has compiled a memorandum of 51 pages in which a number of questions was submitted to the Minister of Interior and Kingdom relations.[3] Many questions targeted the unfocused nature of the dragnet (including what is meant by the 'mandate to investigate' (*onderzoeksopdracht*), the nature and number of data which can be intercepted under the new act and the way data limitation will take place), the relevance and storage limit of the data collected under the new act, the quality of the data analysis and the supervision of the intelligence services. In response to these questions, the Minister of the Interior and Kingdom Relations sent a memorandum of 110 pages answering these questions to the House on 17 January 2017.[4] The watchdog Bits of Freedom noted that this memorandum by the minister makes no contribution in clarifying matters. [5]

---

[1] The Netherlands, National Government (*Rijksoverheid*) (2016),'Gemoderniseerde Wet op de inlichtingen- en veiligheidsdiensten: extra bescherming veiligheid én privacy', Press Release 28 October 2016, available at: www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2016/10/28/voorstel-van-wet-inzake-wijziging-wet-op-de-inlichtingen-en-veiligheidsdienten/voorstel-van-wet-inzake-wijziging-wet-op-de-inlichtingen-en-veiligheidsdienten.pdf

[2] The Netherlands, Prime Minister, Minister of General Affairs / Minister of the Interior and Kingdom Relations / Minister of Defence / Minister Security and Justice (*Minister-President / Minister van Algemene Zaken / Minister van Binnenlandse Zaken en Koninkrijksrelaties / Minister van Defensie*) (2016), Act on the Intelligence and Security Services 20...Bill (Wet op de inlichtingen- en veiligheidsdiensten 20..), available at: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2016/10/28/voorstel-van-wet-inzake-wijziging-wet-op-de-inlichtingen-en-veiligheidsdienten/voorstel-van-wet-inzake-wijziging-wet-op-de-inlichtingen-en-veiligheidsdienten.pdf

[3] The Netherlands, House of Representatives (*Tweede Kamer der Staten-Generaal*), ' Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- enveiligheidsdiensten 20..). Verslag Vastgesteld 30 december 2016, Parliamentary Document 34 588 No. 7, available at:https://www.tweedekamer.nl/kamerstukken/detail?id=2016D51342

[4] The Netherlands, Minister of Interior and Kingdom relations (*Minister of Interior and Kingdom relations*) (2017), Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..), Nota naar aanleiding van het verslag, Parliamentary Document 34 588 No. 18, available at https://www.tweedekamer.nl/downloads/document?id=360ec11d-1a61-44b9-8c6f-d8a90b3dc249&title=Nota%20naar%20aanleiding%20van%20het%20verslag.pdf

[5] De Zwart, H. (2017), 'Kabinet dendert door richting sleepnet', Web page, 21 January 2017, Bits of Freedom, available at: https://www.bof.nl/2017/01/21/kabinet-dendert-door-richting-sleepnet/

Several amendments to the bill were submitted by members of the House of Representatives. [6] Most of these amendments were informed by the recommendations made by the Review Committee for the Intelligence and Security Services (CTIVD) in an advisory report sent to the House of Representatives on 9 November 2016. [7] These amendments aim to achieve a better protection of privacy. On 17 January 2017 the Minister of Interior and Kingdom Relations published a memorandum containing a series of amendments to the bill. [8] The only actor or body which has given a reaction to these amendment is the Review Committee for the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten or CTIVD*).[9] As reported in the Dutch contribution to the FRA Fundamental Rights Report, CTIVD has published its view on the original bill in November 2016 (an English translation of this view was published in December 2016). [10] The CITVD approves of the amendments concerning the introduction of a duty of care for the quality of the processing of data, and the introduction of additional safeguards concerning cases in which the Dutch intelligence services cooperate with foreign services.

The duty of care as formulated by the bill implies that the heads of the two services should ensure the necessary provisions to promote the accuracy and completeness of the processed data and to promote the quality of the data processing, including the used algorithms and models. In the explanatory memorandum to the amendment the minister indicates that there is a sufficient assessment framework for the CTIVD to assess the data processing including the use of algorithms and models. The CTIVD is of a different opinion and criticises this lack of such a framework.

The additional safeguards concerning cases in which the Dutch intelligence services cooperate with foreign services are twofold: firstly, for any sharing of data with foreign services the head of one of the Dutch intelligence services has to request an authorisation by the minister and secondly any authorisation to share unassessed data intercepted by an investigation mandate (the so called dragnet) should be notified to the Review Committee for the Intelligence and Security Services or CTIVD.

At the same time the CTIVD still has a lot criticism (it deplores the lack of clear, verifiable standards and *the lack of clear and verifiable* restrictions for the use of a number of powers) and provides a number of recommendations for further amendments to the bill. The CTIVD is of the opinion that the bill places to much emphasis on traditional safeguards to restrict the use of powers by the intelligence services, such as prior authorisation (Minister) and assessment of the use of the powers (Assessment Committee on the Use of Powers or TIB)). Such traditional safeguards alone are no longer sufficient,

---

[6] The Netherlands, House of Representatives (*Tweede Kamer der Staten-Generaal*), 'Wetsvoorstel 34588 Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..)', Website, available at: https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?qry=%2A&fld_tk_categorie=Kamerstukken&Type=Gerelateerd&dpp=99&clusterName=Gerelateerde+documenten&fldnot_prl_nummer=2016Z19831&fld_prl_dossiernummer=34588&dossier=34588&id=2016Z19831&srt=date%3Adesc%3Adate

[7] The Netherlands, Review Committee for the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten*) (2016), *Zienswijze van de CTIVD. Op het wetsvoorstel Wiv 20..*, The Hague, Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, available at: www.ctivd.nl/documenten/publicaties/2016/11/09/zienswijze

[8] The Netherlands, Minister of Interior and Kingdom relations (*Minister of Interior and Kingdom relations*) (2017), *Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..), Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..). Nota van wijziging*, Parliamentary Document 34 588 No. 19, available at https://www.tweedekamer.nl/downloads/document?id=509eefd9-d7ff-4cdd-9c13-27118d6afe7d&title=Nota%20van%20wijziging.pdf

[9] The Netherlands, Review Committee for the Intelligence and Security Services (*Commissie van Toezicht op de nlichtingen- en Veiligheidsdiensten*) (2017), Standpunt CITVD, *Wetsvoorstel Wiv 20.. - vervolg op de Zienswijze februari 2017*, The Hague, Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, available at: https://www.ctivd.nl/documenten/publicaties/2017/01/31/index

[10] The Netherlands, Review Committee for the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten*) (2016), *The CTIVD's View. On the ISS Act 20.. Bill, The Hague, Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten*, available at: https://english.ctivd.nl/binaries/ctivd-eng/documents/publications/2016/12/07/index/CTIVD+The+CTIVD%27s+View.pdf

especially for the collection and further processing of large amounts of data (bulk data). The CTIVD has no access to all data and cannot review whether the two intelligence services use their powers in a legal manner. We have summarised these recommendations below under heading 2. All of these recommendation were also given by the CTIVD in its view on the original bill.

A plenary debate of the House Representatives on the bill was planned in week 6 of 2017, probably on 8 February 2016. In the end, the debate took place on 8 February 2017. During the debate it turned out that a majority of the House of Representatives supports the bill.[11] The vote on the bill will take place on 14 February 2017. . The watchdog Privacy Barometer has called on the House of Representatives not to vote on the bill before the elections because of the number of inadequacies in the bill and the criticism voiced against the bill by several bodies.[12] The watchdogs Bits of Freedom, Free Press Unlimited and Internet Society Nederland have started a campaign with a special website to put pressure on members of the House of Representatives to remove the dragnet from the bill. [13]

Update March 2017

On 8 February 2017 the House of Representatives debated the bill for the Act on the Intelligence and Security Services 20.. (*Wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20..*). On 14 February 2017 the House of Representatives (*Tweede Kamer der Staten-Generaal*) passed the bill. 113 members voted in favour of the bill, 37 members voted against the bill.[14]
Before passing the bill the House of Representative voted in favour of three amendments to the bill: two amendments submitted by member of parliament (MP) Verhoeven and one amendment submitted by MP Voortman. One amendment by MP Verhoeven aimed to clarify the legal limits to the obligation for third parties to cooperate with the decryption of data.[15] This amendment clarifies that third parties will never be obliged to weaken the encryption in their systems. The other amendment by Member Verhoeven enables citizens to apply for notice of personal data processed by the intelligence services digitally.[16] In the original bill such a request could only be done in writing by post. The amendment by MP Voortman stipulates that foreign intelligence services may not collect data in the Netherlanders on their own initiative.[17]
The bill will now be debated by the Senate (*Eerste Kamer der Staten-Generaal*). If the political parties in the Senate will vote the same way they have done in the House of Representatives the bill will pass with a clear majority.

---

[11] Siedsma, T. (2017), 'Het sleepnetdebat dat sleepnet gaat er komen'. 9 February 2017, Website Bits of Freedom, available at:nhttps://www.bof.nl/2017/02/09/het-sleepnetdebat-dat-sleepnet-gaat-er-komen/
[12] De Zwart, H. (2017), 'Kabinet dendert door richting sleepnet', Web page, 21 January 2017, Bits of Freedom, available at: https://www.bof.nl/2017/01/21/kabinet-dendert-door-richting-sleepnet/
[13] Bits of Freedom, Free Press Unlimited & Internet Society Nederland (2017), 'Geensleepnet', Website, available at: https://geensleep.net/
[14] The Netherlands, House of Representatives (*Tweede Kamer der Staten-Generaal*) (2017). Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (*Wet op de inlichtingen- en veiligheidsdiensten 20..).Plenaire vergadering 14 februari 2017*, Stemmingsuitslagen, available at: https://www.tweedekamer.nl/kamerstukken/stemmingsuitslagen/detail?id=2017P02011
[15] The Netherlands, House of Representatives (*Tweede Kamer der Staten-Generaal*) (2016). Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (*Wet op de inlichtingen- en veiligheidsdiensten 20..).* Amendement lid Verhoeven, Parliamentary Document (*Kamerstuk*) 34 588 No.13, available at: https://zoek.officielebekendmakingen.nl/kst-34588-13.pdf
[16] The Netherlands, House of Representatives (*Tweede Kamer der Staten-Generaal*) (2017). Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (*Wet op de inlichtingen- en veiligheidsdiensten 20..).* Amendement lid Verhoeven, Parliamentary Document (*Kamerstuk*) 34 588 No.29, available at: https://zoek.officielebekendmakingen.nl/kst-34588-29.pdf
[17] The Netherlands, House of Representatives (*Tweede Kamer der Staten-Generaal*) (2017). Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (*Wet op de inlichtingen- en veiligheidsdiensten 20..).* Amendement lid Voortman, Parliamentary Document (*Kamerstuk*) 34 588 No.31, available at: https://zoek.officielebekendmakingen.nl/kst-34588-31.pdf

The bill as it stand now is under review of the Senate (*Eerste Kamer der Staten-Generaal*). [18] On 4 April 2017 the bill will be debated by a committee of the Senate.[19] This committee decides whether the bill can immediately be put on the agenda of the full Senate or whether there should first be a preparatory study of the bill. If a bill is immediately put on the agenda of the full Senate, it will be passed as a formality without a debate. The preparatory study of a bill consists mainly of written correspondence and the exchange of documents.

The bill will replace the current Intelligence and Security Services Act 2002.[20] This act lays down the authorities of the General Intelligence and Security Service (*Algemene Inlichtingen en Veiligheidsdienst* or AIVD) and the Military Intelligence and Security Service (*Militaire Inlichtingen- en Veiligheidsdienst* or MIVD). It dates from 2002 and has been amended several times but was deemed not to be up to date anymore. One underlying reason for the need of a replacement bill is the increase of internet traffic since 2002.

The official goal of this bill is to extend the powers of the two services to intercept internet traffic and email and phone communications while at the same time providing additional requirements to guarantee the privacy of citizens. The bill has 172 articles and is 67 pages long. Below we will discuss the bill considering the surveillance techniques it offers to the intelligence service, the system of authorisations concerning these techniques and the assessment in advance, and the system of review and complaints handling afterwards. We focus on the use of surveillance techniques and not on the more traditional investigation techniques used by intelligence services like opening letters without the consent of the sender or the addressee.

The bill for the Act on the Intelligence and Security Services 20… [21] permits the two intelligence services to use several surveillance techniques.

- Article 45 of the bill permits the intelligence services to hack computers and other devices.
- Article 47 enables the services to tap, receive, record and monitor any form of conversation, telecommunication or data transfer by means of an automated work in a targeted manner. This article applies to the interception targeting a specific person or organisation.
- Article 48 of the bill enables the services to perform an "investigation-mandated interception" ("*onderzoeksopdrachtgericht interceptie*") of data.

Interception is defined in this article as follows: with the aid of a technical device, to tap, receive, record and monitor in a targeted manner any form of telecommunication or data transfer by means of an automated work, irrespective of where this takes place. This includes the power to undo the encryption of the conversations, telecommunication or data transfer. The explanatory memorandum to the bill [22] states that investigation-mandated interception of data will target certain geographical areas

---

[18] The Netherlands, Prime Minister, Minister of General Affairs / Minister of the Interior and Kingdom Relations / Minister of Defence / Minister Security and Justice (Minister-President / Minister van Algemene Zaken / Minister van Binnenlandse Zaken en Koninkrijksrelaties / Minister van Defensie) (2016), Act on the Intelligence and Security Services 20...Draft (Wet op de inlichtingen- en veiligheidsdiensten 20..), Bill as amended on 14 February 2017, available at: https://www.eerstekamer.nl/9370000/1/j9vvhwtbnzpbzzc/vkbsm1saavz3/f=y.pdf

[20] The Netherlands, Intelligence and Security Services Act 2002 (*Wet op de inlichtingen- en veiligheidsdiensten 2002*), 7 February 2002, available at: http://wetten.overheid.nl/BWBR0013409/2017-03-01 ; unofficial English translation available at: https://cyberwar.nl/d/wiv2002en.pdf

[21] The Netherlands, Prime Minister, Minister of General Affairs / Minister of the Interior and Kingdom Relations / Minister of Defence / Minister Security and Justice (*Minister-President / Minister van Algemene Zaken / Minister van Binnenlandse Zaken en Koninkrijksrelaties / Minister van Defensie*) (2017), Act on the Intelligence and Security Services 20...Draft (*Wet op de inlichtingen- en veiligheidsdiensten 20..)*, Bill as amended on 14 February 2017, available at: https://www.eerstekamer.nl/9370000/1/j9vvhwtbnzpbzzc/vkbsm1saavz3/f=y.pdf

[22] The Netherlands, Prime Minister, Minister of General Affairs / Minister of the Interior and Kingdom Relations / Minister of Defence / Minister Security and Justice (*Minister-President / Minister van Algemene Zaken / Minister van Binnenlandse Zaken en Koninkrijksrelaties / Minister van Defensie*) (2017), Act on the Intelligence and Security Services 20...Draft (Wet op de inlichtingen- en veiligheidsdiensten 20..), Explanatory Memorandum, available at: https://zoek.officielebekendmakingen.nl/kst-25877-3.pdf

and certain data streams. At the same time, the explanatory memorandum to the bill states that investigation-mandated interception does not cover the example of the collection of all bulk data for all communications in a certain city for a month and the subsequent assessment whether any relevant data have been collected. The bill and the explanatory memorandum offer no further indications of how an investigation-mandated interception of the data will be performed. The term "investigation-mandated interception" has been dubbed by critics of the current bill "a dragnet" because it authorizes the services to intercept bulk data without any direction or target ("*richting"*).

The following articles provide further details of the powers of the services:

- Article 49 permits both services to use the data collected in accordance with article 48 to investigate the characteristics and nature of the data and to establish the identity of the person or organization associated with the data collected.
- Article 50 permits both services to select the data collected under Article 48 and the use of automated data analysis (provided for in Article 60) with regard to the data collected under Article 48.
- Article 64 permits the two services to share collected data with foreign services.
- Article 89 permits the two service to collect data at request of a foreign service.
- Articles 52 and 53 permits the services to demand the cooperation with the collection of data taking place under articles of 47 and 48 of the bill from providers of communication services. Providers may not refuse such a demand.
- Articles 54, 55 and 56 permits the services to request access to stored data of users and about users from providers of communication services.
- Article 57 enables the services to demand the cooperation with the decryption of data from providers of communication services. Again, providers may not refuse such a demand.

The system of authorisation and assessment in advance, and review and complaints handling afterwards as enshrined in the bill is stratified and complex. For the exercise of powers defined in articles 45, 47, 48, 49, 50, 53, 54, 55, 56, 57, 64 and 89 the intelligence services need the prior authorisation of their minister: in the case of the General Intelligence and Security Service (*Algemene Inlichtingen en Veiligheidsdienst* or AIVD) the prior authorisation of the Minister of Interior and Kingdom Relations is required and in the case of the Military Intelligence and Security Service (*Militaire Inlichtingen- en Veiligheidsdienst* or MIVD) the prior authorisation of the Minister of Defence is required.

Furthermore, the prior authorisations of the two Ministers for the use of powers by the two services as stipulated by articles 45, 47, 48, 49, 54 and 57 of the bill, have to be assessed by a special committee: the *Toetsingscommissie Inzet Bevoegdheden* or TIB, the Assessment Committee on the Use of Powers. The TIB consists of three members. Two members have to be former judges. The TIB will assess whether the prior authorisation granted by the minister is legal (*rechtmatig*). According to article 33 of the bill, the decisions by the TIB are binding.

Article 97 of the bill foresees in a Review Committee for the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten* or CTIVD). The CTIVD already exists but will be split into two separate departments or sub-committees by the bill: a sub-committee which performs a general oversight task by performing investigations and a sub-committee which handles complaints and reports about any suspicion of wrongdoing. The sub-committee which performs the general oversight task consists of three members. It performs its task by reviewing at a regular basis the operations of both intelligence services by investigating whether their operations or actions are in accordance with the existing legal framework for the services. These reviews will be published in special reports which will be made public. The reports contain recommendations. These reports or recommendations are not binding. The sub-committee issues reports on its own initiative or at the request of both houses of parliament (House of Representatives and Senate).

The sub-committee which handles complaints and reports about any suspicion of wrongdoing consists of three members. Article 114 of the bill entitles every person to lodge a specific complaint with the sub-committee on the actions or the alleged actions of persons working for the intelligence services in the implementation of the Act on the Intelligence and Security Services 20… Article 126 of the bill entitles every person to file a general report of any suspicion of wrongdoing by persons working for the intelligence in the implementation of the Act on the Intelligence and Security Services 20.. Article 118 of the bill stipulates that when a person disagrees with a decision by the sub-committee of the CTIVD which handles complaints he or she can make use of the objection procedure as enshrined in title 7 of the General Administrative Law Act (*Algemene Wet Bestuursrecht*). [23]

Finally, article 59 of the bill stipulates the duty to disclosure of the use of three special powers of the service: the power defined in article 44 (opening letters and other consignments without the consent of the sender or the addressee), article 47 (tapping, but only in so far as there was an intrusion) and article 58 (to have access to places or intrusion). Five years after these powers have been exercised and subsequently once every year, the relevant Minister will examine whether a report of the events can be submitted to the person with regard to whom one of these special powers has been exercised.

Update June 2017

On 14 February 2017 the House of Representatives (*Tweede Kamer der Staten-Generaal*) passed the bill for the Act on the Intelligence and Security Services 20.. (*Wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20..*). [24] The bill is under review of the Senate (*Eerste Kamer der Staten-Generaal*). If the political parties in the Senate vote the same way they have done in the House of Representatives the bill will pass with a clear majority. The Senate can only reject or pass a bill, but cannot change it.

On 22 March 2017 the Review Committee for the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten* or CTIVD) sent a letter to the Senate in which it gives its view on the bill.[25] This letter was sent in preparation to a meeting between the CTIVD and members of the Senate which took place on 28 March 2017. The letter follows up on a letter sent by the CTIVD to the House of Representatives and Senate on 9 November 2016[26] and a letter sent to the House of Representatives on 30 January 2017.[27] In the letter of 22 March 2017 the CTIVD points out four problems in the bill which can hinder an effective oversight system and which were also pointed out in the previous letters.

- The first problem is the lack of unity of case law during review, supervision and the handling of complaints. The system of authorisation (by the minister) and assessment (by the Assessment

[23] The Netherlands, Dutch General Administrative Law Act (Algemene wet bestuursrecht), Title 7, available at: http://wetten.overheid.nl/jci1.3:c:BWBR0005537&hoofdstuk=7&afdeling=7.1&z=2017-03-01&g=2017-03-01

[24] The Netherlands, House of Representatives (*Tweede Kamer der Staten-Generaal*) (2017). Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (*Wet op de inlichtingen- en veiligheidsdiensten 20..).Plenaire vergadering 14 februari 2017*, Stemmingsuitslagen, available at: https://www.tweedekamer.nl/kamerstukken/stemmingsuitslagen/detail?id=2017P02011

[25] The Netherlands, Review Committee for the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten*) (2017), 'Wetsvoorstel Wiv 20..', Letter tot he Senate (*Eerste kamer der Staten-Generaal*), 22 March 2017 , The Hague, Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, available at: https://www.ctivd.nl/binaries/ctivd/documenten/brieven/2017/03/28/brief-ek-wiv-20/Brief+CTIVD+aan+EK+Commissie+Biza+t.b.v.+informeel+gesprek_22+maart+2017.pdf

[26] The Netherlands, Review Committee for the Intelligence and Security Services (*Commissie van Toezicht op de nlichtingen- en Veiligheidsdiensten*) (2017), Standpunt CITVD, *Wetsvoorstel Wiv 20.. - vervolg op de Zienswijze februari 2017*, The Hague, Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, available at: https://www.ctivd.nl/documenten/publicaties/2017/01/31/index

[27] The Netherlands, Review Committee for the Intelligence and Security Services (*Commissie van Toezicht op de nlichtingen- en Veiligheidsdiensten*) (2017), Standpunt CITVD, *Wetsvoorstel Wiv 20.. - vervolg op de Zienswijze februari 2017*, The Hague, Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, available at: https://www.ctivd.nl/documenten/publicaties/2017/01/31/index

Committee on the Use of Powers or TIB) in advance, and review and complaints handling afterwards (by the CTIVD) as foreseen in the bill, is stratified and complex. The CTIVD refers to the authorisation of the use of powers like surveillance independently of complaints. The exercise of powers defined in articles 45, 47, 48, 49, 50, 53, 54, 55, 56, 57, 64 and 89 of the bill need the prior authorisation of their minister. For articles 45, 47, 48, 49, 54 and 57 the Assessment Committee on the Use of Powers (TIB) will assess whether this prior authorisation granted by the minister is legal (rechtmatig). The decisions by the TIB are binding. The sub-committee of the CTIVD handles complaints and reports about any suspicion of wrongdoing. Article 114 of the bill entitles every person to lodge a specific complaint with the sub-committee on the actions or the alleged actions of persons working for the intelligence services in the implementation of the Act on the Intelligence and Security Services 20… Article 126 of the bill entitles every person to file a general report of any suspicion of wrongdoing by persons working for the intelligence services.. The CTIVD deems it necessary that the TIB and the CTIVD should explicitly be given the assignment to promote the unity of case-law. The CTIVD wants a legal provision which states that unity of case law (*rechtseenheid*) should be promoted. The CTIVD does not elaborate any further.

- The second problem is a gap in supervision. In the bill the CTIVD must respect the legality of a decision of the Assessment Committee on the Use of Powers and can only report on a decision by the Assessment Committee on the Use of Powers when this decision is based on false information or a lack of information. The CTIVD wants to retain the possibility to test the legality of the use of special powers which the TIB has authorized. In fact : the Review Committee for the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten or CTIVD*) will be split into two separate departments or sub-committees by the bill: one of which will handle complaints and reports about any suspicion of wrongdoing by the two intelligence services. This sub-committee reports to the person who has lodged a complaint or filed a report and to the responsible minister. In its report the sub-committee will decide whether the intelligence services have acted in a legal and appropriate way. The outcome can be threefold: (1) investigation by the services has to stop; (2) the exercise of a power by the intelligence services has to stop; (3) the removal and destruction of data processed by the services. The other sub-committee of CTIVD performs the general oversight task. It consists of three members. It performs its task by reviewing at a regular basis the operations of both intelligence services by investigating whether their operations or actions are in accordance with the existing legal framework for the services. These reviews will be published in special reports which will be made public. The reports contain recommendations. These reports or recommendations are not binding. The sub-committee issues reports on its own initiative or at the request of both houses of parliament (House of Representatives and Senate).

- The third problem is that in the bill the system of cooperation criteria of foreign services comes into force only after a two-year transition period. The CTIVD wants the system of cooperation criteria of foreign services to take effect immediately when the act comes into force. The bill enumerates the following criteria: democratic embedding of the service in the country concerned ; respect for human rights by the country concerned; the professionalism and reliability of the service concerned; the legal powers and capacities of the service in the country concerned; the level of data protection provided by the relevant service. The reason for the transition period in unclear. The CTIVD in its letter states that under the present act a system of cooperation already exists but that this system is not explicitly laid down in the present act (it is worked out in the memorandum to the act and other legal documents). The new bill codifies this system. For this reason the CTIVD does not see any reason for the transition period. There will be no material changes to the present system if this part of the bill takes effect immediately. But when it takes effect immediately citizens enjoy a better legal protection because the system is written down in the act.

- The fourth problem is that the bill lacks specific legal obligations to ensure that storage, analysis and use of data collected by an investigation mandated interception (the so-called dragnet) is as targeted as possible. It also lacks clarity concerning the destruction of data. The CTIVD has in earlier letters proposed specific criteria to be incorporated but these have been rejected by the government and the House of Representatives.

On 10 April 2017 the Standing Committee on the Interior of the Senate sent a report to the government [28] presenting the views of their parliamentary party and putting questions to the Government. On 3 May 2017 the Senate received a memorandum of the Minister of the Interior and Kingdom Relations answering the questions in the Senate report of 10 April 2017.[29]

The questions put to the government were diverse and reflect the criticism already voiced by oversight bodies like the CTIVD and by NGOs like Bits of Freedom or Privacy First which were reported in earlier monthly reports. One point of concern voiced by members of the Senate is that the intelligence services collect too much data of innocent citizens when carrying out an investigation mandated interception (the so-called dragnet). As pointed out by the CTIVD, the bill lacks specific legal obligations to ensure that storage, analysis and use of data collected by an investigation mandated interception is as targeted as possible. In his memorandum to the Senate the Minister of the Interior and Kingdom Relations tries to take away these concerns by describing how bulk data will be assessed in a technical way (with negative filters, positive filters and selection) after which remaining data will be considered "in principle" relevant.[30] Only if the collected data is "obviously not relevant", it should be destroyed. Members of the Senate also asked many questions about the possibility which both intelligences services have under the bill to get real-time and fully automated access to databases of cooperating companies and government agencies. The bill lacks real guarantees against abuse of these powers: there is no previous assessment (By this we mean assessment. Thus the assessment done by TIB on a prior authorisation of the minister which give powers to the services to get real-time and fully automated access to databases of cooperating companies and government agencies.) and there are no clear limits to the scope of this power. In his answers the Minister of the Interior tries to take any concerns by stressing the voluntary character of the cooperation between companies and government agencies on the one hand and the two intelligence services on the other hand. But as the NGO Bits of Freedom points out in an article on the memorandum of the Minister of the Interior: the voluntary character of the decision by companies or government agencies to give one of the intelligence services access to the data of citizens does not mean that the rights of citizens are not violated.[31] Bits of Freedom also stresses that the companies or government agencies are obliged to remain silent about their cooperation with the two intelligences services.

The Memorandum of 3 May 2017 did not take away all concerns of the members of the Senate so the Senate decided on 9 May 2017 to compile a second report putting questions to the government. Members of the Senate can send questions to the Standing Committee on the Interior of the Senate at the latest on 30 May 2017. These questions will be incorporated in the second report to the government. The government has 4 weeks for compiling a memorandum answering all the questions. There is no official calendar. So a precise date on which the Senate will vote on the bill is not known.

2. **Reports and inquiries by oversight bodies**

---

[28] The Netherlands, Senate (*Eerste Kamer der Staten-Generaal*) (2017), *Voorlopig verslag van de vaste commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat / Algemene Zaken en huis van de Koning*, 10 April 2017, available at: www.eerstekamer.nl/9370000/1/j9vvhwtbnzpbzzc/vkdagqyc2gzo/f=y.pdf

[29] The Netherlands, Minister of Interior and Kingdom relations (Minister van Binnenlandse Zaken en Koninkrijksrelaties) (2017), Memorie van Antwoord, 3 May 2017, Sent to the Senate, available at: https://www.eerstekamer.nl/9370000/1/j9vvhwtbnzpbzzc/vkdxfw8yslzz/f=y.pdf

[30] The Netherlands, Minister of Interior and Kingdom relations (*Minister van Binnenlandse Zaken en Koninkrijksrelaties*) (2017), *Memorie van Antwoord 3 Mei 2017*, 3 May 2017, Sent to the Senate, available at: https://www.eerstekamer.nl/9370000/1/j9vvhwtbnzpbzzc/vkdxfw8yslzz/f=y.pdf

[31] Korteweg, D. (2017), 'Antwoorden Plasterk roepen weer vragen op', Website Bits of Freedom, 11 May 2017, available at: www.bof.nl/2017/05/11/antwoorden-plasterk-roepen-weer-vragen-op/

A position paper [32] by the Review Committee for the Intelligence and Security Services (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten) was written as response to a memorandum published on 17 January 2017 by the Minister of Interior and Kingdom Relations containing a series of amendments to the bill for the Act on the Intelligence and Security Services 20.. (*Wetsvoorstel Wet op de inlichtingen- enveiligheidsdiensten 20..)*. [33] The CITVD welcomes some of the amendments but calls for more changes to the bill. It has the following recommendations: (1) The introduction of a clear standard which ensures that the deployment of powers to intercept is as targeted as possible.; (2) The introduction of specific legal obligations to ensure that storage, analysis and use of the data collected is as targeted as possible place and clarity about the destruction of data. *The CITVD proposes the following legal obligations; (a) the storage of data is limited to data which are related to an individual investigation assignments; (b) an obligation to destroy data not related to an individual investigation assignment in a timely fashion; (c) there should be a difference in the retention period for metadata and content; (d) the selection of data must be more targeted by making it subject to the condition that there is a selection criterion which is related to a specific person or organization or is motivated by a search focused on selection; (e) an obligation to assess selected data and to destroy these data if they are not relevant*; (3) The realization of the duty of care concerning the quality of automated data processing. *The amendment to the bill concerning a duty of care made by the minister on 18 January 2017 is too general in the vision of the CTIVD. The Act must lay down concrete instruments to review the quality of the automated data processing*; (4) The introduction of a legal provision which promotes the unity of case-law during review, supervision and the handling of complaints. *The system of authorisation (Minister) and assessment (Assessment Committee on the Use of Powers (TIB) or court) in advance, and review and complaints handling afterwards (CTIVD) as described in the Bill is stratified and complex. All above-mentioned players will be engaged in the same issues of law. It is important that uniform and consistent application of law is addressed in the new Act by assigning the TIB and the CTIVD the joint task of promoting legal uniformity*; (5) The prevention of a gap in supervision by stressing that supervision can also focus on the legality of the deployment powers to which the Assessment Committee on the use of powers has authorized. *In the present bill the CTIVD must respect the legality of a decision of the TIB and can only report on a decision by the TIB when this decision is based on false information or a lack of information. The CTIVD wants to retain the possibility to test the legality of the use of special powers which the TIB has authorized*; (6) A better protection of journalistic sources.;(7) The introduction of an obligation for prompt destruction of collected data that do not relate to the actual target.; (8) The whole system of cooperation criteria of foreign services should take effect immediately when the act comes into force, and not after a two-year transition period as envisaged by the bill.

The Dutch Data Protection Authority (Autoriteit Persoonsgegevens) and the Council for the Judiciary (Raad voor de rechtspraak) have written position papers for the round table conference on the bill for the Act on the Intelligence and Security Services 20.. (Wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20..) held on 15 December 2016 by the standing committee on the Interior of House of Representatives.

---

[32] The Netherlands, Review Committee for the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten*) (2017), Standpunt CITVD, Wetsvoorstel Wiv 20.. - vervolg op de Zienswijze februari 2017, The Hague, Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, available at: https://www.ctivd.nl/documenten/publicaties/2017/01/31/index

[33] The Netherlands, Minister of Interior and Kingdom relations (Minister of Interior and Kingdom relations) (2017), Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..), Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..). Nota van wijziging, Parliamentary Document 34 588 No. 19, available at https://www.tweedekamer.nl/downloads/document?id=509eefd9-d7ff-4cdd-9c13-27118d6afe7d&title=Nota%20van%20wijziging.pdf

In its position paper [34] the Dutch Data Protection Authority is of the opinion that the bill is not compliant with the requirements of the European Convention on Human Rights (ECHR). The ECHR sets four conditions which the bill must meet. The Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*, AP) believes that key elements of the bill do not meet these four conditions: (1) the need for granting new authorities to the intelligence services is insufficiently substantiated; (2) the proposed new authorities by the intelligence services are insufficiently transparent and predictable for people; (3) the deployment of the proposed new authorities by the intelligence services lack sufficient safeguards to protect the rights of citizens; (4) the intelligence services are not effectively and independently monitored.

In its position paper [35] the Council for the Judiciary has one main point of criticism about this bill and it concerns the independent review committee. The government wants to create an independent review committee which has to monitor the authorization granted by the minister for the deployment of the special powers by the intelligence and security services (AIVD and MIVD). The Council is of the opinion that in this bill the review committee has no direct access to data of the AIVD and MIVD and is insufficiently independent. Furthermore, the bill does not detail the design and staffing of the review committee. So it is unclear whether the committee will have sufficient knowledge and expertise to make a correct judgment. The Council recommends that the bill must stipulate that the members of the review committee are independent. Furthermore, it is recommended to grant members of the review committee sufficient powers and access to adequate information.

Update March 2017

The Netherlands Institute for Human Rights (*College voor de Rechten van de Mens*) has sent a letter to the House of Representatives as input to the debate of the House on 8 February 2017. [36] The Institute summarized in this letter the remaining issues and ambiguities of the bill. It stressed that the need to strengthen the position of the Review Committee for the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten* or CTIVD). The CTIVD needs more powers to carry out effective supervision during the actual implementation of the operations by the two intelligence services according to the Institute.[37] Report and recommendations by CTIVD in the present bill are not binding, only decision by the CTIVD when handling complaints are binding. In the opinion of the Institute, the CTIVD should also review the authorisation by the minister and the assessment in advance of the Assessment Committee on the Use of Powers or TIB and judge the

---

[34] The Netherlands, Dutch Data Protection Authority (Autoriteit Persoonsgegevens) (2016), Reactie Autoriteit Persoonsgegevens op het wetsvoorstel "Wet op de inlichtingen- en veiligheidsdiensten 20..", The Hague, Autoriteit Persoonsgegevens, available at: https://www.tweedekamer.nl/downloads/document?id=7354aedc-fc0b-45fb-bdc8-97fdd095f030&title=Position%20paper%20AP%20t.b.v.%20hoorzitting%2Frondetafelgesprek%20Regels%20met%20betrekking%20tot%20de%20inlichtingen-%20en%20veiligheidsdiensten%20alsmede%20wijziging%20van%20enkele%20wetten%20%28Wet%20op%20de%20inlichtingen-%20en%20veiligheidsdiensten%2020..%29%20d.d.%2015%20december%202016.pdf

[35] The Netherlands, Council for the Judiciary (*Raad voor de rechtspraak*) (2016), *Position Paper voor rondetafelgesprek Wet op de inlichtingen- F (088) 36 10022 en veiligheidsdiensten 20.. op donderdag 15 december 2016*, The Hague, Raad voor de Rechtspraak, available at: https://www.tweedekamer.nl/downloads/document?id=a39788f4-5861-4357-a47c-0d42db5c83d8&title=Position%20paper%20Raad%20voor%20de%20Rechtspraak%20t.b.v.%20t.b.v.%20hoorzitting%2Frondetafelgesprek%20Regels%20met%20betrekking%20tot%20de%20inlichtingen-%20en%20veiligheidsdiensten%20alsmede%20wijziging%20van%20enkele%20wetten%20%28Wet%20op%20de%20inlichtingen-%20en%20veiligheidsdiensten%2020..%29%20d.d.%2015%20december%202016%20.pdf

[36] Netherlands Institute for Human Rights (*College voor de Rechten van de mens*) (2017*), Wetsvoorstel Wet op de inlichtingenen veiligheidsdiensten 20.. (34 588)*, Letter to the House of Representatives (*Tweede kamer der Staten-Generaal*), 3 February 2017, available at: http://zoekservice.mensenrechten.nl/StippWebDLL/Resources/Handlers/DownloadBestand.ashx?id=3306

[37] Netherlands Institute for Human Rights (*College voor de Rechten van de mens*) (2017*), Wetsvoorstel Wet op de inlichtingenen veiligheidsdiensten 20.. (34 588)*, Letter to the House of Representatives (*Tweede kamer der Staten-Generaal*), 3 February 2017, available at: http://zoekservice.mensenrechten.nl/StippWebDLL/Resources/Handlers/DownloadBestand.ashx?id=3306

legality of these decisions. The bill also needs to offer clearer and more focused standards by which the CTIVD can carry out such monitoring supervision. The Institute only points at the unclear and unfocused standards in the bill, it does not specify new standards.

A report[38] by the Review Committee for the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten* or CTIVD) was sent to the House of Representatives by the Minister of Interior and Kingdom Relations on 1 February. This report investigates the way the General Intelligence and Security Service (*Algemene Inlichtingen en Veiligheidsdienst* or *AIVD*) and the Military Intelligence and Security Service (*Militaire Inlichtingen- en Veiligheidsdienst* or MIVD) have carried out the legal obligation to notify persons of the investigative powers that have been used in regard to these persons and which infringe the constitutional right to privacy at home or secrecy of communications. The report covers the years 2015 (for both service) and 2014 (only for the MIVD). Five years after use of the power in question has ended, the service must review whether notification is now possible. This legal obligation is enshrined in article 34[39] of the current Intelligence and Security Services Act 2002. The CTIVD has investigated a sample of 95 decisions about notifications by the AIVD and a sample of 43 decisions about notifications by the MIVD. The CTIVD concludes all decisions by the AIVD and MIVD were well grounded. The decisions by the AIVD were all taken in time. In all its decisions, the MIVD has exceeded the statutory reasonable period. In the current Act on the intelligence services article 34 stipulates that five years after four special powers has been exercised and subsequently once every year, the relevant Minister will examine whether a report of the events can be submitted to the person with regard to whom one of these special powers has been exercised. These special powers are: (1) to open letters and other consignments without the consent of the sender or the addressee; (2) to tap, receive, record and monitor in a directed way any form of conversation, telecommunication or data transfer by means of an automated work, (3) to receive and record non-specific non-cable-bound telecommunication (SIGINT) (4) to have access to places (intrusion). The report does not indicate the actual number of decisions taken about notifications. It also does not provide information for which type of intelligence technique the decisions were made. The report does indicate that the AIVD has notified a total of 96 persons between 2007 (the year in which the legal obligation to notify took effect) and August 2016.

Update June 2017

A report by the Review Committee for the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten* or CTIVD) was sent to the House of Representatives by the Minister of Interior and Kingdom Relations on 28 March 2017. [40] This report investigates the way the General Intelligence and Security Service (*Algemene Inlichtingen en Veiligheidsdienst or AIVD*) and the Military Intelligence and Security Service (*Militaire Inlichtingen- en Veiligheidsdienst* or MIVD) have made use of their special powers to tap journalists and lawyers. The period covers October 2015 – March 2016. The intelligence services have special powers to tap the confidential communication between lawyers and their clients and between journalist and their sources. The special powers are derived from decisions by the courts and by a special temporary regulation which took effect on 1

[38] The Netherlands, Review Committee for the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdienste*n) (2016), *Toezichtsrapport. Over de uitvoering van de notificatieplicht door de AIVD en de MIVD. CTIVD nr. 51*, The Hague, Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, available at: https://www.ctivd.nl/binaries/ctivd/documenten/rapporten/2017/02/01/index/CTIVD+Toezichtsrapport+Notificatieplicht+NR+51_LR.pdf

[39] The Netherlands, Wet op de inlichtingen- en veiligheidsdiensten 2002 (Intelligence and Security Services Act 2002), Article 34, http://wetten.overheid.nl/BWBR0013409/2017-03-01

[40] The Netherlands, Review Committee for the Intelligence and Security Services (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten) (2017),Toezichtsrapport Over de inzet van bijzondere bevoegdhedenjegens advocaten en journalisten door de AIVD en de MIVD, available at: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2017/02/07/toezichtsrapport-commissie-van-toezicht-op-de-inlichtingen-en-veiligheidsdiensten-ctivd/toezichtsrapport-commissie-van-toezicht-op-de-inlichtingen-en-veiligheidsdiensten-ctivd.pdf

January 2016. At present the legal basis of these powers is provided by the special temporary regulation which took effect on 1 January 2016. Before that date the powers were based on the decisions by the court. Before the decision of the courts (second half 2015) the services tapped confidential communication between lawyers and their clients and between journalist and their sources without any assessment. The courts decided that that should stop : there should be a special regulation which foresees in prior assessment. The special regulation foresees in a special assessment committee to which the services have to submit requests for the tapping of communication of lawyers and journalists. The CTIVD describes five cases in which the two services have acted in an irregular way towards lawyers. In one case the AIVD acted in a direct way (by hacking a lawyer). This was done by the AIVD towards a lawyer living abroad. It was unclear whether this person was still a lawyer but the AIVD failed to verify this. The AIVD did not target this person in his role as a lawyer. . In four cases involving lawyers the two services made use of their powers in an indirect way. The AIVD intercepted communications between lawyers and their clients and did not submit a request to the Temporary Assessment Committee in three cases. And in another case the MIVD made use of sigint in order to work out a conversation between a lawyer living in other EU member state and a potential client. The MIVD did not motivate whether this was necessary. This took place before the special temporary regulation took effect so the MIVD did not have to submit a request to the review committee. In all the four cases the discovery of the irregularities had as consequence that the irregular intercepted data had to be destroyed immediately.

The CTIVD also notes that the MIVD has no written rules regarding the processing of intercepted communications between journalists and their sources and between lawyers and their clients and that both the AIVD and the MIVD fail to destroy intercepted communications which are irrelevant and should not be stored.

A second report by the Review Committee for the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten* or CTIVD) was sent to the House of Representatives by the Minister of Interior and Kingdom Relations on 25 April 2017.[41] This report investigates the way in which the General Intelligence and Security Service (*Algemene Inlichtingen en Veiligheidsdienst* or AIVD) and the *Military Intelligence and Security Service (Militaire Inlichtingen- en Veiligheidsdienst* or MIVD) have carried out their authority to hack. The report investigates whether the hacking operation of the two services during the period 1 January 2015 - 17 March 2016 took place in a regular way. The legal basis of these hacking operations is the current Intelligence and Security Services Act 2002 (*Wet op de inlichtingen- en veiligheidsdiensten 2002*). The report covers all hacking operations of the MIVD and a substantial number of hacking operations of the AIVD. The report does not give exact numbers of operations. The CTIVD concludes that most hacking operations take place in a lawful way. At the same time the CTIVD found a number of irregularities. The most common irregularity is that the services structurally fail to destroy data at times when this should be done. By doing so the services act unlawfully. The CTIVD also found another shortcoming in the way both services deal with unknown vulnerabilities, so-called 'zero day's'. Both services lack procedures on how to report on these unknown vulnerabilities. A third shortcoming is that that the procedure for the renewal of the authorisation to hack fails. Due to the organisation of the administrative processes (it is particular the implementation of the legal framework which fails), the AIVD does not include the latest information of the request for renewal of the authorisation. The CTIVD deems this careless. The MIVD fails to submit requests for renewal to the minister as foreseen by the law. This can lead to irregularities.

[41] The Netherlands, Review Committee for the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten*) (2017), *Toezichtsrapport Over de inzet van de hackbevoegdheid door de AIVD en MIVD in 2015*, CTIVD nr. 53, The Hague, Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, available at: https://www.ctivd.nl/onderzoeken/a/aivd-mivd-onderzoek-hackbevoegdheid/documenten/rapporten/2017/04/25/index

3. Work of specific ad hoc parliamentary or non-parliamentary Commissions

No works of specific ad hoc parliamentary or non-parliamentary Commissions identified.

4. Work of non-governmental organisations and academia

A number of position papers was written for the round table conference on the bill for the Act on the Intelligence and Security Services 20.. (*Wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20..)* held on 15 December 2016 by the standing committee on the Interior of House of Representatives. In this section, we will summarise the most important elements of several position papers:

A position paper was written and signed by 27 academics, mostly professors with a legal or technical background.[42] The initiative for this letter was taken by Bas Jacobs, professor of Software Security and Correctness at Radboud University Nijmegen and Nico van Eijk, professor of Media and Telecommunications Law at the University of Amsterdam and Director of the Institute for Information Law. This papers specifies five areas in which the bill should be amended: (1) the supervision of the intelligence services is apportioned to too many agencies. Preventive supervision must be the task of one agency, preferably a specialized court.; (2) More and more information is shared with foreign services. The decisions to share information are not reviewed prior to the sharing. This should change; (3) The bill does not guarantee that the supervisory authorities have enough means to fulfil their tasks. The authors suggest that the budget should be determined independently, for example by the Audit Court of the House of Representatives; (4) The collection and analysis of information, especially bulk information, must happen in a more selective way. For example by using 'select while you collect' methods.; (5) The bill does not regulate what information can be made public or what information can be requested. The bill also does not clarify whether companies involved in the surveillance may talk about their commitment in the surveillance.

A position paper [43] was written by the Digital Infrastructure Association or DNIL is a sectoral organisation that represents the organisations which provide the facilities necessary for the digital economy: data centres, hosting parties, internet service providers, AMS-IX and SURFnet. DNIL is of the opinion that the overview system proposed by the bill is inadequate. The paper contains the following seven recommendations: (1) Remove perverse incentives: no action (buying) vulnerabilities, or other activities that stimulate trade in zero day vulnerabilities.; (2) Do not use structural weaknesses without immediately reporting these to the companies.; (3) Do not violate generic encryption systems (TTP, certificates, SSL) and other safety systems in a structural way.; (4) Do not collect data in bulk without a strong, clear focus on a specific research topic. "Bycatch" should be removed immediately.; (5) Do not store data of individuals and companies which are not the subject of an investigation.; (6)

---

[42] Jacobs, N., Van Eijk, N. et al (2016), Position paper UvA - IViR en meerdere organisaties t.b.v. hoorzitting/rondetafelgesprek Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..) d.d. 15 december 2016, available at: https://www.tweedekamer.nl/downloads/document?id=7862568b-02fe-4cc8-82e1-4291db68fe4a&title=Position%20paper%20UvA%20-%20IViR%20en%20meerdere%20organisaties%20t.b.v.%20hoorzitting%2Frondetafelgesprek%20Regels%20met%20betrekking%20tot%20de%20inlichtingen-%20en%20veiligheidsdiensten%20alsmede%20wijziging%20van%20enkele%20wetten%20%28Wet%20op%20de%20inlichtingen-%20en%20veiligheidsdiensten%2020..%29%20d.d.%2015%20december%202016.pdf

[43] Digital Infrastructure Association (Stichting Digitale Infrastructuur Nederland or DNIL) (2016), Position paper DINL t.b.v. hoorzitting/rondetafelgesprek Wet op de inlichtingen- en veiligheidsdiensten d.d. 15 december 2016, Leidschendam, Stichting Digitale Infrastructuur Nederland, available at: https://www.tweedekamer.nl/downloads/document?id=3ce6e5d8-0d4a-4fcf-9c0e-9f226abfaa84&title=Position%20paper%20DINL%20t.b.v.%20hoorzitting%2Frondetafelgesprek%20Regels%20met%20betrekking%20tot%20de%20inlichtingen-%20en%20veiligheidsdiensten%20alsmede%20wijziging%20van%20enkele%20wetten%20%28Wet%20op%20de%20inlichtingen-%20en%20veiligheidsdiensten%2020..%29%20d.d.%2015%20december%202016.pdf

Only exchange data of a person or company with other intelligence services and countries when there is a specific, targeted suspicion against that person or company.; (7) Waive unfocused tapping, eavesdropping and intervention in international connections, facilities and security systems (nodes, international carrier connections, sea cables, security systems such as TTP, generic infrastructure)

A position paper[44] was written by a professor on Cyber Operations & Cyber Warfare at the Netherlands Defence Academy and Professor by special appointment on law in military cyber operations at the University of Amsterdam. In this paper he outlines in general the need for granting special powers in *cyber space to the intelligence services without examining the bill or giving any comments on the bill.*

A position paper was written by KPN. [45] KPN is a Dutch provider and telecommunications company. KPN started as the public telecommunications company The main concern of KPN regarding this bill concerns the generally formulated cooperation obligations for providers. Providers will have no real possibility to assess the proportionality and content of the required deployment of resources requested by the intelligence services. KPN argues that providers must have the right to be heard by the supervisor before deployment of services are to be done.

In its position paper [46] Microsoft expresses its concerns about the following aspects of the bill. The bill would allow to share metadata collected by the Dutch intelligence services with other (foreign) security services (Article 64), for which moreover only the approval of the Minister is required. The bill would allow for the Dutch services to gather information when requested by a foreign service. The Explanatory Memorandum to the bill states that the new law will have no extraterritorial effect. But Microsoft points out that the bill is ambiguous concerning its extraterritorial effect. Microsoft states that there is a lot of uncertainty about the territorial scope of the act.

In its position paper [47] the Dutch Scientific Council for Government Policy (*Wetenschappelijke Raad voor het Regeringsbeleid*) points at the effects of extending the powers of the intelligences services to intercept internet traffic and email and phone communications for the behaviour of citizens. These so called chilling effects can lead to citizens changing their normal legitimate behaviour because the intelligence services have the power to intercept data on a massive scale.

---

[44] Ducheine, P. A. L. (2016), *De bevordering en bescherming van nationale belangen en militaire missies: Position paper t.b.v. hoorzitting/rondetafelgesprek Tweede Kamer, Commissie BZK vanwege wetvoorstel Wet op de inlichtingen- en Veiligheidsdiensten 20xx Dossiernr. 34 588. Tweede Kamer der Staten-Generaal*., available at: https://pure.uva.nl/ws/files/7795267/Ducheine_TK_WIV_final_correct_20161215.pdf

[45] KPN (2016), Inbreng hoorzitting Tweede Kamer WIV 20.. – 15 december 2016, The Hague, KPN, available at: https://www.tweedekamer.nl/downloads/document?id=26b02d13-2fde-4cc5-b7ae-c6ea48f7b5a4&title=Position%20paper%20KPN%20t.b.v.%20hoorzitting%2Frondetafelgesprek%20Regels%20met%20betrekking%20tot%20de%20inlichtingen-%20en%20veiligheidsdiensten%20alsmede%20wijziging%20van%20enkele%20wetten%20%28Wet%20op%20de%20inlichtingen-%20en%20veiligheidsdiensten%2020..%29%20d.d.%2015%20december%202016%20.pdf

[46] Microsoft (2016), *Inbreng Microsoft. Hoorzitting / rondetafelgesprek Wet op de Inlichtingen- en Veiligheidsdiensten 15 december 2016*, Redmond (USA), Microsoft Corporation, available at: https://www.tweedekamer.nl/downloads/document?id=edd84fe7-26cc-461b-a55b-3f38173031d0&title=Position%20paper%20Microsoft%20t.b.v.%20hoorzitting%2Frondetafelgesprek%20Regels%20met%20betrekking%20tot%20de%20inlichtingen-%20en%20veiligheidsdiensten%20alsmede%20wijziging%20van%20enkele%20wetten%20%28Wet%20op%20de%20inlichtingen-%20en%20veiligheidsdiensten%2020..%29%20d.d.%2015%20december%202016.pdf

[47] The Netherlands, Scientific Council for Government Policy (*Wetenschappelijke Raad voor het Regeringsbeleid*) (2016), *Position paper WRR en EUR t.b.v. hoorzitting/rondetafelgesprek Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..) d.d. 15 december 2016*, The Hague,Wetenschappelijke Raad voor het Regeringsbeleid, available at: https://www.tweedekamer.nl/downloads/document?id=b135edba-3cf7-4e8a-930e-d3b2f9b716b3&title=Position%20paper%20WRR%20en%20EUR%20t.b.v.%20hoorzitting%2Frondetafelgesprek%20Regels%20met%20betrekking%20tot%20de%20inlichtingen-%20en%20veiligheidsdiensten%20alsmede%20wijziging%20van%20enkele%20wetten%20%28Wet%20op%20de%20inlichtingen-%20en%20veiligheidsdiensten%2020..%29%20d.d.%2015%20december%202016%20.pdf

The data protection NGO Privacy First sent a letter to the House of Representatives intended as input for the plenary debate of the House Representatives which was planned in week 6 of 2017, on 8 February 2016.[48] In this letter Privacy First discusses the bill for the Act on the Intelligence and Security Services 20.. (*Wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20..)* as amended. on 17 January 2017 by the Minister of Interior and Kingdom Relations. [49] Privacy First voices many concerns and offers recommendations. Privacy First qualifies the bill as extremely totalitarian and calls on the House of Representatives to improve the bill or to reject the bill. Privacy First criticises the speed by which the government wants to pass the bill through the general elections of 15 March 2017. Privacy First voices many concerns and offers recommendations. The first point of concern is the dragnet entailed in the bill. Privacy First want to remove the dragnet function from this bill. Other points of concern include: the storage period of 3 years is too long and must be deleted; the power to share unanalysed bulk data with foreign services; the powers to obtain data and to use data are virtually limitless (Privacy First urges the House to remove these powers or thoroughly mitigate these powers by providing legal safeguards); the obligation to notify (that they are being targeted) should not only apply to individuals but also to organizations; the power to hack third parties is too extensive; the prior authorisation to the use of powers should be extended ; lack of protection for journalist sources.

Update March 2017

Dutch Daily newspaper "NRC Handelsblad" published an editorial on 8 February 2017. In this editorial it calls on the House of Representatives to postpone the debate and the vote on the previously mentioned bill to a date after the general elections of 15 March 2017.[50] The bill is too far reaching and has too many inadequacies. "NRC Handelsblad" singles out the deficient review system and the far reaching powers for the intelligence services to intercept bulk data and store these data for three years.

On its website, watchdog NGO Bits of Freedom reacted to the passing of the bill by the House of Representatives.[51] It stated that it is beyond disappointing that this bill with such momentous consequences was rushed through the House of Representatives with such relentless determination. In the assessment of Bits of Freedom, a major flaw of the bill is that it allows intelligence services to systematically conduct mass surveillance of the internet. This undermines a core value of a free society, namely that citizens who are not suspected of wrongdoing ought not to be monitored. Other major flaws of this bill pointed out by Bits of Freedom are: (1) it allows the Dutch intelligence services to share collected data with foreign services without having analysed it first; (2) the Dutch intelligence services are granted direct and fully automated access to databases (data and content data) of cooperating organizations without human interference; "cooperating organisations" includes any societal organisations which cooperate with the two Dutch intelligence service. Examples are governmental institutions such as the tax authorities, but also schools, civic organizations and businesses like banks; (3) wanting and unspecified standards (the limitations of the powers of the services will become clear only as we go along). Citizens are offered little clarity in this matter. The

---

[48] Privacy First (2017), *Commentaar Privacy First op wetsvoorstel 34588 (wet op de inlichtingen- en veiligheidsdiensten)*, Letter to the House of Representatives (*Tweede Kamer der Staten-Generaal*), 31 January 2017, available at: www.privacyfirst.nl/images/stories/wetgeving/SPF20170131_Wiv.pdf

[49] The Netherlands, Minister of Interior and Kingdom relations (2017), Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..), Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..). Nota van wijziging, Parliamentary Document 34 588 No. 19, available at https://www.tweedekamer.nl/downloads/document?id=509eefd9-d7ff-4cdd-9c13-27118d6afe7d&title=Nota%20van%20wijziging.pdf

[50] NRC Handelsblad (2017), 'Wet inlichtingendiensten is even ingrijpend als onrijp', Editorial, 8 February 2017, https://www.nrc.nl/nieuws/2017/02/08/wet-inlichtingendiensten-is-even-ingrijpend-als-onrijp-6588317-a1544947

[51] Korteweg, D. (2017), 'Dutch House of Representatives passes dragnet surveillance bill', Web page, Bits of Freedom, 16 February 2017, available at: https://www.bof.nl/2017/02/16/dutch-house-of-representatives-passes-dragnet-surveillance-bill/

bill offers too little guidance for proper assessment. Furthermore, the extent of the encroachment on public liberties will largely be determined by ongoing technological developments.

Update June 2017

The NGO Bits of Freedom has written an article on the memorandum of 3 May 2017 of the Minister of the Interior and Kingdom Relations answering the questions in the Senate report of 10 April 2017.[52]

[52] Korteweg, D. (2017), 'Antwoorden Plasterk roepen weer vragen op', Website Bits of Freedom, 11 May 2017, available at: www.bof.nl/2017/05/11/antwoorden-plasterk-roepen-weer-vragen-op/

ANNEX – Court decisions

Thematic area	Please provide the most relevant high court decision relating to the use of surveillance measure.
Decision date	4 May 2016
Reference details	Netherlands, Administrative Jurisdiction Division of the Council of State (*Afdeling Bestuursrechtspraak van de Raad van State*) (2016), *Case no. 201505432/1/A3*, 4 May 2016,ECLI:NL:RVS:2016:1218, available at: http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RVS:2016:1218
Key facts of the case (max. 500 chars)	On 4 March 2014 the Minister of the Interior refused to make tapping statistics covering the period 1971-2013 (taps being used by the security and intelligence services) available to Bits of Freedom on the basis of national security arguments. Bits of Freedom filed an objection. On 3 December 2014 tapping statistics covering 1991 up to and including 2001 and 1984, 1985 and 1986 were made available. Bits of Freedom wanted to obtain the other information as well and went to a District Court, which held that the minister was right. There was too much of a risk of giving insight into the operations of the security and intelligence services. In appeal, the Council of State annulled this judgement and noted that the minister should take a new decision, taking into consideration a report of 13 June 2012 drawn up by the Review Committee supervising the way the services work (Commissie van Toezicht op de Inlichting- en Veiligheidsdiensten). This report says that the mere publication of the number of taps does not lead to an insight into the functioning of the services and is therefore no risk to national security.
Main reasoning/argumentation (max. 500 chars)	The report by the Review Committee notes the following. The mere publication of tapping statistics does not show by what issues the number of taps is affected, or in which way the taps have been made by the General Security and Intelligence Service. There is no information about a change in the issues that are investigated, new priorities, lack of capacity or the use of additional, special powers. There is a danger only if someone or an organisation can adapt their behaviour on the basis of the information. There therefore is no considerable likelihood of national security being endangered here. The Council of State holds that the minister has not followed up this opinion. The minister says that any risk to national security, and not just some likelihood, is at stake here and that the tapping statistics can therefore not be provided. The State Council holds that the minister should take a new decision in which the opinion of the Review Committee is not passed by.

Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	If there is no considerable likelihood that national security is impeded when tapping statistics by the security and intelligence services are made available, they should be provided. The minister states that any risk to national security should be avoided, but he has not substantiated this so far and he has not given reasons for this line of reasoning so far. He suddenly relies on Article 55, paragraph one, beginning and under b, of the Act on the Intelligence and Security Services (which says that an application for the provision of data will be denied in so far as it could damage national security). He should take a new decision. In other words, the concept of possible damage to national security should be elaborated upon.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The minister has to take a new decision. Appeal will be possible to the Council of State.
Key quotation in original language and translated into English with reference details (max. 500 chars)	. . . is de minister ter zitting nader ingegaan op het rapport. Hij heeft hierbij onder meer te kennen gegeven dat de CTIVD, blijkens paragraaf 7.1.1 van het rapport, ervan uitgaat dat gegevens staatsgeheim zijn, indien door verstrekking van die gegevens een aanmerkelijke kans is op schade aan de nationale veiligheid. Volgens de minister is voor een dergelijke rubricering op grond van de Wiv echter voldoende als een risico op schade aan de nationale veiligheid bestaat. Indien dit risico bestaat, kunnen de verzochte gegevens op grond van artikel 55, eerste lid, aanhef en onder b, van de Wiv niet worden verstrekt. Dit is een absolute weigeringsgrond zodat geen mogelijkheid bestaat hiervan af te wijken, zodat het advies in het rapport in die gevallen niet kan worden gevolgd. Voormelde toelichting van de minister is niet neergelegd in het bestreden besluit noch in enig ander in het dossier voorkomend stuk. . . . Het betoog slaagt. The minister has gone into the report [by the Review Committee] in more detail during the present hearing. He has stated, among other things, that the Review Committee pursuant to paragraph 7.1.1. of the report, presumes that data are confidential within the state, if the provision of these data leads to a considerable likelihood of damage to the national security. According to the minister, however, it is sufficient for such labelling on the basis of the Act on the Security and Intelligence Services if there is a risk of damage to national security. If this risks exists, the data cannot be provided on the basis of Article 55, paragraph one, beginning and other b. It is absolutely prohibited so that there is no possibility to deviate from this, so that the advice in the report, in those cases, cannot be followed. This explanation byt the minister has not been laid down in the decision taken, nor in any other document in the files of

	this case. The appeal is therefore upheld.

Thematic area	Please provide the most relevant high court decision relating to the use of surveillance measure.
Decision date	14 March 2017
Reference details	The Netherlands, Court of Appeal The Hague (*Gerechtshof Den Haag*) (2017), Case no. 200.162.969. ECLI:NL:GHDHA:2017:535, 14 March 2017, available at: http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHDHA:2017:535
Key facts of the case (max. 500 chars)	A number of citizens and NGO's lodged an appeal against a decision of 23 July 2014 in which the district court of The Hague ruled that the collaboration and exchange of data on the basis of trust between Dutch secret services and foreign secret services (the American and British in particular) may simply be continued. According to the court, the importance of national security is the determining factor. The plaintiffs deem this ruling to be in flagrant breach of the right to privacy and have lodged an appeal. The plaintiffs do not seek to ban the collaboration with foreign services as such. They find that when it comes to collaborating and receiving data, strict safeguards should be maintained. The plaintiffs demand that the Dutch services only receive data from foreign intelligence services when it is verified that data were collected by the foreign service in accordance with Dutch and international law.
Main reasoning/argumentation (max. 500 chars)	Plaintiffs argue that the Dutch intelligence services cannot receive data collected by foreign secret services (among which the American NSA) because since the revelations by Snowden it is clear that these services (the NSA in particular) violate the rights of citizens when collecting data. In case one of the Dutch intelligence services receives data from the NSA it is highly likely that these have been obtained in a way which is illegal under Dutch and/or American law. They demand that the Dutch services only receive data from foreign services if they have established that these data are collected in a legal way.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Dutch intelligence service, in case they data receive data from foreign intelligence services, are not obliged to establish whether these data were collected in accordance with Dutch law and/or international law.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The court reject the appeal and rules that the Dutch intelligence services have no obligation to verify whether the data they receive from foreign services were collected in a legal way. According to the court, there are insufficient concrete indications that the NSA and the British secret service violate fundamental rights. The fact that foreign intelligence services sometimes have more powers than the Dutch intelligence services does not mean that the

	Dutch services may not receive data from these foreign intelligence services. This could be otherwise if Dutch intelligence services deliberately circumvented their own legal constraints by taking advantage of the wider powers of foreign intelligence services. However, in this case, the court has not found such abuse. The plaintiffs have indicated that they will challenged the decision and go to the Supreme Court.[53]
Key quotation in original language and translated into English with reference details (max. 500 chars)	"De conclusie uit het voorgaande is dat er in dit geding niet van kan worden uitgegaan dat de inlichtingendiensten gegevens van buitenlandse inlichtingendiensten ontvangen die door de desbetreffende buitenlandse inlichtingendienst op ongeoorloofde wijze zijn verkregen. Voor zover wel de mogelijkheid bestaat dat dit gebeurt is die enkele mogelijkheid niet voldoende om het vertrouwensbeginsel opzij te zetten en om het toezicht te verscherpen en/of van de inlichtingendiensten te verlangen dat zij bij elke ontvangst van gegevens van de NSA of de GCHQ vaststellen dat deze gegevens in overeenstemming met de toepasselijke grondrechten zijn verzameld." "The conclusion from the foregoing is that, in this case, it cannot be assumed that intelligence services receive data from foreign intelligence services obtained unlawfully by the relevant foreign intelligence service. To the extent that this possibility is possible, that simple possibility is not sufficient to set aside the principle of trust and to tighten up the supervision and/or demand from the intelligence services that, at each reception of NSA or GCHQ data, to establish that these data have been collected in accordance with the applicable fundamental rights" The Netherlands, Court of Appeal The Hague (*Gerechtshof Den Haag*) (2017), Case no. 200.162.969. ECLI:NL:GHDHA:2017:535, 14 March 2017, available at: http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:GHDHA:2017:535

[53] Thijm, C.A. & De Vries, C. (2017), Hof Den Haag: "Buitenlandse diensten handelen niet illegaal bij het vergaren van gegevens van burgers", 14 March 2017, Bureau Brandeis, available at: https://www.bureaubrandeis.com/buitenlandse-diensten-handelen-niet-illegaal-vergaren-gegevens-burgers/