National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies

THE NETHERLANDS

Version of 25 September 2014

Art.1, Dutch knowledge centre on discrimination
Jacky Nieuwboer

SUMMARY

Description of the surveillance framework in the Netherlands

[1]. The two actors that are eligible to conduct mass surveillance are the General Intelligence and Security Service (*Algemene Inlichtingen en Veiligheidsdienst*, hereinafter: AIVD) and the Military Intelligence and Security Service (*Militaire Inlichtingen en Veiligheidsdienst*, hereinafter: MIVD). A joint effort of the AIVD and MIVD is the Joint Sigint Cyber Unit, established on 15 June 2014. Its predecessor is the National Signals Intelligence Organisation (*Nationale Signals Intelligence Organisatie*, NSO). The aim of the new Unit is to specifically combat cyber threats. [1] [2]There are currently no publicly disclosed programmes of mass cyber surveillance in the Netherlands, although there were many questions in Parliament after the Snowden revelations. However, the government denied all these questions, so that nothing new was actually revealed.[3]

[2]. The Act governing the AIVD and the MIVD is the Act on Intelligence and Security Services (*Wet op de Inlichtingen en Veiligheidsdiensten*, hereinafter: Wiv).[4] Its main focus is on the powers of the services. In the following, this summary will go into the power to intercept cable-bound communication, non cable-bound communication and the power to exchange information with other services.

[3]. The Dutch intelligence agencies, including the Joint Sigint Cyber Unit, are prohibited from conducting mass cable surveillance at the moment. Telecommunication interceptions of communication that is cable-bound (telephone and internet, glassfibre cables) must be targeted and they need prior ministerial approval. [5] It is assumed that the legislation in this field applies to interceptions abroad as well.[6] The services are allowed to conduct surveillance

---

[1] European Parliament, DG for Internal Policies (2013), National Programmes for mass surveillance of personal data in EU Member States and their compatibility with EU Law, PE 493.032, Brussels, October 2013; www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET(2013)493032_EN.pdf, pp. 73-76.

[2] Netherlands, Minister of the Interior and Kingdom Relatioins, Minister of Defence (*Minister van Binnenlandse Zaken en Koninkrijksrelaties, Minister van Defensie*) (2014), Letter to the Lower House of Parliament (*Tweede Kamer der Staten-Generaal*), no. BS2014018110, 3 July 2014, available at:www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2014/07/03/kamerbrief-over-convenant-joint-sigint-cyber-unit-jscu.html

[3] E-mail correspondence with F.J. Zuiderveen Borgesius, Utrecht University on 2 September 2014, and see https://www.opendemocracy.net/can-europe-make-it/nico-van-eijk/mass-surveillance-dutch-state-of-denial, accessed on 3 September 2014.

[4] Netherlands, Intelligence and Security Services Act 2002 (Wet op de Inlichtingen en Veiligheidsdiensten), 7 February 2002, available at: http://wetten.overheid.nl/BWBR0013409/geldigheidsdatum_14-03-2013

[5] Netherlands, Intelligence and Security Services Act 2002 (*Wet op de Inlichtingen en Veiligheidsdiensten 2002*), Article 25, paragraphs 1-6, available at: http://wetten.overheid.nl/BWBR0013409/geldigheidsdatum_01-08-2014.

[6] Netherlands, Commissie evaluatie Wiv 2002 (2013), Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen, available at: www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2013/12/02/rapport-

focusing on non cable-bound communication (satellite and radio traffic) without limits in terms of prior approval or in terms of geographical limits. They do need ministerial approval once they have specifics, such as an address, or when they use keywords in their search.[7]

[4]. A committee assessing the activities of the services in 2013 recommended Parliament that the powers of the services be widened. The fact that the services have no power to intercept untargeted, cable-bound communication is considered out-of-date. The services should receive this power, also in order to fight cyber attacks. At the same time, ministerial approval should accompany every step of the new surveillance process. The opinions of the Review Committee that oversees the activities of the services at present should become binding, which is not the case at present. All this to strike a balance between safeguarding the interests of the State and ensuring respect for privacy and data protection.[8] The Minister of the Interior and Kingdom Relations is drafting a bill on the basis of the above-mentioned assessment (which was presented to Parliament on 2 December 2013). Part of the bill is ready at this moment. It is expected to be ready for internet consultation by the end of 2014.[9]. The bill is intended to become effective on 1 July 2016 at the latest.[10]

[5]. Intelligence services conduct surveillance for the purpose of national security. There is no definition of this concept in legislation or case law.[11] The Review Committee on the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten*), the expert body that supervises the intelligence services, Those parts which are of vital interest for keeping intact social life must be protected. Investigations may be conducted into persons who give rise to the serious suspicion that they form a threat for

---

evaluatie-wet-op-de-inlichtingen-en-veiligheidsdiensten-2002/rapport-evaluatie-wet-op-de-inlichtingen-en-veiligheidsdiensten-2002.pdf, p. 44.

[7] Netherlands, Intelligence and Security Services Act 2002 (*Wet op de Inlichtingen en Veiligheidsdiensten 2002*), Article 26, paragraphs 1-5, available at: http://wetten.overheid.nl/BWBR0013409/geldigheidsdatum_01-08-2014.

[8] Netherlands, Commissie evaluatie Wiv 2002 (2013), Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen, available at: www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2013/12/02/rapport-evaluatie-wet-op-de-inlichtingen-en-veiligheidsdiensten-2002/rapport-evaluatie-wet-op-de-inlichtingen-en-veiligheidsdiensten-2002.pdf, pp. 78-80, p. 83, p, 87, p. 89 and p. 102.

[9] E-mail correspondence with the Review Committee on the Intelligence and Security Services (CTIVD), 4 September 2014.

[10] The Netherlands, Ministry of the Interior and Kingdom Relations (*Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*) (2014), Voorgenomen en aanhangige wetsvoorstellen die (mede) betrekking hebben op Caribisch Nederland (overzicht juli 2014), The Hague, Ministry of the Interior and Kingdom Relations, available at: www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2014/07/04/bes-wetgeving-in-voorbereiding-rijksbreed/voorgenomen-en-aanhangige-wetsvoorstellen-bes-wetgeving-voor-caribisch-nederland-overzicht-juli-2014.pdf.

[11] The Review Committee on the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten*), the expert body that supervises the intelligence services, has looked into the interpretation of this term, mostly on the basis of the Kamerstukken accompanying the law, since there was some debate on this when the law was developed.

the continuation of the rule of law, for security or other important interests of the State, due to the aims they try to achieve, or due to their activities. [12]

[6]. Dutch intelligence services may co-operate with foreign intelligence services, even if the powers of these services, such as the NSA's, are wider than the powers of the Dutch intelligence services. In a very recent case, the court judged that national security prevailed over the general complaints about lack of privacy of, among others, two interest groups. The interest groups argued that the Dutch services could now use information about Dutch citizens (provided, in particular, by the NSA) which they would not have been able to collect themselves due to restrictions to their powers. However, the court ruled that the information provided by the NSA was obtained by the Dutch intelligence services in bulk and processing and using this information would still be subject to Dutch law. Moreover, the court ruled that the exchange of information was not contrary to EU law (ECHR). A possible restriction of fundamental rights was necessary in a democratic society: it was proportionate to the legitimate aim (national security) pursued,[13] as the complaints of the plaintiffs were only of a general nature and they were not affected individually. Individuals would be able to rely on the CTIVD (Review Committee on the Intelligence and Security Services), which is allowed to carry out investigations. They may ask the Ministers involved for information about personal data and they have recourse to the courts.[14]

[7]. In connection with their power to intercept cable-bound communication, the intelligence and security services have the right to ask specific information from telecom or internet providers. These providers may not refuse to give this information and have to track down this information if they do not have it at their disposal immediately. Data in connection with telephone traffic must be kept for twelve months; data in connection with the internet, e-mail and telephone conversations through the internet, must be kept for six months.[15] [16]Some internet providers have publicised information on how often they have been asked to co-operate with the police in 2012 and 2013. It turned out that the police in dozens of cases wrongly addressed a provider which only provided blocks of IP-addresses and could have no knowledge of the ultimate users. [17] [18] Another provider (partially) rejected most of the

---

[12] Netherlands, Intelligence and Security Services Act 2002 (*Wet op de Inlichtingen en Veiligheidsdiensten 2002*), Article 6, paragraphs 2, under a and d, available at: http://wetten.overheid.nl/BWBR0013409/geldigheidsdatum_01-08-2014.

[13] This balance is also recognized by the European Commission, see - European Commission for Democracy through Law (Venice Commission) (1998), Internal security services in Europe: Secretariat memorandum based on the opinions of Mr John Lundum, Mr Joseph Said Pullicino & Mr Antti Suviranta, Study no. 039 / 97, CDL(1998)011-e, Strasbourg, 19 February 1998; ww.venice.coe.int/webforms/documents/?pdf=CDL(1998)011-e, p. 17.

[14] Netherlands, District Court of The Hague (*Rechtbank Den Haag*) (2014), case number ECLI:NL:RBDHA:2014:8966, 23 July 2014, available at: http://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2014:8966.

[15] Netherlands, Intelligence and Security Services Act 2002 (*Wet op de Inlichtingen en Veiligheidsdiensten 2002*), Article 25 and Article 28, paragraphs 1-4, available at: http://wetten.overheid.nl/BWBR0013409/geldigheidsdatum_01-08-2014.

[16] Netherlands, Telecommunication Act (*Telecommunicatiewet*), Article 13.2a.paragraph 2, under 3a,

[17] RIPE NCC (2013), Law Enforcement Agency Requests 2012, Amsterdam, RIPE NCC, available at: www.ripe.net/ripe/docs/ripe-593.

[18] RIPE NCC (2014), Law Enforcement Agency Requests 2013, Amsterdam, RIPE NCC, available at: www.ripe.net/ripe/docs/ripe-607.

requests for information because they were invalid, incomprehensible, or otherwise had no basis under the relevant law.[19] [20] [21] 2012 and 2013 reports by a third provider show that cable-bound communication was checked and tapped, and information about personal data was asked more than 150 times.[22] [23] Telecom providers are also obliged to provide a list of all their clients on a daily basis to the Central Information Desk Investigations Telecommunication (*Centraal Informatiepunt Onderzoek Telecommunicatie,* CIOT).[24] Services have direct access to this system.[25] [26] The conclusion may be drawn that services often do not approach the right party, do not put their requests in clear language, and check cable-bound communication dozens of times in 2012 and 2013, as far as this has been reported.

Safeguards for privacy and data protection

[8]. The Review Committee on the Intelligence and Security Services (*Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten*) has a number of powers in controlling the activities of the services and the Ministers involved, although its opinions are non-binding. The Committee judges the lawfulness of the activities of the Ministers and the services.[27] The Committee informs the Ministers and advises the Ministers about its findings.[28] More specifically, when

---

[19] De Joode, A. (2013), LeaseWeb first hosting provider worldwide to launch Law Enforcement Transparency Report, Web Page, Amsterdam, LeaseWeb, available at: http://blog.leaseweb.com/2013/04/11/leaseweb-first-hosting-provider-worldwide-to-launch-law-enforcement-transparency-report/

[20] De Joode, A. (2013), Law Enforcement Transparency Report 2013: January 1 – June 30, Web page, Amsterdam, LeaseWeb, available at: http://blog.leaseweb.com/2013/08/28/law-enforcement-transparency-q1q2-2013/

[21] De Joode, A. (2014), Law Enforcement Transparency Report 2014: July 1 – December 31, Web Page, Amsterdam, LeaseWeb, available at: http://blog.leaseweb.com/2014/02/25/law-enforcement-transparency-report-2014-july-1-december-31/

[22] XS4ALL (2013), Transparantierapport 2012, Amsterdam, XS4ALL, available at: https://www.xs4all.nl/media/transparantie/Transparantierapport-2012.pdf

[23] XS4ALL (2014), Transparantierapport 2013, Amsterdam, XS4ALL, available at: www.xs4all.nl/media/transparantie/Transparantierapport-2013.pdf

[24] Netherlands, Decision on the supply of telecommunication data (*Besluit verstrekking gegevens telecommunicatie*), Article 3, paragraph 3.

[25] Netherlands, Netherlands, Departmental Audit Service (Departmentale Auditdienst) (2012), Eindrapport audit CIOT 2011, The Hague, Ministerie van Veiligheid en Justitie, available at: www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/09/25/eindrapport-audit-ciot-2011/eindrapport-audit-ciot-2011.pdf; Netherlands, Netherlands, Departmental Audit Service (Departmentale Auditdienst) (2011),Eindrapport audit CIOT 2010. Een audit naar de opvolging door het CIOT van de aanbevelingen uit de audit 2008 en 2009, The Hague, Ministerie van Veiligheid en Justitie, available at: www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/08/02/eindrapport-audit-ciot-2010/eindrapport-audit-ciot-2010.pdf

[26] Netherlands, Decision on the supply of telecommunication data (*Besluit verstrekking gegevens telecommunicatie*), Article 3, paragraph 2.

[27] Netherlands, Intelligence and Security Services Act 2002 (*Wet op de Inlichtingen en Veiligheidsdiensten 2002*), Article 64, paragraphs 2, under a, available at: http://wetten.overheid.nl/BWBR0013409/geldigheidsdatum_01-08-2014.

[28] Netherlands, Intelligence and Security Services Act 2002 (*Wet op de Inlichtingen en Veiligheidsdiensten 2002*), Article 64, paragraphs 2, under b, available at: http://wetten.overheid.nl/BWBR0013409/geldigheidsdatum_01-08-2014.

asked for information about personal data by individuals concerned, the Minister must inform the CTIVD about his/her decision when s/he decides to refuse the request for information.[29] The Committee also gives advice to the Ministers about complaints.[30] It also carries out investigations into the activities of the intelligence and security services, thereby overseeing these activities.[31] It drafts a report and sends it to the Minister involved. After having received the reaction of the Minister, the Committee will finalise its report. It may make recommendations and will then send the report to the Minister. The Minister, in his or her turn, will send the final report and his or her reaction within six weeks to both Houses of Parliament.[32] Moreover, the Committee reports to Parliament every year before 1 May about its own activities.[33] When the services collect data they have to limit themselves to non-cable bound communication and targeted cable-bound communication. They need prior ministerial approval in the case of targeted cable-bound communication, and also need ministerial approval once they search using specifics, such as keywords. Data may in principle be stored for no longer than a year. This is different when they are analysed.[34] Data must be destroyed when they have lost their significance.[35]

[9]. Safeguards are the following: the Ministers involved have to approve the collection of targeted personal data in advance. Ministers must in principle, five years after the collection and analysis of the data, issue a report to the individual concerned about personal data having been processed. No report will be issued during an ongoing investigation. **[36]** If the Minister cannot disclose the report, he or she will have to inform the Committee.[37]If it turns out that

---

[29] Netherlands, Intelligence and Security Services Act 2002 (*Wet op de Inlichtingen en Veiligheidsdiensten 2002*), Article 47 in conjunction with Article 55, paragraphs 3 and 4, available at: http://wetten.overheid.nl/BWBR0013409/geldigheidsdatum_01-08-2014.

[30] Netherlands, Intelligence and Security Services Act 2002 (*Wet op de Inlichtingen en Veiligheidsdiensten 2002*), Article 64, paragraph 2, under c, available at: http://wetten.overheid.nl/BWBR0013409/geldigheidsdatum_01-08-2014.

[31] Netherlands, Intelligence and Security Services Act 2002 (*Wet op de Inlichtingen en Veiligheidsdiensten 2002*), Article 78, paragraph 1, available at: http://wetten.overheid.nl/BWBR0013409/geldigheidsdatum_01-08-2014

[32] Netherlands, Intelligence and Security Services Act 2002 (*Wet op de Inlichtingen en Veiligheidsdiensten 2002*), Article 79, available at: http://wetten.overheid.nl/BWBR0013409/geldigheidsdatum_01-08-2014.

[33] Netherlands, Intelligence and Security Services Act 2002 (*Wet op de Inlichtingen en Veiligheidsdiensten 2002*), Article 80, available at: http://wetten.overheid.nl/BWBR0013409/geldigheidsdatum_01-08-2014.

[34] Netherlands, Intelligence and Security Services Act 2002 (*Wet op de Inlichtingen en Veiligheidsdiensten 2002*), Article 27, paragraphs 9 and 10, available at: http://wetten.overheid.nl/BWBR0013409/geldigheidsdatum_01-08-2014.

[35] Netherlands, Intelligence and Security Services Act 2002 (*Wet op de Inlichtingen en Veiligheidsdiensten 2002*), Article 43 in conjunction with Article 47, available at: http://wetten.overheid.nl/BWBR0013409/geldigheidsdatum_01-08-2014.

[36] Netherlands, Intelligence and Security Services Act 2002 (*Wet op de Inlichtingen en Veiligheidsdiensten 2002*), Article 34, available at: http://wetten.overheid.nl/BWBR0013409/geldigheidsdatum_01-08-2014

[37] Netherlands, Intelligence and Security Services Act 2002 (*Wet op de Inlichtingen en Veiligheidsdiensten 2002*), Article 34, paragraphs 1 and 2,

data are incorrect or are being analysed without justification, they will be amended or removed.[38]

[10]. The Data Protection Authority is not competent in the area of any of the activities of AIVD or MIVD.[39]

Remedies available

[11]. As to remedies, everyone has the right to file a complaint at the National Ombudsman (*Nationale Ombudsman*) about the acts or alleged acts of the Ministers involved or the services. The individual concerned will first have to inform the Minister involved about his or her complaint, enabling him or her to give his or her views. The Minister will ask for advice from the Review Committee on the Intelligence and Security Services.[40] It should be borne in mind, however, that individuals do not have access to any data during their collection, analysis and storage. Only after they have been processed can they inspect personal data and suggest improvements or deletion, so that, in practice, it is possible to file a well-founded complaint at this stage only. Moreover, the judgements of the National Ombudsman only address the questions of whether the services have acted correctly or not and whether they have acted in line with the proper conduct criteria applicable to all Dutch government institutions. The judgements are not binding.

[12]. Individuals may also turn to the courts, especially in view of the respect of private life.[41] Here, too, this only seems to make sense once data have been processed. A case in 2011 showed that the services need not answer the question whether current personal data are being processed. If this should have been the case, secrecy, in the interest of national security, would be an illusion, the Court argued. It seems, therefore, that national security, the main purpose of the services, for the interest of which investigations take place, prevails over the right to inspect personal data. In the case of non-current data the court is more lenient. Even if the individual has only played a minor part in an investigation, he has the right of inspecting the data. Although the courts may, in theory, judge in full every act of the services during every stage of surveillance, this has not led to any significant case law for the benefit of individuals so far. [42]

---

[38] Netherlands, Intelligence and Security Services Act 2002 (*Wet op de Inlichtingen en Veiligheidsdiensten 2002*), Article 43, paragraph 2, in conjunction with article 49, available at: http://wetten.overheid.nl/BWBR0013409/geldigheidsdatum_01-08-2014.

[39] Netherlands, Data Protection Act (*Wet Bescherming Persoonsgegevens*), Article 2, paragraph 2, under 2.

[40] Netherlands, Intelligence and Security Services Act 2002 (*Wet op de Inlichtingen en Veiligheidsdiensten 2002*), Article 83, in conjunction with General Administrative Law Act (*Algemene Wet Bestuursrecht*), part 9.1.3.

[41] Netherlands, Intelligence and Security Services Act 2002 (*Wet op de Inlichtingen en Veiligheidsdiensten 2002*), Article 55, paragraph 2, under e in conjunction with the Constitution (*Grondwet*), Article 10, paragraph 1.

[42] Netherlands, District Court of The Hague (*Rechtbank Den Haag*) (2011), case number ECLI:NL:RBSGR:2011:BP4872, 16 February 2011, available at: http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBSGR:2011:BP4872.

Annex 1 – Legal Framework relating to mass surveillance

A- Details on legal basis providing for mass surveillance

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
Wet op de inlichtingen- en veiligheidsdiensten 2002 (Intelligence and Security Services Act 2002; hereinafter: Wiv).	Special powers such as interception can only be used for the tasks defined in article 6/2/a and d (For the AIVD)- this means it can only be targeted against a narrowly defined group of individuals. Untargeted interception inherently incorporates communications	**Persons that are suspected to be a threat** Persons that, due to the aims that they try to achieve, or due to their activities, give rise to the serious suspicion that they form a threat for the continuation of the rule of law, for security or for other important interests of the state (Article 6,	**National security, law and order** By the General Intelligence and Security Service (hereinafter: AIVD): Protection of the continuation of the rule of law, security, other important interests of the state, including the safeguard of data the secrecy of which is	**Powers can in principle only be executed after previous approval by Ministers involved; approval must in principle be renewed every three months** Powers can only be executed on the condition that the responsible Minister, or the head of the service involved, on behalf of the Minister, gives his or her	**Collection: intercepting targeted cable-bound communication. Intercepting communication which is not cable-bound. Collecting information about users from providers. Analysis: further details about the target/keywords which are used in the search must be approved of by Minister in**	**Surveillance may in principle take place for any period of time, non-cable bound data may be gathered, irrespective where they come from** Surveillance may take place for any period of time, as permission, if required, may be granted time and again (every three months, in	**Cooperation with services abroad takes place and non cable-bound communication from abroad is surveyed. It is assumed that stipulations about cable-bound communication also apply to communication abroad, although this is not laid down in**

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
	of a larger group. There is no definition for this category, there is also no article in the law that distincts between nationals and non-nationals.	paragraph a and d, Wiv)	necessary on the basis of national security of those parts of the government service and industry which are, according to the Ministers involved, of vital interest for keeping social life intact (Article 6, paragraph 2,under a and d, Wiv). By the Military Intelligence and Security Service (hereinafter:	prior approval. The head of the service may appoint in writing civil servants who are under his or her authority to give approval on behalf of him or her. The responsible Minister will get a copy of the decision (Article 19, paragraphs 1 and 2, Wiv).The approval will in principle be granted for a period of three months at most and be continued for the	**advance. Storage: in principle, data may be kept for no longer than a year, unless processed in more detail. Destruction: data which have lost their significance shall be destroyed.** <u>Processing data in general:</u> Processing data only takes place with a certain purpose and only in so far as required for a good implementation of the Wiv (Article 12,	principle; Article 19, paragraph 3, Wiv). Geographical scope: The services have the power to receive and record with the help of a technical device telecommunicati on which is not cable-bound and which has its origin or destination in other countries,	**the Wiv.**[43] Technical and other forms of support may be given in so far as the interest of intelligence and security services of other countries that may be taken into account apply. This should only take place in so far as their interests are not in conflict with the interests at stake for the Dutch services and the proper

[43] Netherlands, Commissie evaluatie Wiv 2002 (2013), Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen, available at: www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2013/12/02/rapport-evaluatie-wet-op-de-inlichtingen-en-veiligheidsdiensten-2002/rapport-evaluatie-wet-op-de-inlichtingen-en-veiligheidsdiensten-2002.pdf, p. 44.

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
			MIVD): the correct structure and efficient use of the armed forces (Article 7, paragraph 2, under a1, Wiv); the prevention of activities which aim to damage the security or readiness of the armed forces, promotion of a correct course of the mobilization and concentration of the armed forces, an undisturbed preparation and use of the armed forces, in connection with the maintenance and the	same period at a request to this effect (Article 19, paragraph 3, Wiv). The services have the power to tap, receive, record and listen in to each form of conversation, telecommunication or transfer of data by means of an automated work (for example, a telephone or a computer) with the help of a technical device, irrespective of where it takes place. They also have the power to break the code of the conversations, telecommunication	paragraphs 1 and 2, Wiv) Processing personal data by the AIVD can only take place with reference to specific persons (Article 13, paragraph 1, Wiv). The same goes for the processing of personal data by the MIVD (Article 13, paragraph 2, Wiv). Collecting data: Data may be collected from government bodies, civil servants and, furthermore, anyone who may be deemed to be able to supply the necessary data; and from the person responsible for processing data	on the basis of a technical characteristic in order to explore the communication. The services have the power to take notice of the data received. They may also break the code of the telecommunicati on. Other limits: No other limits, except the ones mentioned in the context of approval (the nature of the data: there should be a target –	execution of their tasks (Article 59, Wiv). Moreover, The services have the power to tap, receive, record and listen in to each form of conversation, telecommunicati on or transfer of data by means of an automated work (for example, a telephone or a computer) with the help of a technical device, irrespective of where it takes place. They also have the power to decode the

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
			promotion of the international rule of law in so far as the armed forces are involved or may be involved, according to the expectations (Article 7, paragraph 2, under c, in conjunction with Article 7, paragraph 2, under a2, Wiv). In connection to the above, the promotion of measures which protect these interests, including measures to safeguard data about the armed forces the secrecy	or transfer of data. This power may only be exercised on approval by the Minister involved to the head of the division, upon his or her request. When the MIVD exercises this power, it is only allowed if approval has been given in agreement with the Minister of the Interior and Kingdom Relations, in so far as this power is not exercised in or with places, used by the Ministry of Defence (for example, aircraft carriers). The request for	(Article 17, paragraph 1, Wiv). Data may be tapped, received, recorded and listened in to in the context of each form of conversation, telecommunication or transfer of data by means of an automated work (for example, a telephone or a computer) with the help of a technical device, irrespective of where it takes place. The code may be broken of the conversations, telecommunication or transfer of data. This may only take place on approval by the Minister	Article 25, Wiv) and they may not be cable-bound – Article 26, Wiv); activities are often subject to approval.	conversations, telecommunication or transfer of data (Article25, paragraph 1, Wiv). The services have the power to receive and record with the help of a technical device telecommunication which is not cable-bound and which has its origin or destination in other countries, on the basis of a technical characteristic in order to explore the communication.

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
			of which is necessary (Article 7, paragraph 2, under e, Wiv). The principles of necessity, proportionality and subsidiarity are laid down as a condition for the use of these methods in Articles 18, 31 and 32.	approval includes at least information about the power the services wish to carry out, and, in so far as this applies, it also includes information about the number, referred to in article 1.1., under bb of the Telecommunication Act ("number: ciphers, letters or other symbols, whether or not in combination, which are designed to give access to or identify users, network exploiters, services, network connections or other network elements", for	involved granted to the head of the division, upon his or her request. When the MIVD exercises this power, it is only allowed if approval has been given in agreement with the Minister of the Interior and Kingdom Relations, in so far as this power is not exercised in or with places, used by the Ministry of Defence. The request for approval includes at least information about the power the services wish to carry out, and, in so far as this applies, it includes information on the number,		The services have the power to take notice of the data received. They may also eliminate the coding of the telecommunication (Article 26, paragraph 1, Wiv).

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
				example, telephone number or IP address); data on the identity of the person or the organisation concerned; the reasons for the request. If the number is not known yet, approval will only be granted on the condition that the power may only be executed when the number concerned is known. If the information about the identity is not known yet, approval is only granted on the condition that the information concerned is added	meant in article 1.1., under bb of the Telecommunication Act (for example, telephone number or IP address); data on the identity of the person or the organisation concerned; the reasons for the request. If the number is not known yet, approval will only be granted on the condition that the power may only be executed when the number concerned is known. If the information about the identity is not known yet, approval is only granted on the condition that the information		

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
				as soon as possible. (Article 25, paragraphs 1 u/i 6, Wiv). The services have the power to receive and record with the help of a technical device non cable-bound telecommunication and which has its origin or destination in other countries, on the basis of a technical characteristic in order to explore the communication. The services have the power to take notice of the data received. They may also break the code of the	concerned is added as soon as possible. (Article 25, paragraphs 1 u/i 6, Wiv). A request for approval need not be made in the case of telecommunication being received and recorded in a targeted way, this telecommunication not being cable-bound and having its origin or destination in other countries, on the basis of a technical characteristic. In so far as this telecommunication refers to a military transfer of data no approval is required at all (Article 25,		

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
				telecommunication. No approval is necessary for these activities. As soon as the identity of the person or the organisation from whom the telecommunication has its origin has been determined, a request for approval from the Minister is filed within two days, if the reception and recording of the telecommunication is necessary for a proper execution of the tasks of the service. Until approval, no further investigation is made into the recorded	paragraph 8, Wiv). Data may be received and recorded with the help of a technical device in the context of non cable-bound telecommunication which has its origin or destination in other countries, on the basis of a technical characteristic in order to explore the communication (i.e. foreign communication with a user in the Netherlands). The data received may be taken notice of. A possible code may be broken. No approval is		

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
				telecommunication. If reception and recording is not necessary, the data will immediately be destroyed. (Article 26, paragraphs 1 u/i 5, Wiv). The data thus collected may be selected by the services on the basis of a. information on the identity of a person or an organisation; b. a number as meant in Article 1.1., under bb of the Telecommunication Act (for example, telephone number or IP address), or any technical	necessary. As soon as the identity of the person or the organisation from whom the telecommunication has its origin has been determined, a request for approval from the Minister is filed within two days, if the reception and recording of the telecommunication is necessary for a proper execution of the tasks of the service. Until approval, no further investigation is made into the recorded telecommunication. If reception and recording is not necessary, the data will immediately be		

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
				characteristic; c. keywords related to a subject which is described in more detail. The approval for this selection will be given by the Minister involved for a period of three months at most and it may be prolonged time and again at a request to that effect. The request to grant this approval comprises at least: the information on the basis of which the selection will take place and the reason why the selection will take	destroyed. (Article 26, paragraphs 1 u/i 5, Wiv). Data may be received and recorded, without there being a specific target, in the context of telecommunication which is not cable-bound, with the aid of a technical device (i.e. no foreign actors need to be involved). The code of the telecommunication may be broken. No prior approval is necessary (Article 27, paragraphs 1 and 2, Wiv). Data about a user		

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
				place. The approval for the selection on the basis of the keywords will be given by the Minister involved for a period of one year at most and it may be prolonged time and again. The request for the approval will at least comprise a detailed description of the subject and the reason why the selection has to be made. As to the determination of the keywords Article 19 Wiv applies: powers can	and the telecommunication traffic as to that user may be requested from providers of public telecommunication networks and public telecommunication services in the sense of the Telecommunication Act. The request may only refer to data which have been laid down in a government order and may refer to both data which have been processed at the time of the request and data which after the moment of the request will be processed. No prior approval is		

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
				only be carried out on the condition that the responsible Minister, or the head of the service involved, on behalf of the Minister, gives his or her prior approval. The head of the division may appoint in writing civil servants who are under his or her authority to give approval on behalf of him or her. The responsible Minister will get a copy of the decision (Article 19, paragraphs 1 and 2, Wiv). The approval will in principle be granted for a period of a	necessary. The request will be made in writing and comprise: the number, meant in Article 1.1., under t, of the Telecommunication Act, or data referring to the name, the place of residence of the person or the seat of the organisation to whom or which the number belongs; the data which should be supplied, and the period which the data cover (Article 28, paragraphs 1u/i 4, Wiv) Data on the name, address, ZIP-code, place of residence,		

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
				year at most and be continued for the same period at a request to this effect (Article 19, paragraph 3 in conjunction with Article 27, paragraph 6, Wiv – difference in time limit).(Article 27, paragraphs 1 u/i 6, Wiv)	number and sort of service of a user of telecommunication may be requested from the providers of public telecommunication networks and public telecommunication services in the sense of the Telecommunication Act. A user is defined as the natural person or legal person who has entered into an agreement with the provider as to the use of a public telecommunication network or a public telecommunication service, just as the natural person or		

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
					legal person that actually makes use of a public telecommunication network or a public telecommunication network. No prior approval is necessary when requests are made to these parties to supply information about users. (Article 28, paragraphs 1 u/i 4, Wiv). If the data in question are not known to the provider and they are necessary (Article 25 and 28, Wiv), the service may ask the provider to trace and supply the data		

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
					requested. The services have the power to use a technical device with the help of which the number can be retrieved. (Article 29, paragraphs 1 u/i 3 and 5, Wiv) <u>Analysing data:</u> In the case of non cable-bound communication: The data thus collected may be selected by the services on the basis of a. information on the identity of a person or an organisation; b. a number as meant in Article 1.1., under bb		

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
					of the Telecommunication Act (for example, telephone number or IP address), or any technical characteristic; c. keywords related to a subject which is described in more detail. The approval for this selection will be given by the Minister involved for a period of three months at most and it may be prolonged time and again at a request to that effect. The request to grant this approval comprises at least: the information on the basis of which		

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
					the selection will take place and the reason why the selection will take place. As to the determination of the keywords, Article 19 Wiv applies: powers can only be carried out on the condition that the responsible Minister, or the head of the service involved, on behalf of the Minister, gives his or her prior approval. The head of the service may appoint in writing civil servants who are under his or her authority to give approval on behalf of him or her. The		

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
					responsible Minister will get a copy of the decision (Article 19, paragraphs 1 and 2, Wiv). The approval will in principle be granted for a period of a year at most and be continued for the same period at a request to this effect (Article 19, paragraph 3 in conjunction with Article 27, paragraph 6 Wiv – difference in time limit).(Article 27, paragraphs 1 u/i 6, Wiv). <u>Storing data:</u> As to non-cable bound communication: as far they have not		

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
					been selected, data may be kept for a period of one year at most for the benefit of further selection, in the sense that this selection may only take place in the context of an investigation by service on the basis of a reason determined for a selection, or in the context of a subject which has been described and for which at the moment of reception and recording of the data in question approval had been granted; and in the sense that keeping these data is urgently required for a good exercise of		

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
					the investigation in question. This also goes for data the decoding of which has not taken place yet, in the sense that the period of one year only starts at the moment that the decoding has taken place (Article 27, paragraphs 9 and 10, Wiv). <u>Destruction of data</u>: If receiving and recording non cable-bound telecommunication, having its origin of destination in other countries, is not required for the efficient conduct of their tasks by the		

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
					services, the data recorded shall be destroyed immediately (Article 26, paragraph 1 in conjunction with 5, Wiv) The data which have lost their significance, in view of the aim for which they are processed, shall be removed. If it turns out that the data are processed without justification they shall be improved or be removed. The Minister involved shall inform those to whom he has supplied the data in question as soon as possible. The data		

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
					removed shall be destroyed, unless legal stipulations about storage are in conflict with this. If someone has made a request whether and if yes, which data referring to him or her have been processed by or for the benefit of a service, the destruction of these data shall be postponed until at least the moment the request has been decided upon irrevocably. In so far as the request to inspect the data has been granted, the data shall not be destroyed before the		

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
					moment they have been taken notice of. (Article 43 in conjunction with Article 47 Wiv). Precautions to be taken when communicating data to other parties: The services have the power, in the context of a good execution of their tasks, to inform about or for the benefit of the data processed by the service: the Ministers involved, other government bodies involved, other persons or institutions involved, the intelligence and		

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
					security services of other countries that may be taken into account, and other international security, liaison and intelligence bodies that may be taken into account. The Minister shall supply such information, if the nature of the information gives rise to this. The power to give information processed by the services is limited to the cases laid down in the Wiv. (Article 36, paragraphs 1 u/i 3, Wiv) Information about		

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
					personal data is supplied by the Minister involved or on behalf of the head of the division in writing, if the person or institution that is informed has the power to take measures on the basis of the information supplied. In urgent cases the information may take place verbally. It has to be confirmed in writing as soon as possible. The person or institution may inspect the data underlying the information, but must in principle keep them secret (Article 40, in		

Name and type of the mass surveillance-related law	A definition of the categories of individuals liable to be subjected to such surveillance	Nature of circumstances which may give rise to surveillance	List purposes for which surveillance can be carried out	Previous approval / need for a warrant	List key steps to be followed in the course of surveillance	Time limits, geographical scope and other limits of mass surveillance as provided for by the law	Is the law allowing for mass surveillance in another country (EU MS or third countries)?
					conjunction with Articles 85 and 86, Wiv).		

B- Details on the law providing privacy and data protection safeguards against mass surveillance

Please, list law(s) providing for the protection of privacy and data protection against unlawful surveillance	**List specific privacy and data protection safeguards put in place by this law(s)**	**Indicate whether rules on protection of privacy and data protection apply:** **only to nationals or also to EU citizens and/or third country nationals**	**Indicate whether rules on protection of privacy and data protection apply:** **only inside the country, or also outside (including differentiation if EU or outside EU)**

Netherlands, Constitution (*Grondwet)*, Article 10, paragraphs 2 and 3	The law lays down stipulations to protect private life in connection with recording and supplying personal data. The law lays down stipulations concerning the rights of persons to inspect data referring to them which have been recorded, and pertaining to their use, as well as the improvement of such data.	Constitution covers everyone in the Netherlands.	The Constitution is Dutch and applies only inside the country.
Data Protection Act, Article 2, paragraph 2, under b	This Act does not apply to the processing of personal data by or for the benefit of the intelligence and security services.	This Act covers everyone in the Netherlands.	This Act is a national Act and therefore in principle only applies within the jurisdiction of the country. There are no details about Member States or states outside the EU.
Wiv, Article 47, paragraphs 1 and 2	Everyone who makes a request to be informed will be informed by the Minister involved as soon as possible, but at most within three months, whether, and if yes which, personal data that concern him were processed by or for the benefit of a service. In so far a request is granted, the Minister involved will give the applicant the opportunity to inspect his or her data as soon as possible, but at most within four weeks of the moment that the decision was announced (Article 47, paragraphs 1 and 2, Wiv)	This Act covers every individual, natural person who may be identified or has been identified. (Article 1, under e, Wiv, in conjunction with Article 47, paragraph 1, Wiv)	The Wiv is a national Act and therefore in principle only applies within the jurisdiction of the country. There are no details about Member States or states outside the EU.
Wiv, Article 50, paragraph 1	Article 47 applies accordingly to a request about personal data that have been processed by or for the	Spouse etc. of everyone (Article 50, Wiv), regardless of nationality	The Wiv is a national Act and therefore in principle only applies within the jurisdiction of the country.

	benefit of a service on a deceased spouse, registered partner, child or parent of the applicant.		There are no details about Member States or states outside the EU
Wiv, Articles 53- 56	Grounds for refusal and limitations: a request will be rejected if data concerning the applicant have been processed in the context of any investigation, unless the data were processed more than five years ago; unless since that time no new data concerning him have been processed in this context; unless the data in question are not relevant for any current investigation. The request will also be rejected if no data concerning the applicant have been processed. If a request is thus rejected, the reasons will only be put in general terms.	Applicant may be "everyone" (Article 43, paragraph 1, Wiv)	The Wiv is a national Act and therefore in principle only applies within the jurisdiction of the country. There are no details about Member States or states outside the EU
Wiv, Article 34	In the case of targeted tapping, receiving, recording and listening in to any form of a conversation, telecommunication or transfer of data by means of an automated work (for example, a telephone or a computer) (Article 25, Wiv) or receiving and recording telecommunication which is not cable-bound without a target, whereby data are being selected, among other things, on the basis of	This Act covers every individual, natural person who may be identified or has been identified. (Article 1, under e, Wiv, in conjunction with Article 47, paragraph 1, Wiv): person involved could be anyone.	The Wiv is a national Act and therefore only applies within the jurisdiction of the country. There are no details about Member States or states outside the EU

	identity, a number as referred to in the Telecommunication Act, or any technical characteristic, or a subject based on key words, the following applies (Articles 25, paragraph 1 Wiv and Article 27, paragraph 1 under a and b, Wiv). The involved Minister shall investigate, five years after the exercise of these powers, and after that every year again, whether a report may be issued to the person involved. If this is possible, this will happen as soon as possible. If this is not possible the Review Committee on the Intelligence and Security Services will be informed. Reasons will be given. Issuing a report is not necessary if this is not reasonably possible (Article 34, paragraphs 1 u/i 3, Wiv). The report will be postponed if personal data in an investigation are involved in connection with which a person would not at his or her request get any information either (Article 34, paragraph 6, Wiv in connection with Article 47 and 53, Wiv). The duty to investigate the possibility to issue a report will not be necessary if issuing a report about the exercise of powers is		

	reasonably expected to reveal sources of a service, among which intelligence and security services of other countries, seriously damage relations with other countries and with international organisations or reveal a specific application of a method of a service or the identity of the one who has been helpful to the service (Article 35, paragraph 7, Wiv).		
Article 8:1 of the General Administrative Law Act (Algemene wet bestuursrecht)	An interested party may turn to the court to appeal against a decision taken by, in this case, the Intelligence and Security Services (for example, refusal to inspect data).	This Act applies to any interested party.	The General Administrative Law Act is a national Act and therefore only applies within the jurisdiction of the country. There are no details about Member States or states outside the EU

Annex 2 – Oversight bodies and mechanisms[44]

Name of the body/mechanism	Type of the body/mechanism	Legal basis	Type of oversight	Staff	Powers
in English as well as in national language	*e.g. parliamentary, executive/government, judicial, etc.*	*name of the relevant law, incl. specific provision*	*ex ante / ex post / both/ during the surveillance/etc. as well as whether such oversight is ongoining/regularly repeated*	*including the method of appointment of the head of such body **AND** indicate a total number of staff (total number of supporting staff as well as a total number of governing/managing staff) of such body*	*e.g. issuing legally binding or non-binding decisions, recommendations, reporting obligation to the parliament, etc.*
Review Committee on the Intelligence and Security Services – Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten	Independent	Article 64, Wiv	Ongoing	Three members, appointed by Royal Decree, after having been proposed by the Ministers involved (Article 65, paragraph 2). At least two members, among whom the president, should have the Bachelor and Masters degree in the field of law, or they should have a PhD in law of the right to used the title LLM (Article 65,	The Ministers involved, the heads of the services, the coordinator and everyone who is involved in the execution of the Wiv shall, at the request of the Review Committee on the Intelligence and Security Services, provide all information and further cooperation. If requested, the Review Committee on

[44] Overall, the situation still is the same as in 2011 when an EP-report was published (Wills, A. & Vermeulen, M. (2011), Parliamentary oversight of security and intelligence agencies in the EU, Brussels, European Parliament, available at: (http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf). However, there are discussions to change the Wiv in the sense that the services will get more powers and there will be more checks and balances. E-mail correspondence with the Review Committee on the Intelligence and Security Services, 4 September and 9 September 2014.

				paragraph 4, Wiv). These members should swear or promise that they have not directly or indirectly given or promised someone something, and that they moreover have not received or will receive any gift directly or indirectly from anyone in order to perform a certain act in their service. They will swear or promise to be loyal to the Constitution. They must have the Dutch nationality. They do not perform any functions the execution of which is undesirable in view of a good performance of their function or in view of their impartiality and independence or any trust therein (Article 65, paragraphs 4 u/i 7, Wiv). There are three members on the Committee, a professional secretary and five researchers, and an administrative secretary.[45]	the Intelligence and Security Services shall have direct access to all information processed in the context of the execution of this Act. The Committee may also ask anyone involved to appear as a witness or expert in order to give information. The duty to appear does not apply to the Ministers involved. When a Minister does not appear, he or she will have himself or herself represented (Article 74, paragraphs 1, 3 and 4, Wiv). The Review Committee on the Intelligence and Security Services has the power to assign certain activities to experts (Article 76, paragraph 1). This means that these experts are able to investigate the activities of the intelligence services on the basis of their own expertise, not available to

[45] Netherlands, Review Committee on the Intelligence and Security Services (*Commissie van Toezicht betreffende de Inlichtingen en VeiligheidsDiensten*) (2014), *Over de CTIVD,* website, available at: www.ctivd.nl/?Over_de_CTIVD, accessed on 7 August 2014.

				Apart from the latter all are lawyers. The number of staff has increased since the 2011 EP report was published. In 2011, there were four researchers. [46]	the Committee itself. The Review Committee on the Intelligence and Security Services has the power to carry out investigations into the activities covered by the Wiv (Article 78, paragraph 1). It may also carry out investigations at the request of one of the Houses of Parliament (Article 78, paragraph 2). The Review Committee on the Intelligence and Security Services writes, on the basis of its investigation, a supervisory report. This is public, apart from information about means used by the services in specific matters, secret sources, and the current level of knowledge of the services (Article 79, paragraph 1, in conjunction with Article 8, paragraph 3, Wiv). On the basis of its findings, the Review Committee on the

[46] Wills, A. & Vermeulen, M. (2011), *Parliamentary oversight of security and intelligence agencies in the EU*, Brussels, European Parliament, available at: http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf, p. 256.

					Intelligence and Security Services may make recommendations to the Minister involved (Article 79, paragraph 3, Wiv). The Committee sends a report about its activities to both Houses of Parliament and the Ministers involved every year before 1 May (Article 80, paragraph 1, Wiv). Some information (see above) is kept secret.
Judiciary, Court or Court of Appeal, Supreme Court or Council of State, – rechterlijke macht, Gerecht of het Hof, Hoge Raad of Raad van State	Judicial	Article 87, Wiv In public law legal procedures before a court, if the Minister involved or the Review Committee on the Intelligence and Security Services are required to sub mit information or documents, they may inform the court or the court of appeal that only they may take notice	Ongoing oversight, no limits (Article 87, Wiv)	All judges are appointed for life by Royal Decree on the basis of their independence and integrity, after having been proposed by the Minister of Security and Justice (Act on the Legal Position of Civil Servants in the Judiciary – Wet rechtspositie rechterlijke ambtenaren, Article 2, paragraph 1). 1771 judges work for the District Courts, supported by 6444 civil servants within the judiciary. Distributed among these two groups are 430 managers. 594 judges work for the	Judges pronounce legally binding judgements.

		of the information or the documents. The court can then only pronounce judgement with the approval of the other parties on the basis of that information or those documents. If the Minister involved or the Review Committee on the Intelligence and Security Services refuses to submit (no reasons have to be given) the information or the documents, the courts may draw their conclusions in the way they think they are		Courts of Appeal, supported by 921 civil servants. Among these two groups, there are 81 managers. Not all of the staff work fulltime: there are about 10 per cent less fulltime positions than these figures indicate. No details are available about the Supreme Court. .[47]	

[47] E-mail correspondence with the National Service Desk of the Judiciary (Landelijk Dienstencentrum voor de Rechtspraak), 5 August 2014.

		appropriate. If documents have to be submitted, it is sufficient if they may only be inspected. No copies may be made.			

National Ombudsman (Nationale Ombudsman)	Semi-judicial	Everyone has the right to complain to the National Ombudsman about the activies or alleged activities of the Ministers involved, the heads of the services, the coordinator and the persons employed for the services (Article 83, paragraph 1, Wiv).	Ongoing oversight	The Lower House of Parliament appoints the National Ombudsman on the basis of independence and integrity after a recommendation having been drawn up by the vice president of the Council of State, the president of the Supreme Court and the president of the General Audit Office, consisting of the names of at least three persons (Article 2, paragraph 2, Act on the National Ombudsman). In 2013 there was an average staff of 147 working for the National Ombudsman.[48]	Non-binding judgements
Minister of the Interior and Kingdom Relations – Minister van Binnenlandse Zaken en	Executive/government	Wiv, Article 1, under c, sub 1	Ongoing oversight	Appointed by Royal Decree, after having been proposed by political parties after the elections. Some staff dealing with financial and economic affairs have as one of their tasks to deal with the General	The Ministers involved send a public report to both Houses of Parliament at the same time annually before 1May about the way in which the AIVD and MIVD performed their

[48] Netherlands, National Ombudsman (*Nationale Ombudsman*) (2014), Verslag van de Nationale Ombudsman over 2013, The Hague, National Ombudsman, available at: http://jaarverslag.nationaleombudsman.nl/sites/default/files/Verslag%202013.pdf.

Koninkrijkrelaties				Intellligence and Security Service; the same goes for legislative staff working on constitutional affairs and legislation. The focus of the powers lies with the Secretary General of the Ministry of the Interior and Kingdom Relations. He or she is supported by four fulltime policymakers and advisors (used to be two of them).[49]	tasks in the previous year (Article 8, paragraph 1), , not including information about means used by the services in specific matters, secret sources, and the current level of knowledge of the services (Article 79, paragraph 1, in conjunction with Article 8, paragraph 3, Wiv). The Minister involved may give this information in confidence (Article 8, paragraph 4, Wiv). If there is a reason for this, the Ministers involved will inform both Houses of Parliament at their own initiative (Article 8, paragraph 5, Wiv).
Minister of Defence – Minister van Defensie	Executive/government	Wiv, Article 1, under c, sub 2	Ongoing oversight	Appointed by Royal Decree, after having been proposed by political parties after the elections. The Military Intelligence and Security Service is supervised directly by the Secretary General of the Ministry of Defence. The whole of this service is employed by the	The Ministers involved send a public report to both Houses of Parliament at the same time annually before 1May about the way in which the AIVD and MIVD performed their tasks in the previous year (Article 8, paragraph 1, Wiv), not including

[49] E-mail correspondence dated 24 September 2014 from the Ministry of the Interior and Kingdom Relations.

				Ministry of Defence. There are no intermediate layers.[50]	information about means used by the services in specific matters, secret sources, and the current level of knowledge of the services (Article 79, paragraph 1, in conjunction with Article 8, paragraph 3, Wiv). The Minister involved may give this information in confidence (Article 8, paragraph 4, Wiv). If there is a reason for this, the Ministers involved will inform both Houses of Parliament at their own initiative (Article 8, paragraph 5, Wiv).
Prime Minister, Minister of General Affairs - Minister-President, Minister van Algemene Zaken	Executive/governmen t	Wiv, Article 1, under b and c, sub 3, in conjunction with Article 4	Ongoing oversight	The Prime Minister is a so-called cordinator and as such appointed by Royal Decree after having been proposed by the Minister of the Interior and Kingdom Relations and the Minister of Defence (Article 4, paragraphs 1 and 2,Wiv). There are a specific coordinator and an advisor	The Prime Minister informs the Ministers involved of everything that may be of importance in the context of surveillance in the field of intelligence and security (Article 4, paragraph 4, Wiv). They will have to take this information into account.

[50] E-mail correspondence dated 24 September 2014 from the Ministry of Defence.

				about the Wiv.[51]f.	
Both Houses of Parliament, in particular the Commission for the Intelligence and Security Services (Commissie voor de Inlichtingen en Veiligheidsdiensten)	Parliamentary	Ongoing, regularly repeated		75 MPs (Upper House of Parliament) are elected by the representatives of the Dutch in the various districts of the Netherlands. Hundreds of staff. 150 MPs (Lower House of Parliament) are directly elected by the population. Hundreds of staff. The Commission exercises parliamentary control in connection with the secret aspects of government policies in the framework of the AIVD and the MIVD. All political parties in Parliament are represented by their leaders (eleven).[52]	The Ministers involved send a public report to both Houses of Parliament at the same time annually before 1May about the way in which the AIVD and MIVD performed their tasks in the previous year (Article 8, paragraph 1, Wiv), apart from information about means used by the services in specific matters, secret sources, and the current level of knowledge of the services (Article 79, paragraph 1, in conjunction with Article 8, paragraph 3, Wiv). The Minister involved may give this information in confidence (Article 8, paragraph 4, Wiv). If there is a reason

[51] E-mail correspondence dated 15 September 2014 from the Ministry of General Affairs.

[52] Netherlands, House of Representatives (*Tweede Kamer der Staten Generaal*)(2014), 'Commissie voor de Inlichtingen- en Veiligheidsdiensten', Web page, available at: http://www.tweedekamer.nl/kamerleden/commissies/IV/index.jsp, accessed on 9 September 2014

					for this, the Ministers involved will inform both Houses of Parliament at their own initiative (Article 8, paragraph 5, Wiv). The Review Committee on the Intelligence and Security Services sends a report about its activities to both Houses of Parliament and the Ministers involved every year before 1 May (Article 80, paragraph 1). Some information (see above) is kept secret. The Commission for the Intelligence and Security Services meets about the secret aspects of government policies in the framework of the AIVD and MIVD in secret and annually reports to Parliament.[53]

[53] Netherlands, House of Representatives (*Tweede Kamer der Staten Generaal*)(2014), 'Commissie voor de Inlichtingen- en Veiligheidsdiensten', Web page, available at http://www.tweedekamer.nl/kamerleden/commissies/IV/index.jsp, 9 September 2014

Annex 3 – Remedies[54]

Intelligence and Security Services Act (*Wet op de inlichtingen- en veiligheidsdiensten, Wiv*)				
Stages of surveillance process	**Is the subject informed?**	**Does the subject have a right of access to the data collected on him/her?**	**List remedies available to an individual concerned**	**Legal basis for using the available remedies**
	Yes/No	*Yes/No, please provide details if needed*	*Please list the type of remedial action that can be taken: e.g.: claims lodged with court(s), claims lodged with the oversight body, request to the surveillance authority, etc.* ***AND*** *please specify also the name (e.g. Supreme Court) and type of the body (e.g. judicial, executive, parliamentary) providing such remedies.*	*Violation of data protection, private life, specific legislation, etc.*
Collection*	No	No, on the basis of Article 7, paragraph 1, Wiv, one can only inspect data which have been processed. Moreover, in practice one does not know about data in different stages, because no information is provided. One can therefore not	Everyone has the right to file a complaint at the National Ombudsman about the acts or alleged acts of the Ministers involved, the heads of the services, the coordinator, and the persons working	Article 83, Wiv, in conjunction with Part 9.1.3. of the General Administrative Law Act (Algemene wet bestuursrecht).

[54] In case of different remedial procedures please replicate the table for each legal regime.

* For the definitions of these terms, please refer to the FRA/CoE (2014), *Handbook on European data protection law*, Luxembourg, 2014, pp. 46-47, available at: http://fra.europa.eu/en/news/2014/council-europe-and-eu-fundamental-rights-agency-launch-handbook-european-data-protection

		file a well-founded complaint.	for the services and the coordinator. First, the complainant will inform the Ministers involved and enable him or her to give his or her views. The Minister will ask for advice from the Review Committee on the Intelligence and Security Services. Everyone can turn to the court (in the end the Supreme Court or the Council of State) in connection with the protection of the right to his or her private life.	Article 55, paragraph 2, under e, Wiv, in conjunction with Article 10, paragraph 1 of the Constitution.
Analysis*	No	No, on the basis of Article 7, paragraph 1, Wiv, one can only inspect data which have been processed. Moreover, in practice one does not know about data in different stages, because no information is provided. One can therefore not file a well-founded complaint.	Everyone has the right to file a complaint at the National Ombudsman about the acts or alleged acts of the Ministers involved, the heads of the services, the coordinator, and the persons working for the services and the coordinator. First, the complainant will inform the Ministers involved and enable him or her to give his or her views. The	Article 83, Wiv, in conjunction with Part 9.1.3. of the General Administrative Law Act (Algemene wet bestuursrecht).

			Minister will ask for advice from the Review Committee on the Intelligence and Security Services. Everyone can turn to the court (in the end the Supreme Court or the Council of State) in connection with the protection of the right to private life.	Article 55, paragraph 2, under e, Wiv, in conjunction with Article 10, paragraph 1 of the Constitution.
Storing*	No	No, on the basis of Article 7, paragraph 1, Wiv, one can only inspect data which have been processed. Moreover, in practice one does not know about data in different stages, because no information is provided. One can therefore not file a well-founded complaint.	Everyone has the right to file a complaint at the National Ombudsman about the acts or alleged acts of the Ministers involved, the heads of the services, the coordinator, and the persons working for the services and the coordinator. First, the complainant will inform the Ministers involved and enable him or her to give his or her views. The Minister will ask for advice from the Review Committee on the Intelligence and Security Services.	Article 83, Wiv, in conjunction with Part 9.1.3. of the General Administrative Law Act (Algemene wet bestuursrecht). Article 55, paragraph 2, under e, Wiv, in conjunction with Article 10, paragraph 1 of the Constitution.

			Everyone can turn to the court (in the end the Supreme Court or the Council of State) in connection with the protection of the right to his or her private life.	

Destruction *	No	Yes. The data which have lost their significance, in view of the aim for which they are processed, shall be removed. If it turns out that the data have been processed without justification they shall be improved or be removed. The Minister involved shall inform those to whom he has supplied the data in question as soon as possible. The data removed shall be destroyed, unless legal stipulations about storage are in conflict with this. If someone has made a request whether and if yes, which data referring to him or her have been processed by or for the benefit of a service, the destruction of these data shall be postponed until at least the moment the request has been decided upon irrevocably. In so far as the request to inspect the data has been granted, the data shall not be destroyed before the moment they have been taken notice of.(Article 43 in conjunction with Article 47, Wiv).	Everyone has the right to file a complaint at the National Ombudsman about the acts or alleged acts of the Ministers involved, the heads of the services, the coordinator, and the persons working for the services and the coordinator. First, the complainant will inform the Ministers involved and enable him or her to give his or her views. The Minister will ask for advice from the Review Committee on the Intelligence and Security Services. Everyone can turn to the court (in the end the Supreme Court or the Council of State) in connection with the protection of the right to his or her private life.	Article 83, Wiv, in conjunction with Part 9.1.3. of the General Administrative Law Act (Algemene wet bestuursrecht). Article 55, paragraph 2, under e, Wiv, in conjunction with Article 10, paragraph 1 of the Constitution.

After the whole surveillance process has ended	**Yes. Five years after the services have used their powers a Minister shall investigate whether he or she can issue a report to the person involved.** There are two situations possible. The services have with the aid of a technical device tapped, received, recorded or listened in to any form of conversation, telecommunication or transfer of data by means of an automated work (for example, a telephone or a	Everyone who makes a request to be informed will be informed by the Minister involved as soon as possible, but at most within three months, whether, and if yes which, personal data that concern him were processed by or for the benefit of a service. In so far as a request is granted, the Minister involved will give the applicant the opportunity to inspect his or her data as soon as possible, but within four weeks of the moment that the decision was announced at the latest (Article 47, paragraphs 1 and 2, Wiv). Article 47 applies accordingly to a request about personal data that have been processed by or for the benefit of a service about a deceased spouse, registered partner, child or parent of the applicant (Article 50, paragraph 1, Wiv). The Minister involved informs everyone at his or her request as soon as possible, but within three months at the latest, whether data may be inspected, other than personal data, about a government issue (Article 51, paragraph 1, Wiv). In the case of personal data a request will be rejected in the following case: if data concerning the applicant have been	Everyone has the right to file a complaint at the National Ombudsman about the acts or alleged acts of the Ministers involved, the heads of the services, the coordinator, and the persons working for the services and the coordinator. First, the complainant will inform the Ministers involved and enable him or her to give his or her views. The Minister will ask for advice from the Review Committee on the Intelligence and Security Services. National Ombudsman is a semi-judicial body.	Article 83, Wiv, in conjunction with Part 9.1.3. of the General Administrative Law Act (Algemene wet bestuursrecht). Article 55, paragraph 2, under e, Wiv, in conjunction with Article 10, paragraph 1 of the Constitution.

	computer). The second situation is that the services have selected data, which have been collected by receiving and recording non-cable-bound telecommunication with the aid of a technical device without target and they have selected these data on the basis of information concerning the identity of a person or an organisation, or on the basis of a number as referred to in Article 1.1., under bb of the Telecommunication Act (for example, telephone	processed in the context of any investigation, unless the data were processed more than five years ago; or unless since that time no new data concerning him or her have been processed in this context; or unless the data in question are not relevant for any current investigation. The request will also be rejected if no data concerning the applicant have been processed. If a request is thus rejected, the reasons will only be put in general terms. In a number of cases information about data on government issues will be rejected, such as in the case of national security and in as far as provision of the data does not outweigh interests such as economic or financial interests of the state (Article 55 Wiv).	Everyone can turn to the court (in the end the Supreme Court or the Council of State) in connection with the protection of the right to his or her private life. Judicial body.	

	number or IP address). In these two cases the Minister involved shall investigate five years after ending the process, and after that once a year, whether he or she can issue a report to the person involved. If possible, this will happen as soon as possible. If a report is not possible, the Review Committee on the Intelligence and Security Services will be informed, reasons being given (Article 34, paragraphs 1 and 2, Wiv).			

	A report will not be issued if it has been determined that this is not reasonably possible (Article 34, paragraph 5, Wiv). Issuing the report will be postponed in the following case: if in the case of a request for information this request would be rejected if data concerning the applicant have been processed in the context of any investigation, unless the data were processed more than five years ago; or unless since that time no new data			

	concerning him have been processed in this context; or unless the data in question are not relevant for any current investigation. This also goes for the case in which the request would be rejected if no data concerning the applicant have been processed (Article 34, paragraph 6 Wiv). The duty to investigate the possibility to issue a report will not be necessary if issuing a report about the exercise of powers is reasonably			

	expected to reveal sources of a service, among which intelligence and security services of other countries, seriously damage relations with other countries and with international organisations or reveal a specific application of a method of a service or the identity of the one who has been helpful to the service (Article 34 in conjunction with Article 35, paragraph 7 Wiv).			

Annex 4 – Surveillance-related case law at national level

Please provide a maximun of three of the most important national cases relating to surveillance. Use the table template below and put each case in a separate table.

Case title	ECLI:NL:RBDH:2014:8966
Decision date	23 July 2014
Reference details (type and title of court/body; in original language and English [official translation, if available])	Rechtbank Den Haag, District Court The Hague, civil law section
Key facts of the case (max. 500 chars)	Some natural persons, among whom a criminal lawyer and a reporter, and some legal persons, among whom Internet Society Nederland and Stichting Privacy First, objected to the Dutch state receiving and/or using data from foreign intelligence and security services (among which the American National Security Agency) which were gathered by them using powers which the AIVD and MIVD do not possess. According to the plaintiffs, the Dutch state should inform the persons involved in writing whether it received data (contrary to Dutch and/or international obligations) about them and they should erase these data.
Main reasoning/argumentation (max. 500 chars)	Plaintiffs have a major interest, among which the respect for private life, but there also is the general interest of national security. The mere fact that the state may receive and possibly use data which were gathered by foreign services, using powers that the Dutch do not possess, does not mean that the Netherlands breaches international treaties and national legislation, even though foreign services may intercept untargeted cable-bound communications, whereas the Dutch may not do so. The Wiv provides for cooperation with foreign services. Article 8, paragraph 2 of the ECHR does not as such make unlawful the reception and the use of data without a target, cable-bound, gathered by foreign services. It is of some importance that the data concerned are data in bulk. In this context, a difference should be made between intercepting and processing the data. The question to what extent the exchange of data is a breach of personal life is particularly dependent on what happens to the data after they have been received. There are safeguards in the Wiv. Moreover, there are checks and balances thanks to the Review Committee on Intelligence and Security and recourse in specific cases to the National Ombudsman and the courts. In this case, the interests are of too general a nature to put aside the cooperation with foreign services, which is necessary for national security. Individuals may use the recourse mentioned above. Article 8 of the ECHR does not require from the state to inform the parties involved and erase data. In the case of secret surveillance no absolute duty of notification exists, as this cannot be carried out in practice.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The exchange of data, especially in bulk, with foreign services which may intercept untargeted cable-bound communication, which the Dutch services may not, is allowed.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Netherlands may receive data from foreign intelligence and security services, even if their powers are wider than those allowed within the country. National security prevails.

Case title	ECLI:NL:RBSGR:2011:BP4872
Decision date	16 February 2011
Reference details	Rechtbank ‘s Gravenhage (The Hague District Court)
Key facts of the case (max. 500 chars)	The Intelligence and Security Service did not allow the plaintiff to inspect an amount of non-current personal data that it had at its disposal and it did not allow him to inspect current data. The decision was taken in 2009 and not revoked. The Intelligence and Security Service did not allow the plaintiff to inspect an amount of non-current data about organisations and events (in the context of the Ban the Bomb movement, Anarchism, Green Amsterdam, the political party the Green Left and the advice of the Intelligence Service to the Queen’s Commissioner about granting royal honours that it had at its disposal and it did not allow him to inspect current data about organisations and events. This decision, too, was taken in 2009 and not revoked. The plaintiff appealed to the court and consented to the fact that only the court could inspect the data
Mainreasoning/ argumentation (max. 500 chars)	The defendant regards the requests by the plaintiff as requests for inspection about data that have been processed by the defendant, as laid down in Article 47 Wiv. The plaintiff alleges that it has never been necessary to process data about him and the organisations for which he was active. However, the court can only judge the decisions about the inspection of the data and not about the need to have processed these data. The court judges that, in connection with the defendant’s duty to protect the security of the state and the fact that a certain degree of secrecy is necessary, it is justified that the question whether current data are being processed at all, is not answered. If the defendant should answer this question, secrecy about data being processed would be an illusion. The court has not concluded that the defendant did not allow the plaintiff, without justification, to inspect certain data on the basis of the fact that personal information of third parties would be revealed. The court judges that the defendant justifiably refuses inspection on the basis of the fact that its sources should remain secret. However, this is not justified in the case of data received from public authorities, such as the police and the Public Prosecution Service, which have to supply information to the Intelligence Service on the basis of the law. The refusal on this ground is voidable, although other reasons may lead to the same result. No inspection was allowed of non-current data partly having to do with organsations and events; data in which the plaintiff only plays a minor part. This is not justified in the case of activities where the plaintiff was present or was mentioned as an organisor or inventor. However, other reasons may lead to the same result. In one case a paraphrase of data was given. No reason for not giving the full text was given. The full text should be supplied.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The court can only judge refusals of inspection of data and it cannot judge the question whether it was justified to protect these data. It is justified not to answer the question whether current data are being processed. If this should have been the case, secrecy would be an illusion. It is justified to refuse inspection of data to protect sources, but not in the case of information from public authorities. Even if someone plays a minor part in organisations or events, this is no reason for a refusal to inspect data. Reasons for giving paraphrases of full texts should be given, otherwise the full texts must be provided
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The intelligence service must allow inspection of non-current data if information, revealing sources, has been provided by public authorities and if there are no other reasons for a refusal. The intelligence service should allow inspection of non-current data about organisations or events even if someone has played a minor part. It need not answer the question whether current data are being processed

Case title	Case of Telegraaf Media Nederland B.V. and others v. the Netherlands
Decision date	22 February 2012
Reference details (type and title of court/body; in original language and English [official translation, if available])	European Court of Human Rights, Application no.. 39315/06
Key facts of the case (max. 500 chars)	An official of the AIVD surrendered secret documents and photocopies to some journalists. On 21 January 2006, the newspaper De Telegraaf published an article couched in the following terms: 'AIVD secrets in possession of drugs mafia. Top criminals made use of this information'. Authors were the journalists J. De Haas and B. Mos. The newspaper and the journalists lodged a complaint at the civil court, the journalists saying that their telephones were tapped and that the AIVD, relying on its power to tap targeted cable-bound communication, acted in conflict with Article 8 and 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms (respect for private life, freedom of expression). The Supreme Court held, in the end, that there was an overriding requirement of public interest. The journalists argued that the protection of journalistic sources thus becomes illusory.
Main reasoning/argumentation (max. 500 chars)	Parties agreed before the ECtHR that special powers had been used against the journalists, including the power to intercept and record telecommunications. The ECtHR found that the AIVD sought, by the use of its special powers, to circumvent the protection of a journalistic source. The journalists do not allege that the array of supervisory and monitoring procedurs is in itself insufficient. They contend that they require special safeguards to ensure adequate protection of their journalistic sources. The present case is characterised precisely by the targeted surveillance of journalists in order to determine from whence they have obtained their information. Here, the use of special powers would appear to have been authorised by the Minister of the Interior and Kingdom Relations, if not by the head of the AIVD or even a subordinate AIVD official, but in any case without prior review by an independent body with the power to prevent or terminate it. Review afterwards, such as by the National Ombudsman, cannot restore the confidentiality of journalistic sources once it is destroyed. Violation of Articles 8 and 10 of the Convention.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	When intercepting the telephone conversations of journalists, it is not sufficient that prior approval is given by the Minister involved, as he or she is not independent, provided for by the Intelligence and Security Services Act 2002. Moreover, review afterwards, as provided for, cannot undo possible damage that has occurred. Conflict with the ECHR.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Intelligence and Security Services Act does not provide for proper safeguards to protect journalistic sources.

Annex 5 – Key stakeholders at national level

Please list all the key stakeholders in your country working in the area of surveillance and divide them according to their type (i.e. public authorities, civil society organisations, academia, government, courts, parliament, other). Please provide name, website and contact details.

Name of stakeholder (in English as well as your national language)	**Type of stakeholder** *(i.e. public authorities, civil society organisations, academia, government, courts, parliament, other)*	**Contact details**	**Website**
Prime Minister (Minister President); Minister of the Interior and Kingdom Relations (Minister van Binnenlandse Zaken en Koninkrijksrelaties); Minister van Defensie (Minister of Defence)	Government	Ministerie van Algemene Zaken Binnenhof 19 P.O. Box 20001 2500 EA Den Haag Tel. 070 3564100 fax. 070 3564683 Communication service: Ministerie van Algemene Zaken Dienst Publiek en Communicatie Buitenhof 34 P.O. Box 20006 2500 EA Den Haag Tel. 070 3564249 fax. 070 3641743; Ministerie van Binnenlandse Zaken en Koninkrijksrelaties Turfmarkt 147	www.rijksoverheid.nl

		2511 DP DEN HAAG Tel: 070 426 64 26 P.O. Box 20011 2500 EA Den Haag Ministerie van Defensie Kalvermarkt 32 2511 CB Den Haag P.O. Box 20701 2500 ES Den Haag In all cases there is a possibility to write an e-mail (form on the website www.rijksoverheid .nl), which will be answered within two working days, and a possibility to phone (telephone number 1400).	
National Ombudsman (Nationale Ombudsman)	Public authority (semi-judicial body)	Bezuidenhoutseweg 151 2594 AG Den Haag Tel: 0800 55555 Fax: 070 3607572 From abroad and about questions about current complaints: 070 3563563 P.O. Box 93122 2509 AC Den Haag Free of charge: Antwoordnummer 10870 2501 WB Den Haag Forms on the website to file complaints	www.nationaleombudsman.nl
Bits of Freedom	Civil society	Bits of Freedom Bickersgracht 208 1013 LH Amsterdam	www.bof.nl

		P.O. Box 10746 1001 ES Amsterdam Tel: 06 44995711 info@bof.nl	
Houses of Parliament (Eerste en Tweede Kamer)	Parliament	Eerste Kamer der Staten-Generaal Binnenhof 22 2513 AA Den Haag P.O. Box 20017 2500 EA Den Haag Tel: 070 - 3129200 Fax: 070 - 3129390 E-mail: P.O. Box@eerstekamer.nl Tweede Kamer der Staten- Generaal Lange Poten 4, Plein 2 and Lange Houtstraat 1a, Den Haag, for visitors P.O. Box 20018 2500 EA Den Haag Tel 070-3182211 or 070-3183040 Forms to send an e-mail on the website	www.eerstekamer.nl www.tweedekamer.nl
Review Committee on the Intelligence and Security Services (Commissie van toezicht inlichtingen en veiligheidsdiensten)	Public authority	Anna van Saksenlaan 50 2593 HT Den Haag Tel: 070 - 315 5820 E-mail: info@ctivd.nl.	www.ctivd.nl
General Intelligence and Security Service (*Algemene Inlichtingen en Veiligheidsdienst*); (Militaire Inlichtingen en Veiligheidsdienst)	Public authorities	AIVD Europaweg 4 2711 AH Zoetermeer P.O. Box 20010 2500 EA Den Haag Tel: 079 320 50 50	www.aivd.nl www.mindef.nl/mivd

		Fax: 070 320 07 33 It is not possible to send e-mails. MIVD Ministerie van Defensie P.O. Box 20701 2500 ES Den Haag Tel: 070 3188188 From abroad: 077 4656767 E-mail: mivd@mindef.nl	
District Courts, Courts of Appeal and Supreme Court (*rechtbanken, hoven and Hoge Raad*)	Courts	A great number of addresses, telephone numbers, and e-mail addresses, to be obtained through www.rechtspraak.nl	www.rechtspraak.nl
Internet Society Nederland	Civil society, interest group	Prins Willem-Alexanderhof 5 2595 BE Den Haag Tel. 070-3140385	www.isoc.nl, accessed on 28 July 2014
Stichting Privacy First	Civil society, interest group	Wibautstraat 150 Amsterdam P.O. Box 71909 1008 EC Amsterdam Tel. 020-8100279 E-mail: info@privacyfirst.nl	www.privacyfirst.nl, accessed on 28 July 2014

Annex 6 – Indicative bibliography

Please list relevant reports, articles, studies, speeches and statements divided by the following type of **sources *(in accordance with FRA style guide)***:

1. Government/ministries/public authorities in charge of surveillance

Netherlands, Commissie evaluatie Wiv 2002 (2013), *Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen*, available at: www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2013/12/02/rapport-evaluatie-wet-op-de-inlichtingen-en-veiligheidsdiensten-2002/rapport-evaluatie-wet-op-de-inlichtingen-en-veiligheidsdiensten-2002.pdf

Report by the Dessens Commission, which evaluated the Intelligence and Security Services Act (*Wet op de inlichtingen- en veiligheidsdiensten)*. This report advocates an extension of the powers of the Dutch GISS (AIVD) and the MISS (MIVD). It states that the two organisations should also be authorised to investigate the transfer of personal data by cable.

Netherlands, Departmental Audit Service (*Departmentale Auditdienst*) (2012), *Eindrapport audit CIOT 2011*, The Hague, Ministerie van Veiligheid en Justitie, available at: www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/09/25/eindrapport-audit-ciot-2011/eindrapport-audit-ciot-2011.pdf

Audit report of the Central Information Point for Telecommunications Investigation (*Centraal Informatiepunt Onderzoek Telecommunicatie*, CIOT) on the implementation of Besluit verstrekking gegevens telecommunicatie (Telecommunications (Provision of Information) Decree in 2011.

Netherlands, Departmental Audit Service (*Departmentale Auditdienst*) (2011),Eindrapport *audit CIOT 2010. Een audit naar de opvolging door het CIOT van de aanbevelingen uit de audit 2008 en 2009*, The Hague, Ministerie van Veiligheid en Justitie, available at: www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/08/02/eindrapport-audit-ciot-2010/eindrapport-audit-ciot-2010.pdf

Audit report of the Central Information Point for Telecommunications Investigation (*Centraal Informatiepunt Onderzoek Telecommuncatie*, CIOT) on the implementation of the Telecommunications (Provision of Information) Decree (*Besluit verstrekking gegevens telecommunicatie*) in 2010.

Netherlands, Minister of the Interior and Kingdom Relations (*Minister van Binnenlandse Zaken en Koninkrijksrelaties*) (2013), 'Reactie op het bericht "NSA onderschepte in maand ongeveer 1,8 miljoen telefoontjes in Nederland', Letter to the House of Representatives (*Tweede Kamer der Staten Generaal*), 28 October 2013, available at: www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2013/10/28/brief-aan-tk-inzake-reactie-bericht-nsa-onderschepte-18-miljoen-telefoontjes/brief-aan-tk-inzake-reactie-bericht-nsa-onderschepte-18-miljoen-telefoo.pdf

In this letter to the House of Representatives the Minister of the Interior and Kingdom Relations responds to the news item that the NSA has tapped 1.8 million telephone calls in one month.

Netherlands, Minister of Security and Justice (*Minister van Veiligheid en Justitie*) (2013), 'Tapstatistieken', Letter to the House of Representatives (*Tweede Kamer der Staten Generaal*), 17 July 2013, available www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2013/07/18/kamerbrief-tapstatistieken-2012/tapstatistieken-2012.pdf

In this letter to the House of Representatives the Minister of Security and Justice gives information on the number of telephone taps in 2012 in the Netherlands.

Netherlands, State Secretary for Security and Justice (*Staatssecretaris van Veiligheid en Justitie*) (2013) 'Gegevensbescherming en PRISM', Letter to the House of Representatives (*Tweede Kamer der Staten Generaal*), 2 October 2013, available at: www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2013/10/03/gegevensbescherming-en-prism/lp-v-j-0000004150.pdf

In this letter to the House of Representatives the Minister of Security and Justice gives information on the state of affairs regarding data protection in light of PRISM, the mass electronic surveillance data mining program launched by the National Security Agency.

2. National human rights institutions, ombudsperson institutions, national data protection authorities and other national non-judicial bodies/authorities monitoring or supervising implementation of human rights with a particular interest in surveillance

Netherlands, Review Committee on the Intelligence and Security Services (*Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten*) (2014), *Review report on the processing of telecommunications data by GISS and DISS. CITVD No. 38*, The Hague, Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten., availab CITVD. No.38 le at: www.ctivd.nl/?download=Report%2038%20processing%20telecommunications%20data.pdf

Report on the processing of telecommunications data by the Dutch intelligence and security services (GISS and DISS). It concludes that there had been no systematic acquisition or collections of (personal) data by GISS and DISS in disregard of the law. Nonetheless, the Committee deemed some of the procedures unlawful and holds the opinion that certain other procedures at present contain insufficient safeguards to adequately protect privacy.

Netherlands, Review Committee on the Intelligence and Security Services (*Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten*) (2013),*Toezichtsrapport inzake de inzet van de afluisterbevoegdheid en van de bevoegdheid tot de selectie van Sigint door de AIVD. CTIVD. Nr. 35, The Hague*, Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten, available at: www.ctivd.nl/?download=35Toezichtsrapport%20nr%2035.pdf.

Review report on the use of the power to tap and the power to make use of Sigint by the Dutch GISS (AIVD) covering the period September 2011 through August 2012. It concludes that the AIVD operates in a well considered way.

Netherlands, Review Committee on the Intelligence and Security Services (*Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten*) (2012),*Toezichtsrapport inzake de inzet van de afluisterbevoegdheid en van de bevoegdheid tot de selectie van Sigint door de AIVD. CTIVD Nr. 31*, The Hague, Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten, available at: www.ctivd.nl/?download=CTIVD%20rapport%2031.pdf.

Review report on the use of the power to tap and the power to make use of Sigint by the Dutch GISS (AIVD) covering the period September 2010 through August 2011. It concludes that the AIVD operates in a well considered way. The report did not find any irregularities.

Netherlands, Review Committee on the Intelligence and Security Services (*Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten*) (2011*), Toezichtsrapport inzake de inzet van Sigint door de MIVD*, The Hague, Commissie van

Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten, available at: www.ctivd.nl/?download=CTIVD%20rapport%2028.pdf.

Review report on the use of power to make use of Sigint by the Dutch DISS (MIVD).

Odinot,G., De Jong, D., Van der Leij, J.B.J., De Poot, C.J. and Van Straalen (2012), De Wet bewaarplicht telecommunicatiegegevens, The Hague, Boom Lemma, available at: www.wodc.nl/images/ob304-volledige-tekst_tcm44-453677.pdf.

This study clarifies how the police and judicial authorities use the data kept under the Telecommunications Data (Data Retention Directive) Act (*De Wet bewaarplicht telecommunicatiegegevens*).

3. Non-governmental organisations (NGOs)

Bit (2013), *BIT Transparency Report 2012*, Ede, BIT, available at: www.bit.nl/documents/transparency-2012.pdf.

This report of provider BIT reveals the number of requests for disclosure of personal data and notices-and-takedown requests BIT has received in 2012 and how these requests have been handled.

Bit (2014), *BIT Transparency Report 2013*, Ede, BIT, available at: www.bit.nl/documents/transparency-2013.pdf.

This report of provider BIT reveals the number of requests for disclosure of personal data and notices-and-takedown requests BIT has received in 2013 and how these requests have been handled

Bits of Freedom (2012), *A Loophole in Data Processing. Why the 'legitimate interests' test fails to protect the interests of users and the Regulation needs to be amended*, Amsterdam, Bits of Freedom, available at: www.bof.nl/live/wp-content/uploads/20121211_onderzoek_legitimate-interests-def.pdf.

Report of NGO Bits on Freedom on the processing of personal data by companies and governments on the basis of the so-called 'legitimate interests' ground. The report shows that this ground has served as a basis for virtually unrestricted and unregulated forms of data processing without control of the user. Bits of Freedom concludes that this ground should be curtailed in order to provide clarity and trust for users.

De Joode, A. (2014), *Law Enforcement Transparency Report 2014: July 1 – December 31*, Web Page, Amsterdam, LeaseWeb, available at: http://blog.leaseweb.com/2014/02/25/law-enforcement-transparency-report-2014-july-1-december-31/

This report of provider Leaseweb reveals the number of requests for disclosure of personal data and notice-and-takedown requests it has received in period July - December 2013 and how these requests have been handled.

De Joode, A. (2013*), Law Enforcement Transparency Report 2013: January 1 – June 30*, Web page, Amsterdam, LeaseWeb, available at: http://blog.leaseweb.com/2013/08/28/law-enforcement-transparency-q1q2-2013/

This report of provider Leaseweb reveals the number of requests for disclosure of personal data and notice-and-takedown requests it has received in period January - June 2013 and how these requests have been handled

De Joode, A. (2013), *LeaseWeb first hosting provider worldwide to launch Law Enforcement Transparency Report*, Web Page, Amsterdam, LeaseWeb, available at: http://blog.leaseweb.com/2013/04/11/leaseweb-first-hosting-provider-worldwide-to-launch-law-enforcement-transparency-report/

This report of provider Leaseweb reveals the number of requests for disclosure of personal data and notice-and-takedown requests it has received in 2012 and how these requests have been handled

XS4ALL (2014), *Transparantierapport 2013*, Amsterdam, XS4ALL, available at: www.xs4all.nl/media/transparantie/Transparantierapport-2013.pdf.

This report of provider XS4allreveals the number of requests for disclosure of personal data and notices-and-takedown requests it has received in 2013 and how these requests have been handled

XS4ALL (2013), *Transparantierapport 2012*, Amsterdam, XS4ALL, available at: https://www.xs4all.nl/media/transparantie/Transparantierapport-2012.pdf.

This report of provider XS4allreveals the number of requests for disclosure of personal data and notices-and-takedown requests it has received in 2012 and how these requests have been handled

4. Academic and research institutes, think tanks, investigative media report.

Borger, J. (2013), 'GCHQ and European spy agencies worked together on mass surveillance. Edward Snowden papers unmask close technical cooperation and loose alliance between British, German, French, Spanish and Swedish spy agencies', *The Guardian*, 1 November 2013, available at: www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden.

This article reveals how Britain's GCHQ spy agency maintains strong relations with the Dutch Giss (AIVD) and Miss (MVID).

Fijnaut , C. (2012), Het toezicht op de inlichtingen- en veiligheidsdiensten: de noodzaak van krachtiger samenspel. De vertrekpunten en uitkomsten van een gespreksronde, The Hague, Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten, available at: http://www.ctivd.nl/?download=Boek%20Cyrille%20Fijnaut%20Wiv%202002-2012.pdf

Evaluation study commissioned by the Review Committee on the Intelligence and Security Services (Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten) and made by an independent expert on the oversight system created by the the Act on Intelligence and Security Services (Wet op de Inlichtingen en Veiligheidsdiensten).

Telegraaf (2013), 'Ook AIVD bespiedt internetter', *De Telegraaf*, 11 June 2013, available at: www.telegraaf.nl/digitaal/21638965/__Ook_AIVD_bespiedt_online__.html.

This article reveals that the Dutch Giss (AIVD) had received information from PRISM, the mass electronic surveillance data mining program launched by the National Security Agency of the USA.

Van der Sloot, B. (2014), 'Privacy in het post NSA-tijdperk. Tijd voor een fundamentele herziening?', Nederlands Juristenblad, 2 May 2014, available at: www.ivir.nl/publicaties/sloot/NJB_2014_17.pdf.

This article explores the problems posed by the activities of the NSA for data protection. It focuses in particular on the threat that the activities of the NSA pose for section 8 of the European Convention on Human Rights.

Van Hoboken, J, Arnbak, A, Van Eijk, N. (2013), *Obscured by Clouds or How to Address Governmental Access to Cloud Data From Abroad. Draft*, Amsterdam, Institute for Information Law - University of Amsterdam, available at: www.ivir.nl/publications/vanhoboken/obscured_by_clouds.pdf.

This article addresses the existence and risks of transnational intelligence gathering in the cloud context and the appropriate legal responses to it. It finds that the most sensible way to address the issue would be through the application and possible strengthening of oversight over intelligence agency operations.

Van Hoboken, J, Arnbak, A, Van Eijk, N. (2012), *Cloud diensten in hoger onderwijs en onderzoek en de USA Patriot Act, Amsterdam*, Institute for Information Law - University of Amsterdam, available at: www.ivir.nl/publicaties/vanhoboken/Clouddiensten_in_HO_en_USA_Patriot_Act.pdf.

Institutions have started to move their data and ICT operations into the cloud. This report concludes that the U.S. legal state of affairs implies that the transition towards the cloud has important negative consequences for the possibility to manage information confidentiality, information security and the privacy of European end users in relation to foreign governments.