PRIVACY FIRST

Submission of Privacy First
to the fifth periodic review of the Netherlands
by the UN Human Rights Committee

- Addendum -

2 June 2019

Contact information:
Privacy First Foundation *(Stichting Privacy First)*
PO Box 16799
1001 RG Amsterdam
The Netherlands
Phone: +31 (0)20 81 002 79
Email: info@privacyfirst.nl
Website: www.privacyfirst.nl

Introduction and overview

In December 2016, the Privacy First Foundation has sent a shadow report to the UN Human Rights Committee (hereinafter: the Committee) regarding the human rights situation in the Netherlands from a privacy and data protection perspective.[1] We very much appreciate the fact that some of the most pressing issues that we had mentioned in this report have subsequently been included in the Committee's List of Issues.[2] However, more than two years have passed since then, making it necessary for us to provide the Committee with additional information and to give an update on relevant developments. In particular, Privacy First hereby wishes to draw the Committee's attention to the following issues:

In addition, we hereby take the opportunity to draw the Committee's attention to two other related human rights issues which deserve attention, since they apply to the Netherlands and since they could also set important precedents for the global community of ICCPR States Parties in the context of current international developments:

Relevant international context since September 2017

Partly due to lobbying efforts by Privacy First,[3] the Netherlands received the following recommendation by the UN Human Rights Council in May 2017:

> *Take necessary measures to ensure that the collection and maintenance of data for criminal [investigation] purposes does not entail massive surveillance of innocent persons.*[4]

---

[1] *Submission of Privacy First to the fifth periodic review of the Netherlands by the UN Human Rights Committee*, 12 December 2016.

[2] UN Human Rights Committee, *List of issues prior to submission of the fifth periodic report of the Netherlands*, UN Doc. CCPR/C/NLD/QPR/5 (3 May 2017). Hereinafter: List of Issues.

[3] See https://www.privacyfirst.eu/focus-areas/law-and-politics/656-the-netherlands-under-the-united-nations-magnifying-glass.html (English) and https://www.privacyfirst.nl/aandachtsvelden/wetgeving/item/1071-nederland-onder-de-loep-bij-verenigde-naties.html (Dutch).

[4] *Report of the Working Group on the Universal Periodic Review - Netherlands*, UN Doc. A/HRC/36/15 (18 July 2017), para. 131.121.

The Dutch government accepted this recommendation in September 2017.[5] In the view of Privacy First, this constitutes a relevant benchmark for the evaluation of the Netherlands by the Committee during this session. Despite the international commitment of the Netherlands to adhere to this recommendation, Dutch national practice since then has shown that the Netherlands has already broken its promise to the UN Human Rights Council several times. In particular, the Netherlands has recently adopted (or has the intention to adopt) the following legislative measures which entail massive surveillance of innocent persons:

1. Act on Automatic Number Plate Recognition (ANPR)

The Dutch Act on Automatic Number Plate Recognition (ANPR) was adopted by the Dutch Senate in November 2017 and has entered into force on January 1st 2019. Under this Act, the number plate of each motorist in the Netherlands (thus the travel movements of all motorists) are being recorded and stored in a central police database for four weeks for criminal investigation purposes as well as intelligence purposes, thus treating every motorist as a potential suspect. In addition to Dutch police, the Dutch intelligence services have direct, shielded access to this database. No prior independent (judiciary) oversight for the use of this ANPR database exists. Privacy First is currently preparing a lawsuit in order to have this Act declared null and void due to violation of international and European privacy and data protection laws.

2. Telecommunications data retention[6]

Despite constituting a clear breach of international and European privacy and data protection laws, the Dutch Bill on blanket (general) telecommunications data retention has not been amended yet and is still awaiting debate in the Senate. This presents a major opportunity for the Committee to issue guidance to the Netherlands and to set an important precedent in this field.

3. Dutch Act on Intelligence and Security Services[7]

Despite society-wide resistance and even a national referendum in which the Dutch population rejected the new Dutch Act on Intelligence and Security Services, this Act entered into force on May 1st 2018 largely unmodified. Clear privacy violations in this Act include new massive internet-wiretapping capabilities, making it possible to put a surveillance tap on large parts of the Dutch population at once. In addition, the new Act gives secret services the

[5] See UN Doc. A/HRC/36/15/Add.1 (14 September 2017), p. 2.

[6] See List of Issues, para. 11.

[7] See List of Issues, para. 11.

power to hack into any computer and to demand decryption of any digital file (the latter punishable by jail for non-compliance), direct access to all government databases as well as potential access to any database in the private sector, new datamining and profiling capabilities as well as the international exchange of unevaluated bulk data with foreign secret services, thus compromising huge amounts of sensitive personal information without any effective oversight. Unless this Act will soon be amended by Dutch Parliament, Privacy First and other NGOs reserve the right to start legal proceedings in order to have this Act partially declared null and void.

4. Passenger Name Records (PNR)

The most recent Dutch legislative measure which entails massive surveillance of innocent persons concerns the Dutch implementation Act on Passenger Name Records (PNR). Under this Act, the data of all airline passengers will be stored in a central database for the duration of five years for criminal investigation purposes, counter-terrorism and intelligence gathering. Large amounts of travel data (names and addresses, telephone numbers, destinations, travel companions, financial transaction data, etc) of millions of innocent people will therefore remain available to law enforcement and intelligence services for the purpose of datamining and profiling. Despite this Act already having been considered to be in violation of European privacy and data protection laws by the highest Dutch advisory bodies (the Dutch Council of State as well as the Dutch Data Protection Authority) and despite recent German statistics which show error rates in false positives of 99,7% (!) under the similar German PNR system,[8] the Dutch PNR Act will probably be adopted by the Dutch Senate on June 4th 2019. A large-scale lawsuit by German and Austrian NGOs has recently been initiated in order to have the 'upper' EU PNR Directive declared null and void by the European Court of Justice through preliminary proceedings via the German and Austrian national courts.[9] This moment thus presents a unique opportunity for the Committee to set a high standard in this field on the international level.

5. Dutch implementation of the European Payment Services Directive 2 (PSD2)

Another legislative measure which entails massive risks for privacy in the Netherlands is the Dutch implementation Act under the European Payment Services Directive 2 (PSD2), which entered into force in the Netherlands early 2019. Under this new law, with their general, blanket consent, consumers can share their banking details with parties other than their own bank. Therefore, consumers are not in a position to limit their amount of banking details. Even in case a financial service provider does not need all of these details, all data are shared nevertheless. Such banking details of a consumer also include the details of

[8] See *Überwachung von Flugpassagieren liefert Fehler über Fehler,* Süddeutsche Zeitung 24 April 2019, https://www.sueddeutsche.de/digital/fluggastdaten-bka-falschtreffer-1.4419760 (in German).

[9] See https://nopnr.eu.

contra accounts. Holders of such accounts are unaware of the fact that their details may be shared by others, and are not in a position to prevent that. As transactional data will be analyzed much more widely through the use of Big Data and new profiling techniques than before the introduction of PSD2, there will be an increasing risk of privacy violations. In addition to this, banking details regularly contain sensitive personal data that may only be processed under very strict conditions (such as specific prior consent for the processing of each such transaction). A subscription payment to a trade union, political party or organization that reveals one's sexual preferences, for example, should be considered as sensitive personal data. The same applies to donations to religious institutions or to NGOs, transactions with health insurance companies, pharmacists or hospitals. Currently, there is no way to filter out these data and they will be shared with parties that are not allowed to process them. Consumers who do not want others to share their data with financial service providers should have the opportunity to prevent this. That is why Privacy First has recently taken the initiative to create a national opt-out register for PSD2, similar to existing do-not-call registries (in telemarketing) or do-not-track registries (for WiFi tracking). Privacy First hopes to develop this together with the financial sector and policy makers. Our aim is to have a compulsory opt-out register and to have the current European PSD2 Directive amended accordingly. Given the fact that this will ultimately be a matter of global concern, Privacy First hereby invites the Committee to take a critical stance on this issue.

6. Draft Interpretative Note to FATF Recommendation 15

A recent scientific evaluation of the implementation of counter-terrorism policies in the Netherlands has outlined that social side effects, such as excessive reporting of transactions and its impact on the privacy of citizens, (often) remain underexposed in public discussions.[10] As a case in point, Privacy First has noticed in May 2019 that the Dutch Ministry of Finance downplayed a very impactful counter-terrorism recommendation of the global Financial Action Task Force (FATF) as a technicality towards Dutch Parliament.[11]

The recommendation is phrased in paragraph 7b of an interpretative note for Recommendation 15 of the FATF.[12] It requires all private sector entities to register and submit the names of the parties participating in a virtual asset transfer to all counterparts in the value chain. This is not based on suspicion of criminal behaviour but required as a standard data export for all use cases and customers transferring virtual assets. The virtual

[10] M. Wesseling & M. de Goede, *Counter Terrorism Financing Policies in The Netherlands: Effectiveness and Effects (2013-2016)*, Amsterdam Institute for Social Science Research (December 2018, Amsterdam), available at https://www.wodc.nl/binaries/2689D_Summary_tcm28-372746.pdf.

[11] See Dutch Ministry of Finance, *Report on FATF plenary session*, 21 March 2019, https://www.rijksoverheid.nl/documenten/kamerstukken/2019/03/21/verslag-plenaire-vergadering-fatf.

[12] See FATF, *Draft Interpretative Note to FATF Recommendation 15*, 22 February 2019, Paris, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html.

assets are defined as all non-regulated digital representations of value which may be transferred or held: **'..**countries should consider virtual assets as "property," "proceeds," "funds", "funds or other assets," or other "corresponding value".

The rule has met with very heavy pushback during a recent private sector consultation (in Spring 2019) due to its incompatibility with international privacy laws and its unclear definition. However, the Dutch Ministry of Finance has quietly announced that the rule will not be changed and will be tabled for adoption by June 16-20 in the next FATF meeting. Subsequently, Privacy First has joined the initiative of a group of virtual asset service providers (VBNL) and urgently requested the Ministry of Finance not to approve the proposal.[13] We invite the Committee to point out the discrepancy between the UN Human Rights Council recommendation adopted by the Dutch government in September 2017 (see above) and the intended approval of the FATF interpretative note.

7. Bill on market health care and Ministerial regulation[14]

The Bill that would authorize insurance companies to consult personal medical files of patients has been temporarily withdrawn by the Dutch government. The majority of the Dutch Senate said they would vote against the proposal. The Senators are not convinced it is absolutely necessary to examine personal medical files without asking permission. The Dutch Minister of Public Health has stated he will make minor adjustments to the Bill before presenting it again to Dutch Parliament. These minor adjustments will most likely not include asking permission to examine personal medical files of patients.

However, the insurance companies at the moment already have the authority to examine personal medical files. This is based on a Ministerial regulation and has been the case since at least 2011. The Minister of Public Health has confirmed that the insurance companies will continue examining personal medical files as they have done in the past. By doing so, the Minister continues a practice that the Senate has not approved and was very likely to vote against.

The Bill would have given the current practice a solid legal basis. Because the Bill has been withdrawn before the Senate could vote on it, there is no official verdict against the examining of personal medical files by insurance companies. As it is, the insurance companies will continue their examinations of personal medical files and the Minister can simply wait for the right moment to present his new proposal to Parliament.[15]

---

[13] See Privacy First and VBNL, *Urgent call to Dutch Minister of Finance: please prevent the unbridled export of EU personal data,* https://www.privacyfirst.eu/focus-areas/financial-privacy/677-prevent-the-unbridled-export-of-eu-personal-data.html, 23 May 2019.

[14] See List of Issues, para. 27.

[15] Privacy First wishes to thank the Dutch website Privacy Barometer for the information in this paragraph. For further backgrounds, see

Other issues

8. Abolishment of the Dutch Advisory Referendum Act

In March 2018, on the initiative of five students of the University of Amsterdam, a Dutch national referendum on the new Intelligence and Security Services Act was organized under the Dutch Advisory Referendum Act. In this referendum, a majority of the Dutch population voted against the Intelligence and Security Services Act, forcing the Dutch government to promise several changes to this Act in order to better protect the people's right to privacy and data protection. Even according to (former) supporters of the new intelligence Act as well as opponents of Dutch referenda in general, the way that this referendum had been organized and conducted provided an excellent example of a national referendum. However, despite the successful referendum on the new Intelligence and Security Services Act, Dutch Parliament (on the initiative of the Dutch government) subsequently abolished the Dutch Advisory Referendum Act in July 2018, thus cancelling any possibility for future Dutch referenda on other topics of general interest, such as a new referendum on the controversial new Dutch Act on Organ Donation.

Privacy First very much regrets the fact that the Netherlands has completely abolished the possibility to hold national referenda, as we expect that this will further widen the existing gap between Dutch citizens and their government. Privacy First also expects that will lead to a further loss of confidence in national politics, which is shown by recent national election results. This weakens our democracy and, without the corrective effect of a referendum, also our rule of law.

In an international legal sense, under common Article 1 of the ICCPR and ICESCR, a national referendum is a form of internal self-determination: this constitutes the collective right of a national population to determine its own democratic future. Like all human rights, this right must be protected and promoted. Moreover, the legal possibility to hold a referendum is a democratic achievement that cannot simply be abolished without legitimate cause and objective justification. Such abolishment is possibly contrary to international law, in particular the general ICESCR duty of progressive realization and non-regression which similarly applies to common Article 1 ICESCR / ICCPR. In essence, this comes down to an international prohibition of ruthlessly reversing democratically acquired rights of citizens. Early in 2018, Privacy First fruitlessly tried to draw the attention of Dutch Parliament to this international legal rule. Privacy First subsequently pledged to refer this issue to the United Nations at the earliest relevant occasion, which we are hereby doing by drawing the Committee's attention to this.

Apart from the former German Democratic Republic (East Germany), the Netherlands is now the only country in the world that has abolished a national referendum after its

---

https://www.privacybarometer.nl/nieuws/3942/wetsvoorstel-inzage-medische-dossiers-door-zorgverzekeraars-van-tafel (13 May 2019, in Dutch).

introduction.[16] Given the fact that this Dutch abolishment seems to lack any legitimate cause and objective justification, this may constitute a violation of the right to internal self-determination of the Dutch population under Article 1 ICCPR (as applied and interpreted in accordance with the duty of progressive realization and non-regression under parallel Article 1 ICESCR). Privacy First accordingly invites the Committee to enter into a critical dialogue about this with the Dutch government and to issue relevant recommendations accordingly.

9. Prohibition of propaganda for war

The Netherlands, along with Sweden, is one of the only two countries in the world which have for decades maintained a general, unexplained reservation to the international prohibition of propaganda for war (Article 20 paragraph 1 ICCPR).[17] Out of a current total of 172 States Parties to the ICCPR, merely 16 States have made a reservation to Article 20 paragraph 1 and these are all Western countries. On previous occasions, any arguments that this prohibition would run counter to the freedom of expression have invariably (and rightly) been swept aside by the Committee; incidentally, this has been the standard argument put forward by most countries with such a reservation. Article 20 paragraph 1, after all, only concerns illegal instead of legal warfare; see e.g. the relevant General Comment by the Committee from 1983.[18] In July 2009 this point was also raised (partly on the recommendation of the Dutch section of the International Commission of Jurists, NJCM) during the Dutch ICCPR session in Geneva,[19] which then led to the Committee's concluding observation for the Dutch government to withdraw its reservation. However, since then the Netherlands has refused to withdraw the reservation in question. On the contrary, it has renewed the exact same reservation (still without any explanation) in October 2010. Being the host State of the International Criminal Court, it would be appropriate for the Netherlands to withdraw this reservation a.s.a.p. Accordingly, Privacy First hereby invites the Committee to enter into a critical dialogue with the Dutch government on this issue once again and to issue relevant recommendations. Given the historical background of the UN human rights framework as well as current international (geopolitical) developments, the upcoming Dutch session presents a unique opportunity for the Committee to set a strong global precedent in this regard.

---

[16] See e.g. https://www.nrc.nl/nieuws/2017/11/12/nrc-checkt-alleen-ddr-schafte-eerder-referendum-af-13982755-a1580921 (in Dutch).

[17] Article 20 paragraph 1 ICCPR stipulates that "any propaganda for war shall be prohibited by law." Upon ratification of the ICCPR in 1978, the Netherlands made the following reservation: "the Kingdom of the Netherlands does not accept the obligation set out in this provision in the case of the Netherlands." This reservation was renewed on 11 October 2010. Source: https://treaties.un.org/Pages/ViewDetails.aspx?chapter=4&clang=_en&mtdsg_no=IV-4&src=IND#EndDec .

[18] UN Human Rights Committee, *CCPR General Comment No. 11: Article 20 Prohibition of Propaganda for War and Inciting National, Racial or Religious Hatred*, 29 July 1983.

[19] See UN Docs. CCPR/C/SR.2630 & CCPR/C/SR.2631 (14-15 July 2009).