PRIVACY FIRST

Submission of Privacy First
to the third Universal Periodic Review of the Netherlands
by the UN Human Rights Council

16 September 2016

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

I. Introduction and overview

During its first UPR session in April 2008, the Netherlands received the following general recommendation:

> *"While implementing anti-terrorism measures, respect international human rights obligations, including the right to a fair trial and the right to freedom and security of the person; and consider revising all anti-terrorism legislation to bring it in line with the highest human rights standards."*[1]

This recommendation was accepted by the Netherlands, which replied as follows:

> *"(…) The Dutch government strongly believes that even the most threatening forms of terrorism should be fought against within the framework of the constitutional rights and freedom of individuals.(…)"*[2]

Similarly, during its second UPR session in May 2012, the Netherlands made the following statement:

> *"The need to strike a balance between different interests has sometimes been hotly debated in the Dutch political arena, for example in the context of privacy measures and draft legislation limiting privacy. The compatibility of this kind of legislation with human rights standards is of utmost importance. This requires a thorough scrutiny test."*[3]

The coming UPR session presents an excellent opportunity for such a scrutiny test on the international level. Having been an 'EU entry point' and a testing ground for American counter-terrorism policies for years,[4] the Netherlands has adopted numerous measures which either infringe or violate the right to privacy as protected under Article 8 of the European Convention on Human Rights (ECHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR). Many of these measures have been introduced in the name of counter-terrorism, yet mostly without their necessity having been established and often without any element of choice for innocent citizens. These measures should thus either be abolished or amended in order to make them comply with the right to privacy and data protection. This includes the modern principle of 'privacy by design', making digital systems 'privacy-proof' from the moment they are being designed on the technical drawing-board. In this regard, the current UPR process presents a perfect chance for critical dialogue as well as the sharing of best practices between UN Member States and the Netherlands. In order to facilitate this, Privacy First hereby wishes to draw particular attention to the following topics:

---

[1] UN Doc. A/HRC/8/31 (13 May 2008), at 18 (Recommendation no. 29).
[2] UN Doc. A/HRC/8/31/Add.1 (25 August 2008), para. 40.
[3] Source: https://www.privacyfirst.eu/focus-areas/law-and-politics/547-un-member-states-criticize-netherlands-over-ethnic-profiling.html. This statement was partly triggered by the Privacy First shadow report on the Netherlands of November 2011, see https://www.privacyfirst.eu/focus-areas/law-and-politics/476-privacy-first-puts-dutch-privacy-violations-on-un-agenda.html.
[4] See e.g. https://www.theguardian.com/world/us-embassy-cables-documents/38987.

II. Lack of effective legal remedies

Since the Dutch Supreme Court judgment in the civil law case of Privacy First *et al*. vs. the Dutch government in May 2015, it has become highly difficult for non-governmental organisations (NGOs) to institute legal proceedings *in the general interest* in order to fight human rights violations (including privacy violations) in the Netherlands. This is due to the Supreme Court finding that, if individual legal remedies in the administrative courts exist, civil public interest litigation by an NGO regarding the same (or similar) legal question(s) will be inadmissible. This places a very heavy burden on individuals and leaves NGOs virtually powerless to have relevant Dutch legislation or policy declared unlawful by the judiciary.[5] This undesirable situation is reinforced by the fact that Dutch administrative judges are not allowed to test the compatibility of Dutch legislation and policy with international or European human rights law *directly*.[6] Until May 2015, this could only be done *directly* through civil litigation. Since then, it can only be done *indirectly* in administrative lawsuits brought by individuals, through so-called "exceptional scrutiny" (*exceptieve toetsing*) under Dutch administrative law. In addition, the Dutch judiciary (both civil and administrative) has never been allowed to test the compatibilty of Dutch national legislation with the Dutch Constitution; this is strictly forbidden under Article 120 of the Dutch Constitution itself,[7] making the Netherlands a rare exception in the sense that it virtually has no national constitutional jurisprudence and no effective constitutional protection.

This leads us to our first and most urgent recommendation:

We hereby recommend the Human Rights Council to urge the Netherlands 1) to reinstate the right of NGOs to conduct public interest litigation, 2) to withdraw current legal obstacles to test the compatibility of Dutch legislation and policy with international and European law and 3) to introduce procedures for constitutional review by the courts.

[5] See https://www.privacyfirst.eu/court-cases/639-dutch-supreme-court-passes-on-passport-trial-to-council-of-state.html.

[6] See Dutch General Administrative Law Act (*Algemene Wet Bestuursrecht*), Article 8:3: 'No appeal lies against a decision laying down a generally binding regulation or policy rule.'

[7] Article 120 of the Dutch Constitution reads as follows: 'The constitutionality of Acts of Parliament and treaties shall not be reviewed by the courts.'

III. Profiling

In today's Dutch society, more and more use is being made of datamining and profiling techniques to discover patterns in large amounts of data from various sources (Big Data), thus compiling digital profiles about individual persons and groups without them being aware of this. Both governments and corporations do this on an ever increasing scale, yet mostly without any transparency and accountability and often without any specific legislation in place. Examples include financial profiling to detect creditworthiness and fraud, forensic profiling to trace criminals, counter-terrorism profiling of air passengers, profiling of highway motorists and travellers in public transport, profiling of children through Electronic Child Records, employers profiling (potential) employees, landlords profiling (potential) tenants, commercial (internet) profiling, 'targeted advertising', etc. Digital profiles can be extremely detailed, covering many aspects of someone's life, including (highly) sensitive personal information such as medical data. Profiling can easily lead to discrimination and 'steering' of persons in pre-determined directions, depending on the 'categories' their 'profiles' fit into and without the persons in question being aware of this. From a human rights point of view, people's profiles may thus come to function as digital straitjackets or self-fulfilling prophecies, limiting their right to personal autonomy and free individual development. To counter these negative effects, in line with a recent study on the societal risks of Big Data by the Dutch Scientific Council for Government Policy (WRR),[8] we hereby make the following recommendation:

We recommend the Human Rights Council to urge the Netherlands to implement specific legislation on the topics of datamining and profiling, guaranteeing the right to privacy, transparency, legal remedies, accountability, freedom of choice and the right to correction and removal of personal data.

IV. Automatic Number Plate Recognition (ANPR)

Early in 2013, the Dutch government introduced a Bill to Dutch Parliament regarding the introduction of ANPR on a massive scale for criminal investigation and intelligence purposes, despite the fact that this Bill had already been declared illegal by the Dutch Data Protection Authority (DPA).[9] In the opinion of the DPA and most other privacy experts, a system of ANPR as proposed in this Bill would amount to a collective violation of the right to privacy and data protection due to it being completely unnecessary and disproportionate. This follows from the fact that, under the Bill as currently drafted, not only all 'hits' but also all 'no-hits' will be stored in police databases for a period of four weeks, thus treating each and every motorist as a potential suspect and storing their personal data as such.[10]

---

[8] See http://www.wrr.nl/en/office/staf/article/big-data-privacy-en-veiligheid/.

[9] See Autoriteit Persoonsgegevens (Dutch DPA) 28 February 2011, *CBP adviseert over gebruik ANPR door politie*, https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-adviseert-over-gebruik-anpr-door-politie (in Dutch). Compare e.g. Federal Constitutional Court of Germany 11 March 2008, http://www.bverfg.de/entscheidungen/rs20080311_1bvr207405.html (in German).

[10] See Bill no. 33542, *Wijziging van het Wetboek van Strafvordering in verband met de regeling van het vastleggen en bewaren van kentekengegevens door de politie*, available at

We recommend the Human Rights Council to urge the Netherlands to either revoke its ANPR Bill or to bring it in line with the highest privacy standards, hence excluding all 'no-hits' from its reach and redeveloping the current ANPR system in compliance with modern standards of 'privacy by design'.

V. Automatic border control (@MIGO-BORAS)

Early in 2011 it emerged that the Dutch government had for years been planning to implement a highly privacy-invasive system of ANPR-like border control. This high-tech surveillance system called @MIGO-BORAS[11] subsequently entered into force on January 1st 2012. Under the system, millions of vehicles crossing the Dutch-German and Dutch-Belgian borders are continually photographed and thoroughly screened and profiled through various databases, many of which remain unknown. It is thus even possible to photograph and (biometrically) identify both the driver and passenger(s) inside the vehicle. However, details of @MIGO-BORAS remain confidential and relevant Dutch governmental organisations have until now preferred not to answer any questions about it. As far as Privacy First is aware, these organisations include the Dutch police, Immigration Service (IND), Royal Marechaussee (military police) and both the General and Military Intelligence and Security Services (AIVD and MIVD). Primary goals of the project seem to be the detection of illegal immigration, criminal investigation and intelligence. Media attention about the project has been scarce. In Dutch parliament, hardly any questions have been asked about it. No specific legislation around its implementation has been drafted either (let alone introduced into Parliament), making the political silence around this topic all the more peculiar. Consequently, both because of its secrecy as well as its enormous scale and invasiveness, @MIGO-BORAS constitutes a massive violation of the right to privacy.

We recommend the Human Rights Council to urge the Netherlands to suspend @MIGOBORAS, at least until relevant legislation with specific privacy safeguards has been adopted by Parliament.

VI. Telecommunications Data Retention

Under the Dutch Data Retention Act of 2009, the telecommunications data (telephony and internet traffic) of everyone in the Netherlands used to be retained for 12 months and 6 months, respectively, for criminal investigation purposes. As a result, every citizen became a potential suspect. In interim injunction proceedings against the Dutch government in

---

https://www.rijksoverheid.nl/actueel/nieuws/2013/02/12/wetsvoorstel-over-het-vastleggen-van-kentekens-naar-tweede-kamer. See also https://www.rijksoverheid.nl/actueel/nieuws/2016/09/07/van-der-steur-wijzigt-anpr-wetsvoorstel (in Dutch).

[11] @MIGO-BORAS stands for '*Automatisch Mobiel InformatieGestuurd Optreden* (Automatic Mobile Information-Driven Action) – Better Operational Results and Advanced Security'; see https://www.government.nl/documents/leaflets/2012/07/11/factsheet-on-the-use-of-the-amigo-boras-system.

February 2015, a broad coalition of Dutch NGOs demanded this Act to be rendered inoperative as it violated the right to privacy. The claimant organizations were Privacy First, the Dutch Association of Criminal Defence Lawyers (NVSA), the Dutch Association of Journalists (NVJ), the Netherlands Committee of Jurists for Human Rights (NJCM), Internet provider BIT and telecommunications providers VOYS and SpeakUp. According to the claimant parties, the Dutch Data Retention Act constituted a violation of fundamental rights that protect private life, communications and personal data. This was also the view of the European Court of Justice in April 2014, and subsequently that of the Dutch Council of State (*Raad van State*), the Dutch Data Protection Authority and the Dutch Senate. Similarly, in April 2014 the UN Human Rights Committee had taken the position that States parties to the ICCPR should "refrain from imposing mandatory retention of data by third parties".[12] However, the former Dutch Minister of Security and Justice, Ivo Opstelten, refused to withdraw the Dutch Data Retention Act. Opstelten wanted to uphold the Act until a legislative change was implemented, which could have taken years. Rather uniquely (Dutch laws are seldomly rendered inoperative by a judge, let alone in interim injunction proceedings), on 11 March 2015, the district court of The Hague made short shrift of the entire Act by repealing it immediately as it was in breach of the right to privacy.[13] The Dutch government decided not to appeal the ruling, which has been final since then. By now, all telecom providers concerned have deleted the relevant data. In relation to criminal investigations and prosecutions, so far this does not seem to have led to any problems. However, recently the current Dutch Minister of Security and Justice, Ard van der Steur, has submitted a new Bill into Parliament which introduces blanket data retention for all telecom providers (and all citizens) once again.[14] This leads us to the following recommendation:

We recommend the Human Rights Council to urge the Netherlands not to re-introduce blanket data retention and to withdraw its current data retention Bill.

VII. New Act on Intelligence and Security Agencies

The Dutch government has recently presented a draft Bill which will completely replace the current Dutch Act on intelligence and security agencies (*Wet op de inlichtingen- en veiligheidsdiensten*, Wiv).[15] A section of this new Bill which is currently causing national upheaval concerns the introduction of new massive internet-wiretapping capabilities for the Dutch secret services. Under the Bill as currently drafted, it will become possible to put a surveillance tap on the entire (or a large part of the) Dutch population at once. In addition, there will hardly be any judicial control over the intelligence powers conferred, including an unregulated competence for secret agents to commit criminal acts, the ability for agencies to hack into any computer and demand decryption of digital files (the latter punishable by

[12] See UN Doc. CCPR/C/USA/CO/4 (April 2014), para. 22(d).

[13] See https://www.privacyfirst.eu/court-cases/624-privacy-first-wins-lawsuit-against-dutch-data-retention-act.html.

[14] See Bill no. 34537 regarding 'adjustment of telecommunications data retention', https://www.tweedekamer.nl/kamerstukken/wetsvoorstellen/detail?id=2016Z16486&dossier=34537 .

[15] See *Wetsvoorstel voor de inlichtingen- en veiligheidsdiensten (Wiv) 20XX*, available at http://www.volkskrant.nl/media/kabinet-houdt-vast-aan-massaal-aftappen-internetverkeer~a4291392/.

jail for non-compliance), direct access to government databases as well as any database in the private sector, new datamining and profiling capabilities as well as the international exchange of unevaluated bulk data, thus compromising huge amounts of sensitive personal information.[16]

We recommend the Human Rights Council to urge the Netherlands to scrap its newly proposed blanket surveillance powers and to introduce prior judicial control over its intelligence and security agencies.

VIII. Police hacking Bill

Early in 2013 the former Dutch Minister of Security and Justice Ivo Opstelten introduced the idea to authorize the Dutch police force to hack into any computer – home and abroad – and to enable the police to demand that people decrypt their encrypted computer files. This was subsequently put into a legislative proposal which is currently before the Dutch House of Representatives.[17] Under this Bill, the Dutch police will be authorized to hack into *any* ICT device, including car systems, smartphones and even people's pacemakers. In addition to being in violation of the right to privacy, this Bill as currently drafted will thus also endanger road security and physical safety. In addition, acting unilaterally and without prior foreign permission, the Dutch police will be authorised to hack into any foreign computer, thus operating in violation of the principle of territorial jurisdiction under public international law and setting a perilous precedent.

We recommend the Human Rights Council to urge the Netherlands to either withdraw its current police hacking Bill or to bring it in line with the highest standards of the right to privacy as well as public international law.

IX. Electronic Health Records (EPD)

In April 2011, after long and intensive debates about privacy and security concerns, the Dutch Senate unanimously rejected a Bill under which a centralized Electronic Health Record system (*Elektronisch Patiëntendossier*, EPD) would have been introduced for every Dutch citizen (except for those who had opted-out in advance). However, as soon as this Bill had

[16] On the issue of the international exchange of personal data regarding Dutch citizens between Dutch and foreign secret services, a Dutch coalition of citizens and NGOs (including Privacy First) is currently conducting legal proceedings against the Dutch government and has also intervened in the current British case of Big Brother Watch *et al.* before the European Court of Human Rights (Application no. 58170/13; see https://www.privacyfirst.eu/court-cases/648-appeal-and-european-intervention-in-citizens-v-plasterk-case.html.

[17] See *Wetsvoorstel Computercriminaliteit III* (Legislative proposal on Cybercrime III) available at https://www.rijksoverheid.nl/actueel/nieuws/2015/12/22/wetsvoorstel-computercriminaliteit-bij-tweede-kamer-ingediend (in Dutch).

been rejected, no such thing as 'the end of history' of the EPD ensued. On the contrary, relevant market players (including ICT and insurance companies) immediately started working on a new, privatized start for the exact same yet non-subsidized EPD. The Dutch Minister of Health subsequently endorsed the idea of introducing this same centralized EPD without government funding and control (but through an 'opt-in' instead of 'opt-out' for citizens), thus circumventing the Senate and largely ignoring privacy concerns. This was then even reinforced by a majority motion in the Dutch House of Representatives which asked the Minister to request relevant organizations (including privacy experts) to facilitate a continuation *(doorstart)* of this same EPD, which in turn prompted the Senate to respond that it would only support a *regional* instead of a centralized version of the EPD *under very strict privacy and security conditions*. Privacy First has consistently supported the latter view and, since early 2014, Privacy First has even started a national campaign to this effect: www.SpecifiekeToestemming.nl (regarding the right of patients to specific, prior and fully informed consent to share their medical data). However, since then, technical connections to the American-built central infrastructure of the EPD (called LSP or *Landelijk SchakelPunt*, Central Switch Point) have gradually expanded and are effectively becoming compulsory for all medical professionals in the Netherlands, mainly through contracts with insurance companies. This is putting heavy pressure on the professional right to medical confidentiality and patient privacy in the Netherlands, since these rights cannot be guaranteed to be respected in the LSP infrastructure.[18] Accordingly, we hereby recommend as follows:

We recommend the Human Rights Council to urge the Netherlands to facilitate the development of alternative (regional) 'opt-in' EPD systems which comply to the highest standards of 'privacy by design'.

X. Public transport chip cards (*OV Chip Card*)

The Dutch OV Chip Card (*OV-chipkaart*[19]) is a contactless RFID smart card system which since 2005 has gradually been introduced on all public transport in the Netherlands, including on trains, metros, trams and buses. The OV Chip Card replaced the former paper *strippenkaart* completely in late 2011. Three versions of the OV Chip Card are currently available: a disposable OV Chip Card, an anonymous OV Chip Card and a personalized OV Chip Card (the latter holding the owner's name, photograph and date of birth). In addition to the technical differences between the old paper *strippenkaart* and the electronic OV Chip Card, a difference lesser known but highly relevant from a privacy perspective concerns the degree of anonymity between the two. With the paper *strippenkaart*, everyone had a guaranteed right to travel freely and anonymously. However, with the introduction of the "anonymous" OV Chip Card, the freedom of anonymous travel has practically disappeared. This is due to the fact that 1) every "anonymous" OV Chip Card has a unique identification number inside its RFID chip and 2) all transactions made with this chip are being recorded and stored in databases of relevant banks and public transport companies. All of these data can

[18] See e.g. http://www.vphuisartsen.nl/nieuws/gp-organization-vphuisartsen-fights-fundamental-court-case-health-information-exchange-consent-design/. This court case by GP organization *VP Huisartsen* regarding the legality of the LSP is currently before the Dutch Supreme Court.
[19] The full name in Dutch is *Openbaar Vervoer chipkaart* (Public Transport chip card).

subsequently be requested and combined by Dutch law enforcement or intelligence agencies. This essentially turns people's "anonymous" OV Chip Card into a (potential) government surveillance card through which travel patterns of people who thought they were travelling "anonymously" can easily be traced (and predicted). In addition to this, travel discounts are only available on personalized OV Chip Cards, thus forcing many people to give up their right to anonymous travel in order to save money. In our view, this situation comes down to a double violation of the right to privacy and anonymous (domestic) travel.

We recommend the Human Rights Council to urge the Netherlands to develop a truly anonymous OV Chip Card system which includes technical capabilities for discounts.