PRIVACY FIRST

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

28 November 2011

Contact information:
Privacy First Foundation *(Stichting Privacy First, SPF)*
PO Box 71909
1008 EC Amsterdam
The Netherlands
Phone: +31 (0)20 81 002 79
Email: info@privacyfirst.nl
Website: www.privacyfirst.nl

I. Introduction and overview

During its previous UPR session in April 2008, the Netherlands received the following 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]

Since '9/11', especially since the Madrid and London bombings of 2004 and 2005, 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).[3] Many of these measures were introduced in the name of 'counter-terrorism', yet mostly without their necessity having been established and often without any element of choice for individual citizens. Examples include massive storage of telecommunications (data retention), biometric passports, ID cards and related databases, RFID-cards for public transport, Automatic Number Plate Recognition, Passenger Name Records and body-scans at airports, Electronic Child Records and Electronic Health Records, loss of medical privacy and professional confidentiality due to compulsory registration and application of Diagnosis Treatment Combinations (*DBC*s), heavily increased CCTV surveillance, preventive searching of persons and houses without reasonable suspicion and automatic profiling, telephone and internet wiretapping without judicial oversight. All of these measures should 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 an excellent opportunity for international scrutiny and the sharing of best practices between UN Member States.

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] For an overview in English, see Privacy International, *Netherlands – Privacy Profile* (January 2011), https://www.privacyinternational.org/article/netherlands-privacy-profile.

II. Biometric passports and ID cards

In June 2009, in order to implement the European regulation on passport security, the Dutch Senate (without a vote) passed a new law which introduced biometric passports and ID cards containing an RFID-microchip with digital information about the passport owner.[4] Under the European regulation, a digital facial image and the fingerprints of the passport owner had to be stored on this microchip for verification purposes and in order to prevent fraudulent use.[5] However, by including provisions on the storage of the biometric data of all Dutch passports and ID cards in a national database for *identification* (1:n) instead of *verification* (1:1) purposes as well as criminal investigation, disaster control and intelligence purposes (including counter-terrorism), the Netherlands had legislated in order to go a giant leap further than was originally intended by the European regulation. This 'national fingerprint database' would thus come to include the fingerprints of every Dutch citizen, regardless of any criminal activity, hence turning people's travel documents for personal use into security documents for use by the State. Citizens would hardly have any control over the biometric information stored about them. Many experts had also warned that privacy violations, function creep, data breaches and biometric identity theft on a large scale would become inevitable. Both the Dutch Data Protection Authority and other experts had consequently found this new law on biometric passports to be in serious violation of the right to privacy and had warned against its entry into force.[6] Only weeks after its relatively silent adoption by the Senate, this led to a broad coalition of NGOs putting the new Dutch Passport Law (along with many other privacy concerns) on the agenda of the UN Human Rights Committee (HRC).[7] The HRC subsequently issued the following Concluding Observation:

> *"The State party should amend its legislation to ensure that its counter-terrorism measures do not conflict with article 17 of the [ICCPR] and that effective safeguards, including judicial oversight, are in place to counter abuses."*[8]

Not only did the adoption of the new Passport Law trigger the HRC to issue this statement, it also triggered a lot of debate, unrest and turmoil in Dutch society at large, including the establishment of several new NGOs and a large series of political and legal protests which continue to this day.[9] More than a dozen different court cases against this Passport Law have since been instituted, including an early request by Dutch NGO *Vrijbit* for interim measures

---

[4] *Wijziging van de Paspoortwet in verband met het herinrichten van de reisdocumentenadministratie*, adopted by the Dutch Senate on 9 June 2009. For the text of the law (in Dutch), see Parliamentary Documents I, 2008/09, 31 324 (R1844) A, 20 January 2009. This law partially entered into force on 21 September 2009.

[5] See *Council Regulation (EC) No. 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States*, arts. 1(2) and 4(3).

[6] See e.g. Data Protection Authority *(College Bescherming Persoonsgegevens)*, *Advies betreffende wijziging Paspoortwet i.v.m. de herinrichting van de reisdocumentenadministratie*, 30 March 2007, available (in Dutch) at http://www.cbpweb.nl/downloads_adv/z2007-00010.pdf; Tilburg University, Tilburg Institute for Law, Technology and Society (TILT), *Open Letter to Parliament*, 8 June 2009, available (in Dutch) at http://vortex.uvt.nl/TILTblog/?p=69#more-69; IKON Radio, 7 June 2009, *Nederland: rechtsstaat of snuffelstaat?*, available at www.ikonrtv.nl/daw/uitzending.asp?lIntItem=1&lIntEntityId=185. Cf. *S. and Marper v. United Kingdom*, ECtHR 4 December 2008, Appl. Nos. 30562/04 and 30566/04.

[7] See http://www.njcm.nl/site/press_releases/show/25.

[8] UN Doc. CCPR/C/NLD/CO/4 (11 August 2009), para. 15.

at the European Court of Human Rights. The largest (collective, civil) court case against the new Passport Law was initiated by Privacy First and 22 Dutch citizens in May 2010 and is currently at the appeals stage.[10] Other (individual, administrative) court cases are currently before the Dutch Council of State (*Raad van State*). In April 2011, due to overwhelming societal, political, legal and scientific pressure as well as technical difficulties in enrolling people's biometrics and developing the national biometric database, the Dutch Minister of the Interior announced that he would halt the entire project and revise the Dutch Passport Law accordingly.[11] Nonetheless, the Minister also stated that 'a national biometric database would remain the long-term goal of the Dutch government'. This leads us to our first recommendation:

We hereby recommend the Human Rights Council to urge the Netherlands to withdraw its long-term plans and preparations to develop a national biometric database.

III. Mobile fingerprint scanners

The Dutch government is currently considering the introduction of wireless mobile 'fingerprint scanners', to be generally used in the streets of the Netherlands by the Dutch police. A pilot project to publicly test these fingerprint scanners is being conducted between November 2011 and early 2012 by four regional police forces[12] as well as the Royal Netherlands Marechaussee (military police).[13] The primary objective of these scanners is to detect illegal immigrants by digitally verifying the fingerprints of individuals against those in the national database for asylum seekers (*Basisvoorziening Vreemdelingen*, BVV) as well as the European Visa Information System (VIS). Secondary purposes include the detection of fugitives and persons with false identities or outstanding fines.[14] However, similar use of mobile fingerprint scanners in the United Kingdom has already led to arbitrary practices, ethnic profiling and discrimination, mainly targeting persons of African and Asian descent.[15] In addition, recent experiences with biometric passports and ID cards in the Netherlands show biometric error rates in fingerprint verification between 21 and 25%, thus proving this technology completely unsuitable for large-scale use. Besides mass violations of people's privacy and physical integrity, the use of mobile fingerprint scanners will probably shift from one goal to the next (function creep), eventually treating every Dutch citizen as a

---

[9] See e.g. Vincent Böhre, *Happy Landings? Het biometrische paspoort als zwarte doos* (research report commissioned by the Dutch Scientific Council for Government Policy (WRR), The Hague, October 2010), http://www.wrr.nl/content.jsp?objectid=5525.

[10] See http://www.privacyfirst.nl/acties/proces-tegen-de-paspoortwet.html.

[11] See Parliamentary Documents II, 2010/11, 25764, 46 (26 April 2011).

[12] Amsterdam-Amstelland, Rotterdam-Rijnmond, Hollands Midden and Noordoost-Gelderland.

[13] See Appendix to Parliamentary Documents II, 2011/12, 395, 25 October 2011.

[14] See e.g. Trouw, *Politie neemt vingerafdruk af op straat*, http://www.trouw.nl/tr/nl/4492/Nederland/article/detail/2810726/2011/07/20/Politie-neemt-vingerafdruk-af-op-straat.dhtml (20 July 2011); Binnenlands Bestuur, *Politie scant vingerafdruk op straat*, http://www.binnenlandsbestuur.nl/openbare-orde-en-veiligheid/nieuws/nieuws/politie-scant-vingerafdruk-op-straat.1411906.lynkx (19 July 2011).

[15] See e.g. BBC, *More minorities scanned for ID*, http://news.bbc.co.uk/2/hi/uk_news/7913073.stm (27 February 2009).

potential suspect. Not only will this lead to many cases of unjustified arrest and detention, it will also lead to mutual feelings of insecurity, irritation and perhaps even aggression. It follows that, both from a privacy and from a broader human rights point of view, the introduction of mobile fingerprint scanners should be abandoned.

We recommend the Human Rights Council to urge the Netherlands to halt developments towards the introduction of mobile fingerprint scanners.

IV. OV Chip Card

The Dutch OV Chip Card (*OV-chipkaart*[16]) 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 on 3 November 2011. At the start of a journey, a traveler checks in by holding his/her OV Chip Card up to an RFID-reader in the vehicle or at the station. A check-in fee is then debited from the card. When leaving the vehicle or the station, the passenger checks out by holding the card up to the reader and the check-in fee is refunded minus the fare for the journey actually made. 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 subsequently be requested and combined by Dutch law enforcement or intelligence agencies.[17] 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.

[16] The full name in Dutch is *Openbaar Vervoer chipkaart* (Public Transport chip card).
[17] See e.g. Rathenau Instituut, *Databases. Over ICT-beloftes, informatiehonger en digitale autonomie* (The Hague, November 2010), at 32-41, http://www.rathenau.nl/publicaties/databases-over-ict-beloftes-informatiehonger-en-digitale-autonomie.html.

V. Automatic Number Plate Recognition (ANPR)

The Dutch government is currently preparing to present a Bill to Dutch Parliament regarding the introduction of ANPR on an extensive, national scale for criminal investigation purposes, despite the fact that this Bill has already been declared illegal by the Dutch Data Protection Authority (DPA).[18] 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 1) unnecessary and 2) disproportionate to the aims of criminal investigation and the detection of fugitives. 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.

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 ANPR system in compliance with modern demands of 'privacy by design'.

VI. Automatic border control (@MIGO)

Early in 2011 it emerged[19] that the Dutch government has for years been planning to implement a highly privacy-invasive system of ANPR-like border control which is set to enter into force on January 1st 2012. Under this new, high-tech surveillance system called @MIGO (or @migo-boras[20]), each and every vehicle which crosses the Dutch-German or Dutch-Belgian border will be photographed (front and side, instead of 'just' number plates) and thoroughly screened through various databases, many of which remain unknown. It will thus even be possible to photograph and (biometrically) identify both the driver and passenger(s) inside the vehicle. However, the details of @MIGO remain confidential and relevant Dutch governmental organisations have until now preferred not to answer any questions about it. As far as Privacy First is currently aware, these organisations include the Dutch police, Immigration Service (IND), Royal Marechaussee (military police), TNO[21] and the General Intelligence and Security Service (AIVD). Primary goals of the project seem to be detection of

[18] See College Bescherming Persoonsgegevens (CBP) (Dutch DPA) 28 February 2011, *Vastleggen en bewaren kentekengegevens door politie - CBP adviseert wetsvoorstel niet in te dienen*, http://www.cbpweb.nl/Pages/adv_z2011-00044.aspx (in Dutch). Compare Federal Constitutional Court of Germany 11 March 2008, http://www.bverfg.de/entscheidungen/rs20080311_1bvr207405.html (in German).

[19] See Dimitri Tokmetzis, *Staat bouwt digitale hekken aan de grenzen*, http://sargasso.nl/archief/2011/01/19/staat-bouwt-digitale-hekken-aan-de-grenzen/ (19 January 2011). See also a summary of Bart de Koning's subsequent speech at the CPDP Conference in Brussels (26 January 2011), http://www.njcm.nl/site/newsposts/show/273.

[20] @migo-boras means '*Automatisch Mobiel InformatieGestuurd Optreden* (Automatic Mobile Intelligence Led Operations) - *better operational result and advanced security*'.

[21] See Netherlands Organisation for Applied Scientific Research (TNO), *@MIGO: Border Control*, http://www.tno.nl/content.cfm?context=thema&content=markt_product&laag1=893&laag2=194&laag3=192&item_id=1393&Taal=2.

illegal immigration and human trafficking. An investigation into the compliance of @MIGO with the European Schengen agreements is currently being conducted by the European Commission. Media attention about the project has been very scarce: Dutch national newspapers NRC Handelsblad and NRC Next recently published a similar article about it,[22] which was subsequently picked up by German WDR Online[23] and ZDF Television. In Dutch parliament, no questions seem to have been asked about it yet. No specific legislation around its implementation seems to have 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, implementation of @MIGO will *a priori* constitute a massive violation of the right to privacy.

We recommend the Human Rights Council to urge the Netherlands to clarify and suspend @MIGO, at least until relevant legislation has been introduced into Parliament.

VII. 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 been rejected, no such thing as 'the end of history' of the EPD ensued. On the contrary, relevant market players and special interest groups 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.[24] 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. We hereby confirm this position and accordingly recommend as follows:

We recommend the Human Rights Council to urge the Netherlands to develop an alternative (regional) 'opt-in' EPD system which complies to the highest standards of 'privacy by design'.

---

[22] For a digital summary, see NRC.nl, *Nut van nieuw camerasysteem langs de grenzen niet bewezen*, http://www.nrc.nl/nieuws/2011/10/31/nut-van-nieuw-camerasysteem-langs-de-grenzen-niet-bewezen/ (31 October 2011).

[23] See WDR.de, *Kamerakontrolle an den Grenzen: Niederlande planen Autoüberwachung*, http://www1.wdr.de/themen/panorama/kontrolle102.html (17 November 2011).

[24] See http://www.privacyfirst.nl/aandachtsvelden/gezondheid-a-privacy.html For a comparison of opposite developments in the United Kingdom, see *Department of Health press release 22 September 2011, Dismantling the NHS National Programme for IT*, http://mediacentre.dh.gov.uk/2011/09/22/dismantling-the-nhs-national-programme-for-it/.

VIII. Profiling

In today's society, more and more use is being made of datamining techniques to discover patterns in large amounts of digital information, 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, 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, accountability, freedom of choice and the right to correction and removal of personal data.