Contribution Bits of Freedom to the Second Universal Periodic Review of the Netherlands by the United Nations Human Rights Council

November 2011

Contact information
Bits of Freedom
Ot van Daalen
P.O. Box 10746
1011 ES Amsterdam
The Netherlands
ot.vandaalen@bof.nl
+31 6 54386680
www.bof.nl

Summary of recommendations

1. Overarching Privacy Strategy
   We recommend the Human Rights Council to insist that the Netherlands develops a set of criteria for all policies restricting the right to privacy. These criteria should be applied to policy proposals and existing policy, and to enforcement measures. The set of criteria would have to ensure that each potential privacy restriction is necessary in a democratic society and proportionate towards a legitimate aim. The privacy risks and impact, not only of the policy in isolation, but also in relation to other policies, should be analysed in advance. All privacy infringing policies should be periodically reviewed and evaluated after implementation.

2. Data retention
   We recommend the Human Rights Council to insist that the Netherlands (1) revokes the implementation of Directive 2006/24/EC, (2) restrains from obliging telecommunication providers to retain traffic and/or location data of its subscribers, and (3) takes action against the European Commission to annul the Data Retention Directive.

3. Restriction of access to information and the monitoring and blocking of internet traffic
   We recommend the Human Right Committee to insist that the Dutch government explicitly rejects any measures which would lead to the blanket monitoring of internet traffic and that all governmental powers to render information inaccessible should be subject to prior judicial supervision. In order to allow for parliamentary control, we also recommend the Human Rights Committee to demand from the Netherlands that any government action restricting the right to communication freedom and privacy is explicitly based on a law.

4. The introduction of a 'data breach notification obligation'
   We recommend the Human Rights Council to insist that the Netherlands introduces an obligation to notify those whose data have been affected and a central authority as soon as possible, after an organisation becomes aware of a potential breach of security which could lead to accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access to or disclosure of personal data.

Introduction

5. Bits of Freedom is the Dutch digital rights organisation (NGO), focusing on privacy and communications freedom in the digital age. Bits of Freedom is one of the founders and a member of European Digital Rights (EDRi). She strives to influence legislation and self-regulation, on a national and a European level.

6. During previous Universal Periodic Reviews of various states, the Dutch government recommended to guarantee free and unrestricted access to the internet and to remove all internet monitoring and control facilities restricting the use of the internet thereof.[1] Bits of Freedom supports this foreign policy but cannot deny the contradiction between these recommendations and Dutch domestic policy.

7. In this report Bits of Freedom wishes to inform the Human Rights Committee on recent developments concerning the violation of privacy and internet freedom by the Dutch government.

Overarching Privacy Strategy

8. The Netherlands lacks an overarching privacy framework for the evaluation of its policies. Meanwhile, the Dutch constitution prohibits judicial review of the constitutionality of such policies. As a result, the Dutch government does not thoroughly review the impact of policy proposals on the right to privacy, nor thoroughly examines the necessity and proportionality thereof and often ignores concerns raised by civil society and the Dutch data protection authority ('DPA'). After adoption, the Dutch government often does not seriously address the problems associated with the lack of such a framework.

9. This is illustrated by the ongoing privacy infringements related to the central telecommunications database for investigative purposes (the Centraal Informatiepunt Onderzoek Telecommunicatie, 'CIOT'). This database stores the personal data of all Dutch communications subscribers and is accessed on a massive scale: almost three million times per year in 2009. Year after year, internal and external auditors continue to find grave privacy breaches in relation to the operation of CIOT.[2] In fact, the DPA in 2011 found that 9 out 11 reviewed data requests via CIOT of the Dutch national police were without legal basis.[3] The government has, so far, not taken any serious action to prevent infringements and even embraced an increase in access requests per year as an explicit policy goal.[4]

10. Given the above, it is crucial that every privacy-restricting policy proposal of the Dutch government is subjected to a strict test in order to ensure conformity with the right to privacy and related rights. In addition, existing policy needs to be reviewed and subjected to this test on a periodic basis. The Dutch government, by not consistently and thoroughly applying such strict criteria, ignoring advice by the DPA and dismissing concerns by civil society infringes the rights set out under article 12 Universal Declaration of Human Rights (UDHR), article 17 International Covenant on Civil and Political Rights (ICCPR) and article

[1] See for example the Report of the Working Group on the Universal Periodic Review Islamic Republic of Iran (15 March 2010), recommendation 58, Report of the Working Group on the Universal Periodic Review Kazakhstan (23 March 2010), recommendation 123. 97-21 and Report of the Working Group on the Universal Periodic Review Lao People's Democratic Republic (15 June 2010), recommendation 56, 97-3.

[2] See the audit reports of the CIOT of 2008, 2009 and 2010, to be found at https://rejo.zenger.nl/focus/wob-20090703-eindrapport-audit-2008.pdf, https://rejo.zenger.nl/files/eindrapport-audit-ciot-en-omgevingen-2009.pdf respectively http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2011/08/02/eindrapport-audit-ciot-2010/eindrapport-audit-ciot-2010.pdf.

[3] College Bescherming Persoonsgegevens., Onderzoek CIOT-bevragingen, Onderzoek Dienst Nationale Recherche, z2010-00170, Rapport definitieve bevindingen April 2011.

[4] See *Kamerstukken II* 2011/12, 33 000 VI, nr. 2, p. 60.

16 Convention on the Rights of the Child (CRC).

11. *We recommend the Human Rights Council to insist that the Netherlands develops a set of criteria for all policies restricting the right to privacy. These criteria should be applied to policy proposals and existing policy, and to enforcement measures. The set of criteria would have to ensure that each potential privacy restriction is necessary in a democratic society and proportionate towards a legitimate aim. The privacy risks and impact, not only of the policy in isolation, but also in relation to other policies, should be analysed in advance. All privacy infringing policies should be periodically reviewed and evaluated after implementation.*

Data retention

12. In the Universal Periodic Review of 2008, the Netherlands was recommended to revise all anti-terrorism legislation to bring it in line with the highest human rights standards.[5] However, the Data retention-law (Wet bewaarplicht telecommunicatiegegevens[6], the implementation of the Data retention Directive 2006/24/EC) is still in place. The Dutch law obliges telecommunication companies to store telephone- and internet traffic data, as well as the location data of mobile devices, of all their subscribers. These have to be stored for six months for internet data and for twelve months for telephone data, even though the European directive permits to restrict the duration for a period of six months. There are no exceptions in the Dutch law to protect the confidentiality of communications of attorneys, medics, journalists and other professionals for which confidential communications is simply a necessity. At this very moment, millions of Dutch citizens are the victim of this privacy interference: it can be assumed that the location or traffic data of a Dutch citizen in 2010 was stored every six minutes on average.[7]

13. This law is clearly not in line with the highest human right standards and a clear breach of the rights protected under article 12 UDHR, article 17 ICCPR and article 16 CRC. The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression concluded that the collection of information about individuals' online activities by States, constitutes a violation of Internet users' right to privacy, and undermines people's confidence and security on the Internet, thus impeding the free flow of information and ideas online.[8] More specifically, it is no surprise that the European Data Protection Supervisor calls data retention the most privacy invasive instrument ever adopted by member states in the EU.[9] European Constitutional Courts have indeed rejected the principle of blanket and indiscriminate telecommunications data retention out of hand (in Romania) or have firmly rejected the national implementation laws (in case of Germany, Cyprus, Bulgaria and in the Czech Republic). Moreover, cases against other national implementation laws are pending in Hungary and Ireland.[10] Meanwhile, the Dutch government has failed to demonstrate the necessity and effectiveness of this law.

14. Given the above, the Dutch government should have followed up on the recommendations

5 Universal Periodic Review, Human Rights Council, 13 May 2008 A/HRC/8/31, recommendation no. 29.
6 Wet bewaarplicht telecommunicatie stb. 2009/333.
7 CEPOS, Logningsbekendtgørelsen bør suspenderes med hendblik på retsikkershedsmæssig revidering, p. 4, 20 July 2010, based on official figures for 2008 from the Danish Ministry of Justice, http://www.cepos.dk/publikationer/analyser-notater/analysesingle/artikel/afvikling-af-efterloen-og-forhoejelse-af-folkepensionsalder-til-67-aar-vil-oege-beskaeftigelsen-med-1370/.
8 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 16 may 2011, par. 82.
9 Conference 'Taking on the Data Retention Directive', Brussels, 3 December 2010, 'The moment of truth for the Data Retention Directive' by European Data Protection Supervisor Peter Hustinx.
10 European Digital Rights, Shadow evaluation report on the Data Retention Directive (2006/24/EC), 17 April 2011, to be found at: http://www.edri.org/files/shadow_drd_report_110417.pdf.

of the Universal Periodic Review of 2008 and revoked its Data retention law. It should in the meanwhile have started an action against the European Commission to annul the Data Retention Directive because it is not in line with the right to privacy as set out in the international instruments mentioned above. It has failed to do so, however. Instead, it has repeatedly attempted to defend this blatant privacy violation, in the Dutch parliament and on a European level.[11]

15. *We recommend the Human Rights Council to insist that the Netherlands (1) revokes the implementation of Directive 2006/24/EC, (2) refrains from obliging telecommunication providers to retain traffic and/or location data of its subscribers, and (3) takes action against the European Commission to annul the Data Retention Directive.*

Restriction of access to information and the monitoring and blocking of internet traffic

16. Several policy proposals launched or facilitated by the Dutch government would ultimately lead to the restriction of access to information or even the monitoring and blocking of internet traffic and thus restrict the right to privacy (article 12 UDHR, article 17 ICCPR and article 16 CRC) and the right to freedom of expression (article 19 UDHR and article 19, paragraph 2, ICCPR).

17. Firstly, the Dutch government in 2010 launched draft legislation which would give the public prosecutor the authority to block access to information on the internet without judicial supervision.[12] The lack of judicial supervision risks restricting access to lawful material or self-censorship. Despite very public opposition from civil society, the Dutch government has not revoked the draft.

18. In addition, the Dutch government in 2011 announced its new copyright policy.[13] It intends to restrict the right to make a private copy from works distributed without authorisation of a copyrightholder. The measure is directed at a very private activity: downloading material from the internet in the privacy of one's own home. Ultimately, such a measure can only be enforced by monitoring the internet traffic of all internet users in order to effectively identify and block copyright infringing material.

19. The same policy also envisages allowing courts to order Internet Service Providers (ISPs) to block access to entire websites or services which facilitate copyright infringement. All measures, which could lead to the imposition of far-reaching monitoring or blocking obligations on internet service providers are fundamentally at odds with the right to freedom of expression, since these lead to overblocking and because such a measure has chilling effects. Depending on the implementation of these blocking orders, these could also require internet surveillance.

20. In addition, the government in the past years increasingly takes its recourse to facilitating public-private partnerships in order to introduce internet policy. This has a major drawback: the Dutch parliament cannot fully check these measures as it would be able to do with legislative proposals. Moreover, the Dutch freedom of information laws do not apply to

[11] See for example *Handelingen II* 15 juni 2011, 32185 and the analysis of the Dutch input on the effectiveness of the Data retention directive published on https://www.bof.nl/2010/12/16/waardeloze-inbreng-justitie-voor-europese-evaluatie-bewaarplicht/.

[12] See Conceptwetvoorstel versterking bestrijding computercriminaliteit, 28 July 2010, to be found at http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2010/07/28/wetsvoorstel-versterking-bestrijding-computercriminaliteit/wetsvoorstel.pdf.

[13] *Kamerstukken II* 2011/12, 29 838, nr. 29.

negotiations between private parties.

21. The above proposals and the increasing use of public-private partnerships to introduce internet policy infringes on the right to privacy of the Dutch population (article 12 UDHR, article 17 ICCPR and article 16 CRC) and the right to freedom of expression (article 19 UDHR and article 19, paragraph 2 ICCPR).

22. *We recommend the Human Right Committee to insist that the Dutch government explicitly rejects any measures which would lead to the blanket monitoring of internet traffic and that all governmental powers to render information inaccessible should be subject to prior judicial supervision. In order to allow for parliamentary control, we also recommend the Human Rights Committee to demand from the Netherlands that any government action restricting the right to communication freedom and privacy is explicitly based on a law.*

The introduction of a 'data breach notification obligation'

23. Every day, the privacy of Dutch citizens is infringed when personal data is collected without necessity, and if stored, not secured sufficiently. Bits of Freedom since approximately one and a half years maintains a list of personal data breaches in The Netherlands which are known to the public. The real number of incidents is likely to be bigger: it is likely that most incidents are not reported, and even if they are, do not receive attention from the media. The list demonstrates that all organisations processing personal data are vulnerable to breaches. It also shows that most frequently, the breach is caused by insufficient security measures.

24. In addition, the Dutch government should impose a 'data breach notification obligation' for all organisations dealing with personal data of Dutch citizens. When an organisation becomes aware of a potential breach of security which could lead to accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure of personal data, it should inform those whose data has been affected and a central authority as soon as possible. All these breaches should be registered in a public registry. The Dutch government to date has not introduced such an obligation. This endangers the right to privacy (article 12 UDHR, article 17 ICCPR and article 16 CRC) of Dutch civilians.

25. *We recommend the Human Rights Council to insist that the Netherlands introduces an obligation to notify those whose data have been affected and a central authority as soon as possible, after an organisation becomes aware of a potential breach of security which could lead to accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access to or disclosure of personal data.*