GLOBAL INFORMATION SOCIETY WATCH 2011

INTERNET RIGHTS AND DEMOCRATISATION

Focus on freedom of expression and association online

Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

This edition of Global Information Society Watch is dedicated to the people of the Arab revolutions whose courage in the face of violence and repression reminded the world that people working together for change have the power to claim the rights they are entitled to.

Printed in Goa, India
by Dog Ears Books & Printing

Global Information Society Watch
Published by APC and Hivos
South Africa
2011

ISSN: 2225-4625
APC-201111-CIPP-R-EN-PDF-0105
ISBN: 978-92-95096-14-1

APC and Hivos would like to thank the Swedish International Cooperation Agency (Sida) for its support for Global Information Society Watch 2011.

Sida

THE NETHERLANDS

A PRIVACY DISASTER? RFID CARDS FOR PUBLIC TRANSPORT IN THE NETHERLANDS

Institute for Information Law
Frederik Zuiderveen Borgesius
www.ivir.nl

Introduction

The ever-growing use of networked computers and databases makes life considerably easier. However, this also makes it easier to keep an eye on citizens. The average Dutch person is registered on 250 to 500 databases.[1] Is the Netherlands "sleepwalking into a surveillance society"?[2] Four years ago, a Big Brother Award was granted to the Dutch citizen: "He is the biggest threat to privacy according to the jury. Due to indifference – 'I have nothing to hide' – and lack of interest in what happens to their personal data, citizens share responsibility for the disappearance of privacy in the Netherlands."[3] This report deals with an example of a database system that threatens privacy: the new electronic payment system for Dutch public transport. The reaction that this system has provoked shows that Dutch citizens seem to be slowly waking up.

Database systems in the Netherlands

A recent report by the Rathenau Institute identifies three recurring problems regarding the introduction of database systems. First, there is often insufficient attention to security and privacy at the design phase. Second, frequently databases are designed with primarily the interests of the company or the state organisation in mind, overlooking the interests of the individual. Third, policy makers often have high expectations of the benefits of databases, which may not always be realistic.[4] A related problem is that sometimes people are not offered a choice on whether or not to participate in a system.[5] All these points are relevant for the OV-Chipcard system.

The OV-Chipcard is a card to pay for public transport services in the Netherlands, comparable with the Oyster card in London and the Octopus card in Hong Kong. Travellers can store credit on the OV-Chipcard, and pay for trips by checking in and checking out of public transport by holding the card against a card reader. One of the primary reasons to launch the OV-Chipcard project was to obtain insight into the use of public transport lines in order to improve efficiency.[6] The OV-Chipcard is supposed to replace all older public transport cards, and in some cities this is already the case.

The OV-Chipcard is RFID-equipped. RFID is short for "radio frequency identification", which is a technology that enables reading and storing information on RFID chips from a distance. RFID chips can be used in objects, such as entrance tags for buildings or library books, and may replace the ubiquitous barcode in the near future. RFID chips can also be inserted into living beings. A famous example is the Dutch discotheque Baja Beachclub, where certain customers had RFID chips implanted that enabled them to pay for their drinks by holding their arm close to an RFID reader.[7] The use of RFID chips in public transport cards and the subsequent storage of data gives us an early glimpse of what it means to live in the "Internet of Things".[8]

Is the Dutch travel card a privacy disaster?

Since the start of the project, the OV-Chipcard system has been plagued with problems. For example, in 2008 researchers found several flaws in the security of the card: it is possible to clone the card and to restore travel credit. Bart Jacobs, professor at the Digital Security Group of the University of Nijmegen, calls the

1 Schermer, B.W. and Wagemans, T. (2009) *Onze digitale schaduw. Een verkennend onderzoek naar het aantal databases waarin de gemiddelde Nederlander geregistreerd staat* (Our digital shadow. An exploratory study on the number of databases in which the average citizen is registered), Considerati, Amsterdam.

2 Richard Thomas, the English Information Commissioner, quoted in Ford, R. (2004) Beware rise of Big Brother state, warns data watchdog, *The Times*, 16 August.

3 www.bigbrotherawards.nl/index_uk.html

4 Munnichs, G. et al. (2010) *Databases. Over ICT-beloftes, informatiehonger en digitale autonomie* (Databases. About ICT promises, data hunger and digital autonomy), Rathenau Institute, The Hague, p. 26-27. www.rathenau.nl/en.html

5 Van 't Hof, C. et al.(2010) *Check in/check uit. Digitalisering van de openbare ruimte* (Check in/check out. Digitization of the public space), NAI, Rotterdam.

6 Vaststelling van de begrotingsstaten van het Ministerie van Verkeer en Waterstaat (XII) voor het jaar 2005 (Adoption of the budget of the Ministry of Transport (XII) for the year 2005), Parliament 2004-2005, 29 800 Chapter XII, Nr. 2, p. 126.

7 European Technology Assessment Group (2007) *RFID and Identity Management in Everyday Life*, Scientific Technology Options Assessment, Brussels, p. 41-42.

8 International Telecommunication Union (2005) *ITU Internet Reports 2005: The Internet of Things*, ITU, Geneva. www.itu.int

OV-Chipcard "technically (...) a nightmare" and a "privacy disaster".[9] He highlights five problems.[10]

First, the OV-Chipcard uses an old kind of RFID chip with poor security, which can be read by anybody using a card reader bought for only ten euro. The RFID chip will show its unique number to any card reader, which makes it possible to recognise and track persons carrying a card. Second, the card is an "open wallet": it is possible to change the contents on the card, unbeknownst to the person carrying the card. It is also possible to read the five last travels from a card.[11] Third, the transaction data of the card (for example, the location where someone gets on and off a bus and the exact times) are processed in a centralised database. "The former East German Stasi would have been jealous of such a database," according to Jacobs. Fourth, the OV-Chipcard is an identity-based system, while before the OV-Chipcard was implemented, one only had to show a ticket (this was an attribute). Jacobs poses the question: "Is it really necessary to tell who you are when you enter a bus? Do we want such a society?"[12] Lastly, although anonymous prepaid cards are available, they are very impractical. Unlike with personalised cards, it is not possible to make use of discount programmes. Most machines accept only coins, not paper money, to store credit on the card (they also accept bankcards, but that would break the anonymity of the process). Jacobs calls the anonymous cards "a sad joke" and concludes: "Privacy is the last thing the designers of the OV-chip system cared about – in sharp contrast with the principle of privacy by design."[13] The privacy and security issues do not end here. In 2010 the website of one of the participating public transport companies exposed the personal data of over 100,000 people,[14] and in 2011 different software packages to hack the cards were distributed on the internet.[15]

The risk of function creep

The creation of large databases always entails the risk of function creep. When data are collected for one purpose, new purposes to make use of those data usually present themselves soon. The OV-Chipcard system is no exception. For example, public transport companies want to use individual travel patterns for direct marketing purposes.[16] One could imagine the scenario that if one travels to Amsterdam, a coupon for a reduction at the local hamburger shop is offered, and if one often travels by first class, a coupon for a more expensive restaurant is offered.[17]

Now that the system is in use in a large part of the Netherlands, function creep has already started. On one occasion, the police asked a public transport company for a list with all identification numbers of the OV-Chipcards used at fare gates of two metro stations during a certain period. The police asked for the name, address, zip code, city of residence and any available photographs of the users. After initially refusing to provide the photographs, the public transport company provided all requested information to the police. It did, however, file a complaint with the court, arguing that the police should have obtained a written authorisation from the examining magistrate in order to demand the photographs. After much litigation, the Dutch Supreme Court confirmed that in this case, demanding the photographs without an authorisation was not in accordance with the law. In short, the Supreme Court held that photographs can contain sensitive personal data, namely data regarding race, which the police could only demand with a written authorisation.[18]

Not surprisingly, the OV-Chipcard project was met with some criticism, for example from Bits of Freedom. This is a Dutch digital rights organisation focusing on privacy and communications freedom in the digital age. Together with a large number of volunteers, the organisation strives to influence policy, for example, by organising campaigns and providing advice. Every year Bits of Freedom organises the Big Brother Awards, and gives an award to individuals, companies, government agencies and proposals that are most threatening to privacy. The public can suggest parties for nominations, and can vote which party should be granted the public award. Bits of Freedom has been following the developments around the OV-Chipcard from the beginning. The company holding the central database with travel data, Trans Link Systems, was nominated in 2003 and 2005. The Dutch railway company was granted a Big Brother Award in 2007 for its role in the OV-Chipcard. In 2011 Trans Link Systems had

9 Jacobs, B. (2010) Architecture Is Politics: Security and Privacy Issues in Transport and Beyond, in Gutwirth, S. et al. (eds) *Data Protection in a Profiled World*, Springer, Dordrecht, p. 292-293.

10 Ibid., p. 292.

11 Ibid., p. 293.

12 Ibid., p. 294.

13 Ibid., p. 294 (internal footnote omitted).

14 Zenger, R. (2010) Datalek: gegevens 168.000 reizigers gelekt via OV chipkaart website (Data breach: data from 168,000 passengers leaked through OV-Chipcard website), *Bits of Freedom*, 18 May. www.bof.nl

15 de Winter, B. (2011) Onzichtbare OV-chiphack vrij beschikbaar (Invisible OV-chip hack is freely available), *Webwereld*, 14 February. www.webwereld.nl

16 OV-Chipcard FAQ: www.ov-chipkaart.nl/faq/?n=64

17 Jacobs (2010) op. cit., p. 293.

18 Hoge Raad (Supreme Court Netherlands), 23 March 2010, *LJN* BK6331.

the dubious honour of winning both a jury award and the public award.

Student action against travel cards

Protests have not been limited to coverage on blogs, websites and traditional media. In early 2010 a group of students became worried and lodged a complaint with the Dutch Data Protection Authority.[19] Most Dutch students are eligible for a state-funded study grant, which includes the right to a card for public transport. The card offers free travel during the week, and discounted travel on the weekend (or vice versa if a student chooses so). An OV-Chipcard for students is personal and the RFID chip contains *inter alia* a unique number, the date of birth, the amount of credit loaded on the card, and the last ten transactions. A picture and the name of the student is printed on the card, but not stored on the RFID chip. When a student checks in and checks out of public transport, the data being processed include: the number of the card, the location where the student checks in, the date and exact time, the credit stored on the card and the credit used for the trip.

In their complaint to the Data Protection Authority the students argued first that on days on which they are eligible for free travel, there is no need to check in and check out. According to the students, it must be possible to open the gates of a metro station without registering a student checking in. Because of this their detailed travel data should not be collected. Second, the public transport companies stored the data – which were not sufficiently anonymised – for seven years in the central database. The students said that this was disproportionate. In addition, the students complained about the lack of transparency about what happens to the processed data. They also questioned whether the database with personal and travel data is sufficiently secured against data breaches and attacks from hackers. In short, the students doubted whether the companies complied with Dutch privacy regulation.[20]

The Data Protection Authority, which had been critical about the OV-Chipcard system from the beginning, started an investigation. In late 2010 the Authority published a scathing report about Trans Link Systems and three of the participating public transport companies. Two public transport companies and Trans Link Systems were found to store the data for a disproportionate period. (After the investigation Trans Link Systems changed the seven-year retention period to two years.) All three companies were found to process data in breach of privacy regulations.[21]

The Authority said that the Dutch railway company provided insufficient information to students. As the students are eligible for free travel during the week, there is no need to register the students checking in or out when they travel by train. However, the railway company fails to adequately inform students that they are not required to check in and out. Moreover, the general information provided by the railway company (such as posters in the stations and messages announced on the train) implies that everybody is required to check in and to check out. Therefore, the railway company did not have legitimate grounds to store and process the students' travel data. In short, each of the investigated companies was in breach of requirements of Dutch privacy regulation. The companies agreed to implement shorter retention periods. However, in July 2011 the Authority found that the railway company was still not informing students sufficiently. If the railway company still fails to inform students by the end of 2011, it has to pay penalties up to a maximum of 375,000 euro.[22]

Influence of citizens

In summary, the OV-Chipcard system is an example of how *not* to design a database system; privacy was clearly an afterthought during the design phase. Because of projects like this, the Dutch Data Protection Authority warns that the Netherlands might be turning into a "glass society".[23] However, there is some (very cautious) reason for optimism. Although the Dutch public seemed to be sleepwalking, a new trend seems to be emerging. Citizens and civil rights organisations make their voices heard more and more, for example on blogs and on social media. Mainstream media have started to report on these protests; sometimes they even make the evening television news.

In some cases, protests against the introduction of poorly designed database systems have influenced policy makers. In 2011 several government plans were adapted, largely because of privacy concerns. A government plan to store four fingerprints of each citizen in a database has been halted after

19 For an overview of the complaint see: www.clinic.nl/wiki/index.php?title=Handhavingsverzoek_studenten_OV-chipkaart

20 Wet bescherming persoonsgegevens (Dutch Data Protection Act).

21 CBP (2010) OV-bedrijven bewaren gegevens reisgedrag in strijd met de wet (Public transport companies store travel data in breach of the law), 9 December. www.cbpweb.nl

22 CBP (2011) CBP dwingt invoering bewaartermijnen reisgegevens af via dwangsom (Data Protection Authority ensures retention periods of travel data are shortened, under threat of penalties, 26 July. www.cbpweb.nl

23 Kohnstamm, J. and Dubbeld, L. (2007) Glazen samenleving in zicht' (Glass society in sight), *Nederlands Juristenblad*, 2007, p. 2369-2375.

civil rights organisations protested for years.[24] The Dutch senate voted against a law implementing national electronic infrastructure through which doctors could exchange patients' medical data, because of insufficient security and privacy safeguards.[25] A plan to introduce compulsory "smart" electricity meters that automatically send a message to the electricity company every fifteen minutes has been adapted as well, as electricity use can reveal much about your life such as your daily habits and rhythm. People are no longer required to have a smart meter installed.[26] So protests can eventually influence policy makers. However, it is important to protest at an early stage. Although protests seem to have some influence on the OV-Chipcard system now, it does not seem plausible that its main characteristics will be changed.

Action steps

- Try to convince policy makers who decide about new database systems to pay attention to privacy by design and to strengthen the position of the individual, for example, by making data processing more transparent. Tell them data should only be used for the original purpose.
- Make your voice heard at an early stage. Protest during the design phase when privacy-threatening systems are planned. Prevention is better than damage control at a later stage.
- The most important advice is to the Dutch public: do not embarrass yourself by winning another Big Brother Award. In other words, do not sleepwalk! ■

24 Letter of the Minister of Justice to the Parliament, 26 April 2011.

25 State press release, Eerste Kamer stemt tegen landelijk elektronisch patiëntendossier (Senate votes against national electronic patient record), 5 April 2011. www.rijksoverheid.nl

26 State press release, Slimme meter kan snel ingevoerd (Smart meter can be introduced soon), 22 February 2011. www.rijksoverheid.nl

GLOBAL INFORMATION SOCIETY WATCH 2011

In the year of the Arab uprisings **GLOBAL INFORMATION SOCIETY WATCH 2011** investigates how governments and internet and mobile phone companies are trying to restrict freedom online – and how citizens are responding to this using the very same technologies.

Everyone is familiar with the stories of Egypt and Tunisia. **GISWATCH** authors tell these and other lesser-known stories from more than 60 countries. Stories about:

PRISON CONDITIONS IN ARGENTINA Prisoners are using the internet to protest living conditions and demand respect for their rights.

TORTURE IN INDONESIA The torture of two West Papuan farmers was recorded on a mobile phone and leaked to the internet. The video spread to well-known human rights sites sparking public outrage and a formal investigation by the authorities.

THE TSUNAMI IN JAPAN Citizens used social media to share actionable information during the devastating tsunami, and in the aftermath online discussions contradicted misleading reports coming from state authorities.

GISWATCH also includes thematic reports and an introduction from Frank La Rue, UN special rapporteur.

GISWATCH 2011 is the fifth in a series of yearly reports that critically cover the state of the information society from the perspectives of civil society organisations across the world.

GISWATCH is a joint initiative of the Association for Progressive Communications (APC) and the Humanist Institute for Cooperation with Developing Countries (Hivos).

GLOBAL INFORMATION SOCIETY WATCH
2011 Report
www.GISWatch.org

ISBN 978-92-95096-13-4
9 789295 096134

APC

HIVOS