Technology Assessment

Databases

The promises of ICT, the hunger for information, and digital autonomy

Geert Munnichs, Mirjam Schuijff & Michiel Besters (editors)

Rathenau Instituut

The **Rathenau Instituut** promotes the formation of political and public opinion on science and technology. To this end, the Instituut studies the organization and development of science systems, publishes about social impact of new technologies, and organizes debates on issues and dilemmas in science and technology.

Databases
The promises of ICT, the hunger for information, and digital autonomy

Rathenau Instituut
Anna van Saksenlaan 51

Correspondence:
P.O. Box 95366
NL-2509 CJ Den Haag

Telephone: +31 (0)70-342 15 42
Fax: +31 (0)70-363 34 88
E-mail: info@rathenau.nl
Website: www.rathenau.nl

Publisher: Rathenau Instituut
Translation: Balance, Amsterdam/Maastricht
Design: Smidswater
Photography: iStockphoto, Hollandse Hoogte
Print: Drukkerij Groen, Hoofddorp

This book is printed on FSC-certified paper.

This is a slightly revised translation of: Munnichs, G., M. Schuijff & M. Besters (red.): Databases – Over ICT-beloftes, informatiehonger en digitale autonomie. Den Haag, Rathenau Instituut, 2010.

First printing: 2012

ISBN/EAN: 978-90-77364-41-3

Preferred citation:
Munnichs, G., M. Schuijff & M. Besters (eds.): Databases - The promises of ICT, the hunger for information, and digital autonomy. The Hague, Rathenau Instituut, 2012.

Databases

The promises of ICT, the hunger for information, and digital autonomy

Editors
Geert Munnichs
Mirjam Schuijff
Michiel Besters

Foreword

Society is becoming rapidly digitised and a life without computers and the Internet is now inconceivable. The benefits are countless: improved communication, increased efficiency, and greater convenience for the citizen. Databases play an important role in all this, making it possible to store, exchange, and process enormous quantities of data. They are the digital backbone of our information society.

But as the present study shows, the use of databases is not without its problems. The study compares six digital information systems. It reveals that the interests of those about whom the data is being collected play only a subordinate role. This is shown not only by the often scanty attention devoted to securing data – with the citizen or consumer generally being the one who then suffers – but also in the generally tenuous legal position of the citizen. It is often difficult, for example, for someone to ensure that errors in databases are rectified. The use of databases can also lead to increasing dependence on government bureaucracy or the commercial sector. The citizen, client, or consumer increasingly risks losing control of who does what with his data. Databases are therefore not risk-free systems.

This study also warns against too high expectations regarding the possibilities opened up by ICT. Databases are not a solution to all problems. More data does not by definition lead to greater efficiency or improved services. A well-considered utilisation of databases and a responsible approach to the associated risks demand well thought-out choices regarding their design.

The digitisation of society is an ongoing process that will be shaped over the coming decades. Our dependence on the functioning of digital information systems will therefore only increase. With the recommendations formulated in this study, the Rathenau Instituut hopes to contribute to the debate on the future of our information-based society.

Jan Staman, director Rathenau Instituut

Index

Summary

This study demonstrates that the increasing use of databases in our digitised society does not come without risks and that we must learn useful lessons from our experience thus far.

Databases are being used in our society for a growing number of purposes. Databases seem to offer untold possibilities for storing, exchanging, processing, and analysing data. Companies use customer data to better tailor their product ranges to the customer's needs, our travels by public transport are surveyed in order to more efficiently deploy railway equipment, and healthcare providers exchange electronic files in order to provide better medical care.

This database use is not free of risks. Issues that arise are those such as: what purposes is the data used for, how secure is the data, how reliable is that data, what possibilities do citizens have for rectifying errors in registrations, and do databases actually contribute to achieving the purposes for which they were created?

This study examines these questions by presenting six case studies. We have opted to include the following topical examples:

- the public transport chip card and the kilometre charge for cars
- the electronic patient record
- the electronic child record
- customer profiles on the Internet
- the Schengen Information System
- the Municipal Personal Records Database

Four of the six case studies involve Dutch databases, while the remaining two (customer profiles and the Schengen Information System) concern international databases. The Dutch case studies are interesting for other countries because they have had comparable developments in the areas of e-health and electronic transport cards. Above all, the lessons to be drawn from those six cases have a broader base of applications than just the Netherlands.

The case studies focus on the architecture – or design – of the databases. The design does not refer just to the technical design of the databases – such as whether or not data is encrypted, or whether data is stored centrally or locally – but to the broader context within which the databases function as well. It also refers, for example, to the control citizens may exercise on the data collected about them, or the degree to which the use of databases reinforces citizen dependency or has the opposite effect of reinforcing their autonomy. The case studies show that, depending on a database's architecture, it can be used for other purposes, but that such other uses involve other risks.

The case studies also make it clear that these risks are often not adequately considered when designing a database. The security of personal information, for example, often continues to be an issue. The public transport chip card uses the Mifare Classic chip, which proved to be fairly simple to crack. That could have been prevented by choosing a different type of card. The security measures relating to the national electronic patient record, which look good on paper, seem to be vulnerable. That security could have been better by making more use of technical security measures that would simply make certain forms of access to the data impossible.

In addition, mistakes in registrations and the risk profiles based on those registrations are an issue. In the case of the electronic child record, this may result in children living under a certain combination of circumstances being considered as 'children at risk', even though that is not the case. Customers regarding whom companies gather data from the Internet may be excluded from particular services, such as obtaining an insurance policy or being forced to pay a higher premium, through a coincidental data match. An issue requiring attention in this regard is the generally weak legal position of those about whom the data is being collected. Statutory rights to examine and correct data are more than once rights on paper only, as they are difficult to exercise. Errors in data collection and processing are thus hard to rectify. The person who pays the price in this regard is generally the citizen, customer, or consumer.

The design of a database, furthermore, is often tailored to the needs and interests of the principal or operator (the government, transport company, or the company that collects customer data via the Internet), generally ignoring the needs and interests of citizens and consumers. As a result, the dependency aspects of these relationships are reinforced rather than reduced. As the case study on the Municipal Personal Records Database shows, ICT also offers possibilities to strengthen citizens' positions, for instance by allowing them more control over their data. That option is not often elected, however.

Finally, there are doubts regarding the effectiveness of database use. The case study on the Schengen Information System shows that databases do not always do what they were intended to do. Ambitions that are too high can work to their disadvantage. The Schengen Information System is on the brink of technical and organisational failure to meet a large number of its objectives.

Taking everything together, the case studies present a fairly disturbing image of what can go wrong with using databases in practice. These risks relate to the choices that are made regarding the architecture of the relevant database. Based on this, the following lessons can be learned for a well-considered database design:

Make as much use as possible of technical data-protection measures.

Strengthen the position of the citizen. Facilitate citizens' exercise of their rights to examine and correct their data and give them as much control as possible over their own data.

Keep it simple. Choose a well-defined goal and restrict data collection to the areas necessary for achieving that goal.

These three recommendations are closely interrelated. Securing data in a strong, technically sound manner will make it difficult or impossible to use that data for purposes such as tracing. The means and objective must therefore be examined in their mutual context. That makes decision-making regarding the utilisation of databases much more complex.

The exponential pace at which society is being digitised entails a similarly increasing need for well-considered database architecture. This requires an overview of the risks associated with database use and alternative design choices. That demands knowledge of ICT possibilities and impossibilities. In order to test the decision-making regarding database design, the design phase should be supervised by an independent agency, such as a national ICT authority. This agency would also have to ensure that the databases are operating properly. This leads to a fourth recommendation:

Ensure independent, continuous supervision of the design and operation of databases.

This study contains six case studies. These are preceded by an essay that provides an overview of the results of the case studies and the lessons that can be drawn from them.

1 Databases on display: lessons from Dutch experiences

1 Databases on display: lessons from Dutch experiences

Geert Munnichs, Michiel Besters & Mirjam Schuijff

1.1 Introduction: digital architecture

Our society is becoming ever more information-based, with more and more aspects of our lives being rapidly digitised. Never before have we made so much use of the opportunities offered by ICT, and never before have our daily lives left so many digital footprints in our wake, whether we are paying with a debit card, travelling using a public transport chip card, surfing the Internet or visiting the doctor. As Van 't Hof, Van Est and Daemen (2011) demonstrate, our trusted, physical world is being increasingly interwoven with the virtual world of bits and bytes. This study examines the role databases play in these developments. The term 'databases' refers to digital data files and information systems that enable large amounts of data to be stored, processed, analysed and exchanged with others. They are the digital backbone of our information-based society.

The digitisation of our society offers unprecedented possibilities for speeding communication, improving the efficiency of business processes, enabling better cooperation between government organisations, and making life more convenient for citizens and consumers. The possibilities that databases offer are being used increasingly. Supermarkets are using customer cards to be able to better gear their product ranges to customer needs; electronic child records are used to improve the communication between youth-services providers; and the Dutch government has established a system of municipal personal records databases so that citizens will not have to continually repeat their personal information every time they visit a different government agency. The use of databases has thus grown exponentially in recent years. A study performed at the behest of the Dutch Data Protection Authority showed that the average Dutch national is registered in at least 250 to 500 private or public databases (Schermer & Wagemans 2009).

There can be no doubt that the use of databases greatly benefits governments, companies, and citizens. The degree to which all sorts of digital services play a role in our daily lives also means that, realistically speaking, there is no going back. Nevertheless, there are issues that need to be raised regarding the use of digital data files and information systems. The study's primary assertion is that databases are not risk-free systems with unlimited possibilities. They are not neutral instruments that can be used indiscriminately to improve process efficiency or citizen convenience. They have their own logic and dynamic, which require that their use be a product of careful consideration.

This study examines the terms and conditions for responsible database use and formulates recommendations in that regard. The digitisation of society is an ongoing process that will be shaped over the coming decades. Enough experience with using databases has already been accrued to derive lessons for how we deal with digital information systems. Using six topical examples, we will discuss these experiences. We examine the following cases:

- the public transport chip card and the kilometre charge for cars
- the electronic patient record (EPR)
- the electronic child record (ECR)
- customer profiles on the Internet
- the Schengen Information System (SIS)
- the Municipal Personal Records Database

Four of the six case studies involve Dutch databases, while the remaining two (customer profiles and the Schengen Information System) concern international databases. The Dutch case studies are interesting for other countries because they have had comparable developments in the areas of e-health and electronic transport cards. Above all, the lessons to be drawn from those six cases have a broader base of applications than just the Netherlands.

The case studies focus on the architecture – or design – of the databases. In his contribution to this study regarding the EPR, Jacobs describes this architecture as '… the structural organisation of hardware, applications, processes and data streams, along with the related organisational consequences, within companies, governments or society in a broader sense'. This description makes it clear that the issue is not simply the technical design of databases – such as whether or not data is automatically deleted after a given period, encrypting data, or central or local storage of data – but also the broader context within which information systems function. The issue, for example, is how doctors deal with the required check of the Citizens Service Number on EPRs, or how the patients are afforded their rights to examine and correct their data.

With this study, we wish to show that, depending on a database's architecture, it can be used for other purposes, but that such other uses involve other risks. The study is not primarily intended to analyse the goals of such phenomena as kilometre charges or the Schengen Information System. We are not asking ourselves whether these ICT systems are the best way to reduce traffic jams or combat cross-border crime. We are primarily attempting to better understand the dynamic between the design, opportunities and risks of databases. The results, of course, may very well lead to reconsidering those objectives. The case study about the electronic child record raises, for example, the question of whether it is actually wise to formulate a risk profile for each child.

In this essay, we present the main results of the case studies and formulate policy recommendations. The case studies will be discussed by theme, with

several case studies being addressed for each theme. In the order given, we address the following topics: the purposes for which databases are employed (Section 2), data security (Section 3), data reliability (Section 4), the legal position of citizens (Section 5), the degree to which databases reinforce or undermine citizen autonomy (Section 6) and the effectiveness of database use (Section 7). We finish with our conclusions and recommendations (Section 8).

1.2 Improving efficiency, profiling and other use

As briefly indicated above, databases are used to improve communication, increase efficiency, or make life more convenient for citizens. These are recurring themes in the case studies. The digitisation of data files and information systems must result in organisational or business processes being improved, made faster or expanded. The modernisation of Municipal Personal Records Database must make government organisations more efficient, improve their cooperation, and improve their services to citizens. The implementation of the public transport chip card must result in more information about travel, so that public transport capacity can be more effectively and efficiently deployed.

Digitised data files also offer the possibility to process data in all sorts of ways. By linking various data files to one another and searching the data collected with computer applications using key terms or statistical relationships, a new understanding may be created of, for example, individual or group behaviour. Computerised searches of large data files is referred to as 'data mining' (Hildebrandt & Gutwirth 2008). This is how companies use online and offline customer data to identify patterns in consumer behaviour – customer profiles – based on which customers' 'potential' needs may be anticipated. This enables them to make offers that are tailored specifically to their customers.

Data mining and profiling are also creating new application possibilities. The data collected in an electronic child record (ECR) enables youth healthcare workers to use risk profiles to classify children according to risk category. Their score on risk factors must clarify what chance a child has of developing psychosocial problems. This must enable youth healthcare workers to identify potential problem children at an early stage so that preventative care may be provided.

Once they have been created, databases also easily lend themselves to other uses. Because digital data can be gathered, exchanged and processed much more easily and in greater volumes than data on hard copy, it takes relatively little effort to later use a database for a purpose other than that for which it was created. The electronic patient record (EPR) was initially intended primarily for the exchange of patient information between healthcare providers. During the EPR's development, however, the Dutch House of Representatives imposed a requirement that the medical record should also be viewable by patients on the Internet. When the original, Dutch version of this study was published in 2010, the EPR was still in the process of being developed. However, the Dutch Senate blocked the implementation of the EPR in the spring of 2011, amongst other reasons because of security and privacy concerns.

A second example of the alternate use of databases may be observed in the case of the public transport chip card. This card was created in order to more accurately track travellers' journeys so that staff and equipment could be deployed more efficiently. All journeys paid for with the chip card are recorded in a central database. That database also contains the personal details of travellers who use non-anonymous chip cards. Police officers and prosecutors can examine this central database. While the chip card database may be a handy tracking tool, it was never intended to be used that way. In his case study on the chip card, Teepe questions whether it is advisable to permit such use, which essentially gives police and prosecutors carte blanche to follow the comings and goings of ordinary citizens (see also Vedder et al. 2007).

These examples demonstrate that digitised data files can create new application possibilities that are often extremely useful, but which may have their drawbacks as well. Section 7 contains a more detailed discussion of the purposes for which databases are created and the question of whether databases do what they are supposed to do.

1.3 Procedural and technical security measures

The theme of security is the focal point in the political and societal debate concerning databases. As the case studies show, that focus is more than justified. The security of personal information is and will continue to be an issue. This is even more the case when extra-sensitive medical data is involved, for example in the electronic patient record (EPR) or electronic child record (ECR), or if the data provides a more intimate view of someone's private life, as it does with the public transport chip card or the customer data that companies collect on the Internet.

Notwithstanding the focus on this theme, various cases demonstrate that the security of personal data leaves much to be desired. In his case study on the public transport chip card, Teepe demonstrates that the chip card's implementation was accompanied by various incidents involving the card's security. The Mifare Classic chip, which is used for both the anonymous and registered versions of the chip card, can be cracked fairly easily. That could have been prevented if the company in charge, Trans Link Systems, had chosen a different type of card.

At first blush, the national EPR seems to be a positive exception to this poor security trend. While the EPR was being developed, a good deal of attention was devoted to security measures. For example, healthcare providers must meet strict security requirements (Well Managed Healthcare System) before

being permitted to connect to the national EPR network. In comparison with the regional electronic patient records, which had been around for some time, the national EPR appeared to be a step forward.

But issues arose even with regard to the intended security of the national EPR. According to Jacobs, the security measures taken were largely procedural and required strict compliance by participants in order to achieve the desired level of security. Healthcare providers are required to exercise extreme care with regard to the identification pass (the 'UZI pass') giving them access to the EPR, even though the healthcare sector is known for being insufficiently conscious of security risks. This, taken in combination with the large number (hundreds of thousands) of UZI passes, makes the system vulnerable.

This begs the question of whether an alternative architecture for the EPR, one that put more emphasis on technical security measures, would not have been a better option. In this regard, Jacobs refers to the possibility of decentralised storage of medical data, which would empower patients themselves to control access to their records. The main feature of this decentralised architecture would be that healthcare providers could only access patients' medical data with the patients' advance permission. According to Jacobs, there is no clear reason for the Ministry of Public Health, Welfare and Sport to have decided against the decentralised option. Perhaps this is attributable to the fact that the patient's position was not the top priority of the national EPR design from the outset, but only garnered attention later on.

Teepe also discusses the possibilities created by technical measures to increase vigilance in securing personal data. He does this by referring to the 'fat' version of the kilometre charge. In this system, a journey taken in a car would be stored so that only the motorist would be able to access it. The operator would only have access to the encrypted data based on which he may prepare an invoice, but he would not be able to see the actual journeys travelled by individual cars. Teepe presents this alternative – regarding which there is no certainty as to its possible implementation – in contrast to the degree of detail the public transport chip card provides of travellers' journeys.

The fat version of the kilometre charge would use zero-knowledge cryptography. In the past, this technology could not be applied to RFID chips like the public transport chip card. According to Teepe, however, that situation has recently changed. The question this prompts is whether public transport companies should make the transition to a zero-knowledge version of the chip card, or should in any case give the traveller the option of using it.

Finally, it is noted that securing databases is an ongoing process. Constant attention and monitoring are required to protect large ICT information systems such as the EPR from hackers and theft, as well as from careless use of access passes and passwords. At an expert meeting regarding the EPR in the Senate, Jacobs added that the supervision for ICT systems as large as the EPR requires the creation of an independent ICT authority. Agencies such as the Dutch Data Protection Authority and the Dutch Healthcare Inspectorate are ill-equipped for such duties (Dutch Senate 2009-2010a; see also Dutch Senate 2009-2010b).

1.4 Data reliability

In addition to sufficient security, data reliability is another important condition for a properly functioning database. Errors in data that is stored, exchanged or processed can have negative consequences for the people affected by that data. These errors might be the product of faulty data entry, identity theft, or problems with interpreting data.

One of the objectives on the electronic patient record (EPR) was to reduce the number on medication-related mistakes. Better communication between healthcare providers was intended to result in more reliable medical records. In his case study on the EPR, however, Jacobs warns against undue optimism. In his view, not all medication-related errors are the result of faulty communication between healthcare providers and, moreover, the EPR may result in certain errors – such as accidentally clicking on an adjacent type of medication on the screen – occurring more often.

To this can be added the fact that the exchange on medical records through the EPR requires a standard 'uniformity of language', which may lead to interpretation problems. Specifically, patient records do not contain only 'objective' information, such as that relating to medications or laboratory results, but 'subjective' information as well, such as patient complaints and physician diagnoses. Often, this subjective data can only be accurately understood in the context in which it appears. The question is whether the national standards for the registration of medical data – which are still under development – offer sufficient leeway for describing that context (Munnichs 2009). There is a risk that a lack of context could lead to interpretation problems and to mistakes in treatment.

The use of profiles to search through large data files also creates data reliability problems. In her case study of the electronic child record (ECR), Van der Hof shows that the large quantity of data collected about children and the risk profiles based on that data may serve to obfuscate the data that is actually relevant.

The ECR collects data for all children under age 19 regarding their physical, cognitive and psychosocial development, as well as regarding family issues such as divorced parents, unemployment or parental psychiatric problems. Children are classified in risk profiles depending on their scores regarding certain risk factors. In the example Van der Hof refers to, children are classified

as either 'yellow' (low risk), 'orange' (medium risk) or 'red' (high risk). This means that the focus is shifted from the individual child to the type of child. According to Van der Hof, the danger of this sort of classification is that a virtual identity will be created for a child that may not bear any resemblance to that child. A combination of circumstances could lead to a child unjustifiably being classified as 'red', and thus as a potential problem child, or as 'yellow' even though the child has issues requiring attention. Both cases will result in undesirable consequences for the child.

The use of customer profiles on the Internet by companies may even more seriously affect how, in this case, customers are treated. Hildebrandt and Van Dijk illustrate how earlier buying behaviour, personal data provided voluntarily by customers and unconsciously 'leaked' data – such as surfing and clicking behaviour on the Internet – provide companies with enormous quantities of customer data. Advanced computer applications are used to explore this sea of data and reveal statistical patterns in consumer behaviour. Marketers claim that the 'knowledge' they derive in this way can be used to predict future buying behaviour more accurately than the information provided by customers themselves in such forums as focus groups. This knowledge regarding consumer behaviour puts companies in a better position to aim targeted advertising at their customers.

Just as is the case with the ECR, customer profiling creates a virtual identity which may bear little resemblance to the real person associated with it. Hildebrandt and Van Dijk note that this may easily cause companies to miss the boat. Because large numbers of customers are involved, approaching customers in this way continues to be profitable for companies. From the consumers' perspective, however, this profiling is not without problems. After all, consumers have no opportunity to examine the data being collected about them, the customer profile into which they are categorised, or the consequences that that profile will have on how a particular company treats them. That need not be a problem when the issue at stake is misdirected 'targeted' advertisements, but the situation may be different if customers are excluded from certain services – such as insurance policies – or have to pay a higher fee for them because they have been 'misprofiled'.

1.5 Legal position of citizens

The previous sections make it clear that those affected by databases (citizens, patients, consumers) could suffer the consequences if there are defects in the security or reliability of data. That is the case, for example, if errors find their way into medical records, if others are given unauthorised access to sensitive information regarding psychiatric disorders, or if people are put at a disadvantage by an erroneous risk or customer profile.

The question that then becomes relevant is what possibilities people have for examining and correcting the data collected about them. According to the Dutch Data Protection Act, individuals are entitled to examine and correct any personal data regarding them. The case studies show that the methods for exercising these rights leave much to be desired. It would seem to be arranged well in the case of the electronic patient record and the fat version of the kilometre charge. The electronic child record, however, raises the issue of whether children (or their parents) are afforded sufficient opportunity to correct errors in their data or profile.

The citizens' legal rights seem to be completely ignored in the case of the Schengen Information System (SIS). The SIS was implemented in order to safeguard the external borders of the Schengen Area. This is accomplished by registering 'undesirable aliens' (who may not enter the Schengen Area) and persons sought by the police (who may not leave the Area). Besters demonstrates that the rights of registered persons go begging. First, there is legal inequality between the Schengen countries, because each country can further interpret the registration criteria. This creates significant differences between the participating countries. For example, failing to pay alimony or child support is a crime in Spain, which can result in an alert in the SIS. This is in contrast to other countries, where failure to meet this obligation is a civil matter. Second, there is no legal justification for some of the alerts in the SIS. For example, the German authorities label those who have been refused political asylum as undesirable aliens, which contravenes the criteria set forth in the Schengen Agreement. In addition, people are not always notified that they have been registered, which means that they are not afforded an opportunity to assert a defence to that registration. In cases in which they are aware of it, moreover, there is a lack of effective procedures in place to dispute a registration. The tenuous legal position becomes even more of a problem when one considers that registration in the SIS can have far-reaching consequences for those who are registered. In some cases, people may be denied access to the Schengen Area for decades.

Hildebrandt and Van Dijk demonstrate that the legal position of consumers about whom data is collected on the Internet is also uncertain. This mostly has to do with the invisible methods used to collect such data about consumers. Using the cookies stored on an Internet user's computer, that user's keyboard, mouse and surfing behaviour can be established. That can be used to collect detailed information about the user without that user having any idea of it. This can include sensitive information. By examining surfing behaviour, for example, estimates can be made of whether someone suffers from specific diseases – information that healthcare and life insurance providers would find extremely interesting. Because consumers have no idea that this data is being collected

and that it may serve as the basis for a customer profile, they are powerless to verify whether that data is correct. Consumers are thus also not afforded an opportunity to object to negative decisions based on that information.

This harmful situation is compounded because no clarity has been provided as to whether keyboard and mouse behaviour must be considered as personal data eligible for protection under the Dutch Data Protection Act. This also means that it is not clear whether the statutory right to examine and correct personal data applies to 'leaked' data that companies collect on the Internet. This prompts the question of whether the statutory provisions have evolved at pace with our times.

1.6 Digital autonomy

The case studies make it clear that the use of databases involves more than just unknown third parties gaining access to what may be extremely personal information. It also involves the fact that, based on that data, others form a particular image of an individual and take decisions that may profoundly affect that individual's life. For example, the Youth Care Agency may become involved in a family viewed as a problem family, people may be is refused a life insurance policy based on an analysis of surfing behaviour that indicates that they have an increased risk of developing certain diseases, or a person seeking political asylum may be denied that relief because he or she is registered as an undesirable alien.

But the position of the citizen in a broader sense is also at issue. The use of databases may also have implications for doctor-patient, consumer-company and citizen-government relationships. Hildebrandt and Van Dijk, for example, note that the often invisible means by which companies collect customer data from the Internet actually creates an information deficit on the part of the consumer. Companies can use this to their advantage. The consumer's information deficit distorts the relationships of 'the free and equal market' which is supposed to put consumers and manufacturers in equal bargaining positions. In order to counteract this infringement on the consumer's position, Hildebrandt and Van Dijk advocate more transparency on the part of businesses. They should provide consumers with more information about how consumer data is collected and how customer profiles are used.

The case study on the Municipal Personal Records Database extensively discusses the influence that government registrations have on the relationship between citizen and government. According to Boschker, Castenmiller and Zuurmond, the modernisation of Municipal Personal Records Database has laid an overly one-sided emphasis on efficient government structure, with the priority being thinking in terms of management and control. This goes hand in hand with an insatiable hunger for information on the government's part (see also BB Digitaal Bestuur 2010). The authors illustrate how the recording

of personal data in databases has become an unquestioned and automatic administrative routine. As indicated in the introduction, this tendency is paired with an explosive growth in the number of government databases. According to Boschker, Castenmiller and Zuurmond, governments are obtaining increasingly detailed pictures of their citizens. In addition, digital data files have a less flexible nature than their hard-copy predecessors. Computer systems are providing less leeway for personal interaction and exceptional cases. They believe that the ever-increasing use of databases will lead to new dependencies on the part of citizens.

This last point may be illustrated with an example that the report De burger in de ketens [The Citizen in Chains] by the Dutch National Ombudsman. It involves a business man who was for years registered as a drug offender in the government information system. As a consequence, he was repeatedly arrested and his house was repeatedly searched, with dire consequences for both his business and personal life. The erroneous registrations were the result of identity theft committed by one of the man's former acquaintances. Although the businessman was always able to demonstrate that he was not the party the police were seeking, he was not able to clear his name and have the erroneous registrations deleted (Nationale ombudsman 2009).

Boschker, Castenmiller and Zuurmond do not believe, however, that digitisation must necessarily lead to more far-reaching dependencies. Traditionally, government registrations have not only been characterised by an emphasis on management and control, but also their fulfilment of an emancipatory function. For example, registrations establish citizens' right to vote as well as their claims to social security facilities, which thus promotes their autonomy. By one-sidedly emphasising the increase in efficiency resulting from modernising the Municipal Personal Records Database, however, this emancipatory dimension is becoming lost. Then again, ICT solutions also offer possibilities for reinforcing citizens' position and giving them more control over their own personal data. This can be accomplished, for example, by better enabling them to exercise their rights of examination and correction. As things stand now, that right is often – and literally – confined to paper. Citizens must generally submit a written request to have erroneous data in files corrected (see also Leenes 2010). Databases could also be structured such that citizens can examine and alter their data through the Internet. The site www.mijnoverheid.nl enables citizens to examine certain data that the government has collected on them. For now, however, this site remains an exception to the rule.

Most of the case studies indicate that database architecture is primarily tailored to the needs of the principal or operator, with little attention devoted to the interests of the people about whom the data is being collected. This applies to both Municipal Personal Records Database and to the tenuous legal position held by persons registered in the SIS or consumers about whom information is

gathered on the Internet. The public transport chip card is also an example in this regard. Teepe demonstrates that the structure of the database containing travel data is primarily geared to the interest in optimal business operations. The aforementioned security problems of the chip card, as well as the long data-retention period of two to three years, the price inequality for anonymous users, and the poor legal position of travellers involved in disputes with public transport companies indicate that the travellers' best interests rated low on the list of priorities when the chip card was designed.

We can conclude from this that the structure of databases begs the question of how much their use strengthens or weakens the autonomy of patients, travellers and consumers.

1.7 Do databases do what they are supposed to do?

The final question relevant here is whether databases accomplish the objectives they are intended to accomplish. Does the electronic patient record actually result in a suitably secure exchange of medical data that prevents unnecessary medical errors? Does the electronic child record reduce the rate of child abuse? And does the Schengen Information System adequately guard the external borders of the Schengen Area?

Not all of the case studies address the effectiveness of databases. When they do, doubts are expressed. As stated, Jacobs warns against undue optimism regarding the EPR and asserts that the possibility of the EPR leading to new medical errors must be kept in mind. In addition, the medical sector does not seem to adequately secure the data in question. Based on these grounds, Jacobs reaches the conclusion that it is uncertain whether the pros of the national EPR would outweigh the cons.

Van der Hof also questions the specifics of the ECR. She wonders whether the huge amount of data collected in the ECR will actually result in better care. She believes that the endeavour to collect more and more data, link files from different agencies to one another and identify potential problem children using risk profiles threatens to overreach itself. Specifically, the result could be an unworkably large number of children at risk without identifying which children and families actually need help. Moreover, it may result in care providers having to divide their attention over so many possible problem children that they have little time left to address actual problem situations. According to current estimates, there are approximately 30,000 possible problem children in the Rotterdam area alone (NRC Handelsblad 2007; see also www.iederkindwint.nl). That is approximately 20% of the entire children and youth population (www.iederkindwint.nl). That would constitute an unworkably large number of cases to be addressed by youth workers. Van der Hof therefore questions whether it would not be wiser to collect more targeted information concerning cases that have already come to the attention of youth workers.

The case study about the SIS paints what may be an even more daunting picture. The information system itself is threatening to crash because it must serve such a large number of purposes. Besters demonstrates how the development of the various alternative versions of the SIS are continually plagued by technical and organisational problems, deadlines that are forever being extended and increasing costs. The problems relate to the new demands that are constantly being placed on the system. It is not only that the number of countries has gradually and significantly increased – from the original seven Member States to the current 25 – but the number of functions that the system is expected to serve has also increased. For example, the second-generation SIS (SIS II) will have to offer, amongst other things, broader access for authorities and store fingerprints for biometric identification. The practical implementation of the system is also complicated. Leaving aside the issue that the implementation criteria have not been harmonised – which means that each of the 25 countries has its own registration standards – each country has its own executive agency. Furthermore, there are problems with the absence of democratic supervision of the operation of the system and – as we have already seen – inadequate legal protection in place for those registered in the SIS. Besters thus questions whether a database of the size and complexity of the SIS can function properly.

1.8 Conclusions and recommendations

Taking everything together, the case studies present a fairly disturbing image of what can go wrong with using databases in practice. Prominent examples are the ease with which the public transport chip card may be cracked, the disadvantages that consumers may encounter as a result of an incorrect customer profile and the inadequate legal protection of persons registered in the SIS. The most important conclusion that may be drawn from the case studies is, thus, that databases are not risk-free systems. In this section, we formulate our conclusions about the areas requiring attention in order to adequately address these risks and recommendations for responsible database design.

The risks associated with the use of databases relate to the context within which the databases function. One example is the electronic patient record (EPR). On paper, the security measures put in place seem to be well thought-out, with UZI passes, login codes and the requirements for a Well Managed Healthcare System. But the functioning of the national EPR will ultimately stand or fall based on the care that doctors and other healthcare providers exercise in practice in complying with the security requirements. The chance that the security of the data will be compromised can be reduced by making more use of technical security measures. These measures simply make it impossible to examine or alter data in certain ways. The use of zero-knowledge cryptography in the fat version of the kilometre charge is a good example of this. The first priority for database design, therefore, should be using the technical possibilities for securing data. With regard to the public transport chip card,

for example, a transition could be made to using the zero-knowledge variant, which would offer travellers the possibility to benefit from discounts without having to surrender their anonymity.

A second priority regards the position of the patient, citizen or consumer about whom data is collected. The case studies show that the interests of citizens and consumers often play a subordinate role in database design. This is shown not only in the often scanty attention devoted to securing data, but also in the generally tenuous legal position held by citizens. This is embodied in the fact that although citizens have a right – at least on paper – to examine and correct the data collected about them, that right is difficult to exercise. And when things go wrong, the person who pays the price in this regard is generally the citizen, customer or consumer. The citizen is the one left holding the bag. And that problem only increases in proportion to the degree to which citizens are dependent on database operation in their everyday lives.

The more fundamental question in this regard is whether citizens', patients' or consumers' digital autonomy is reinforced or undermined by the use of databases. Just asking the question requires a shift in perspective. Often, the design of a database is almost automatically tailored to the needs and interests of the principal or operator (the government, transport company, company that collects customer data on the Internet) – generally ignoring the needs and interests of citizens and consumers. But databases can also be constructed so that they serve the interests and autonomy of the citizen. In designing databases, therefore, the question that arises is the degree to which the citizen can control his or her own data, as well as control who will use that data and how it will be used. The German Gesundheitskarte and the example of the kilometre charge demonstrate that there are real alternatives for controlling one's own personal data. Digital autonomy of the citizen may also mean, in the context of the public transport chip card, that the traveller will be offered the option to decide whether to use the zero-knowledge variant.

A third priority regards the effectiveness of databases. Policymakers and upper-echelon businesspeople tend to be unduly optimistic about what databases have to offer in the way of increasing the efficiency of processes, improving communication or resolving problems. For example, in its report Lessen uit ICT-projecten bij de overheid [Lessons from Government ICT Projects], the Netherlands Court of Audit warned against unduly high policy expectations in the area of ICT (Nederlandse Algemene Rekenkamer 2007; see also Automatisering Gids 2010). The plodding, faltering development of the SIS is a clear example of this. Because the system must serve too many divergent policy goals, a technical and organisational crash of the system may be on the horizon. The conclusion that may be drawn from this is that a database cannot be designated to meet random goals.

This conclusion applies to the electronic child record (ECR) as well. Attempting to make a risk profile for every child under the age of 19 is fed by the desire to identify all children who may develop problems, in order to facilitate timely intervention. This attempt seems to be primarily leading to an unworkably large number of children who may be at risk. Conversely, attention may be devoted to children who do not have problems that need addressing at the cost of the children who do – and who are often already known to require that help. The ECR is in jeopardy of missing the target. This begs the question of whether it would not be wiser to collect targeted data about known problem cases.

The examples of the SIS and the ECR demonstrate how excessive ambitions can undermine the achievement of a goal. This can be prevented by more carefully formulating the goal that a database must serve and by then collecting only the data necessary for achieving that – well-defined – goal. The effective use of databases requires people to resist the temptation to collect as much data as possible. Instead, the premise that should be lived up to is 'select before you collect' (Brouwer Commission 2009).

Based on the foregoing, we formulate the following recommendations regarding database design:

Make as much use as possible of technical data-protection measures.

Strengthen the position of the citizen. Facilitate citizens' exercise of their rights to examine and correct their data and give them as much control as possible over their own data.

Keep it simple. Choose a well-defined goal and restrict data collection to the areas necessary for achieving that goal.

These three recommendations are closely interrelated. Securing data in a strong, technically sound manner will make it difficult or impossible to use that data for other purposes such as tracing. A more focused deployment of ICT to identify problem children will mean that the goal of formulating a risk profile for every child will have to be abandoned.

Design choices may therefore also require one's initial objectives to be re-evaluated. The means and objective must be examined in their mutual context. In that sense, a price will have to be paid for every choice made. That makes decision-making regarding the utilisation of databases much more complex.

The exponential pace at which society is being digitised entails a similarly increasing need for well-considered database architecture. The case studies demonstrate that database design often fails to devote sufficient attention to the risks associated with database use. Knowledge of the possibilities and limitations of ICT is mandatory to properly assess these risks and possible alternative design choices. This essay has already referred to the necessity of continuously monitoring databases, because they are never completely secure. This requires long-term database-operation supervision by an independent agency, perhaps in the form of a national ICT authority. We endorse this position. An independent agency such as this would not only have to supervise database operation, but would have to ensure adequate database design. The decision-making process regarding database design must contain a test phase during which independent experts may investigate whether sufficient account has been taken of security requirements, the position of the citizen and the necessity of collecting the data. We thus conclude this essay with a fourth recommendation:

Ensure independent, continuous supervision of the design and operation of databases.

The public transport chip card and the kilometre charge: an electronic ankle tag for travellers?

2

2 The public transport chip card and the kilometre charge: an electronic ankle tag for travellers?

Wouter Teepe

2.1 Introduction: improved efficiency in public transport

With the introduction of the public transport chip card and road pricing for cars (the 'kilometre charge'), central databases can be created, depending on the chosen technology, in which every one of our journeys can be recorded in a central database, with the data then being held for years. It is as if travellers are being monitored and are wearing an electronic tag around their ankle. This is the first time that there have been databases with so much detail regarding the movements of Dutch citizens.

One important aim of introducing the public transport chip card and the kilometre charge is to improve efficiency. Accurate information about pressure on public transport (particularly peak pressure) can facilitate precision planning of the deployment of staff and equipment. Expensive capacity can then be deployed more efficiently, which is good for travellers' comfort and cost control. Charging drivers specifically for using their car during the rush-hour encourages them to change their behaviour, for example by simply avoiding the rush-hour. The thinking is that this will reduce road congestion and benefit the environment.

When considering efficiency improvements, it can be instructive to take a look at the modern raw materials processing industry, which attempts to avoid even the slightest waste. That is good for the company's operating profit and often also for the environment. Improvements in efficiency are recorded using precise measurement methods and control instruments. Precise measurements clarify the actual efficiency of an industrial process, for example by showing whether there is an excess or a shortage of materials at some point within it. Measurements ensure transparency: where are the bottlenecks? And what do the various components of the process cost? Precise control tools can increase efficiency, for example by running the assembly line faster or slower. Precisely coordinating the measuring and control tools with one another can enable the company to achieve optimum efficiency.

Just like items on the assembly line in a factory, public transport users can be tracked and controlled. But there is still a lot of room for improvement in the public transport context. Accurate measurements are lacking and the control tools are only crude. The wish to keep close track of how transport capacity is used is by no means strange. Measurements in the public transport context make it possible to pass on the costs to users more precisely and consequently more equitably. Public transport subsidies can also be distributed more fairly. Measurement also produces a precision control tool: certain travel behaviour can be encouraged or discouraged by means of differential pricing. In the case of the kilometre charge, that objective has been announced publicly: according to the Dutch government, the charge is intended to bring about a reduction in congestion and the use made of environmentally unfriendly vehicles. The same aim can be found in the case of the public transport chip card: the collaborating transport companies – united in Trans Link Systems (TLS) – wish to use the data collected on passengers specifically to encourage them to travel during off-peak periods.

The public transport chip card is currently being widely introduced in the Netherlands. Plans for the kilometre charge were abandoned in 2010, however, partly because of the cost to drivers. For the purposes of the present study, a comparison of the two proposals remains instructive, however.

2.2 Procedural and technical privacy guarantees

Introduction of the public transport chip card and of the kilometre charge is viewed as a modern electronic means of paying for mobility. Such a system can be highly effective and user-friendly, but it can also be seen as a threat to privacy. The outcome depends on the architecture of the system.

The public transport chip card and the kilometre charge can lead to the construction of large central databases that record every journey made. The data contained in those databases makes it possible to derive a detailed picture of somebody's life: where he lives, where and when he works, when he goes on holiday, when he goes out the evening, and where and in what kind of neighbourhoods his family and friends live. That picture is very much more detailed, for example, than that which can be derived from the data that airlines are now required to collect on travellers flying to the United States; the latter does not involve constant recording of where the passenger is at any given moment.

One can distinguish between two different types of measures for dealing with the privacy issues raised by these kinds of ICT applications, namely procedural measures and technical measures. The former focus on agreements: who can access the database and who is responsible for its security. Procedural measures do not amount to much if there are no serious penalties for improper use of data or for neglecting the security precautions. In practice, such penalties are often lacking. Technical measures involve constructions within computer programs that make unauthorised behaviour physically impossible, for example by applying cryptography. Cryptography is the collective name for mathematical techniques to process data in such a way that it is no longer suitable for general use but only for specific predefined applications.

In actual practice, technical measures offer firmer guarantees for privacy protection than procedural measures. That will be made clear below on the basis of the various different architectures used for the public transport chip card and the kilometre charge for cars. The architecture of the current card comprises few technical measures to protect the user's privacy. By contrast, the version of the kilometre charge considered here is to a great extent based on technical measures.

2.3 The public transport chip card: privacy at risk

The public transport chip card is a travel ticket with the form factor of a credit card. The user must check in and out at the start and end of his journey by holding the card up to a card reader. The use of 'RFID' chips means that this can be a quick and contactless procedure, requiring the card to be held within ten centimetres of the reader. The card reader is a small computer terminal linked to a central database. The card, the card readers, and the database jointly ensure that detailed travel data is recorded and that the journeys made are paid for.

Payment with the public transport chip card can be based on a monetary balance loaded onto the card – perhaps in combination with discount arrangements recorded on the card (for example an off-peak discount arrangement) – but also on the basis of 'travel products' that are also 'loaded' onto the card (for example a one-day travel arrangement for the Amsterdam metro). Instead of buying a paper ticket, the passenger loads travel products, discounts, and money onto the card. Money can also be loaded automatically if desired; this requires the user to have issued a direct debit authorisation. Means of payment other than the public transport chip card have been almost completely phased out in the last few years, with the public transport chip card ultimately being the sole travel document accepted.

There are three versions of the public transport chip card: the personally registered (i.e. non-anonymous) card, the anonymous card, and the disposable card. The registered card allows the user to carry out all the actions described above, i.e. to load any of the available travel products and discounts. The anonymous card does not allow one to load discounts but only non-personal travel products and a monetary balance. The disposable card is sold pre-loaded with a travel product of a specific limited value. After that product has been used, the disposable card ceases to be valid. It cannot be used for more expensive journeys, for example for a long-distance journey by train.

The disposable card is the most convenient option for people who only make occasional use of public transport. For someone who makes fairly regular use, the registered card is the cheapest and most convenient option. The discounts that can be loaded onto the registered card usually quickly pay for themselves; they cannot, however, be loaded onto the anonymous card. Examples are the statutory travel discounts for the under-12s and over-65s; these only apply if one uses the registered card. Netherlands Railways' popular off-peak discount arrangement is also only available with the registered card. There is therefore pricing pressure to choose a non-anonymous card.

2.3.1 What data is recorded?

In order to acquire the registered card, the user must give his/her name, address and date of birth, and provide a passport photo. The card is then sent to the address given, with the name, date of birth, and passport photo printed on it. This data is recorded centrally with Trans Link Systems; the individual transport companies do not have access to it. For some travel products and discounts – for example the public transport pass issued to students and the off-peak discount arrangement – the user must also provide the relevant transport company with a copy of a valid identity document. The anonymous card and the disposable card can simply be bought at sales outlets.

A transaction takes place each time the user checks in or out. Originally, transaction details were retained for a period of seven years. TLS believed that the Dutch Tax and Customs Administration had imposed this retention requirement, although the latter denied this (De Winter 2008). After five law students forced the Dutch Data Protection Authority to act upon the matter, the formal retention period has been reduced to 18 months (Bakker 2011). However, the data is still being retained for two to three years. The data for the last ten transactions is also recorded on the card itself.

The following data is recorded for each transaction:

- the number of the card;
- the date;
- the time (exact to the minute);
- the location (including the stop or station);
- the type of transport: bus, tram, metro, or train;
- in the case of the train: first or second class;
- in the case of the bus and tram: the number of the vehicle;
- the means of payment: by means of a travel product or from the balance on the card, and whether a discount applies.

For each card number, a travel company can see the transactions for all journeys made via its infrastructure. If a registered card is used, the transport company can also identify the user on the basis of the card number. TLS can see the transactions for all transport companies for each card number, plus any associated personal details.

However, it is also possible to trace the journeys of users who travel using an anonymous card. This is because the great majority of card loading terminals do not accept banknotes; cards can only be loaded with a monetary balance or

travel products if the user inserts coins or makes a PIN payment. In the case of PIN payments, the bank provides the recipient the account number of the customer. For people who make regular use of public transport, paying by inserting coins is highly inconvenient. Users of anonymous cards will normally therefore pay by giving their PIN, and can consequently be identified indirectly on the basis of their bank account number. The Dutch Central Bank has in fact prohibited linking bank accounts to personal details for commercial purposes. The police and judicial authorities, however, are authorised to link this data and can also compel access to the central database.

The database allows the transport companies to see how many people were travelling at any time on a given mode of transport at a given location. They and TLS can also see each user's transactions. This is of course not possible if someone uses more expensive disposable cards, or purchases a new anonymous card for each journey.

Besides optimising operational processes, electronic payment also serves a second purpose: the transport companies can use the public transport chip card to provide services. Users can be offered certain services in the light of their travel data, for example information about altered train times or disruptions. An opt-out arrangement applies: unless they opt out, users of a registered card will be offered these services and the travel companies can record the relevant travel data. This proposal was approved by the Dutch Data Protection Authority (College bescherming persoonsgegevens 2008). More active profiling of users for commercial purposes – for example to alert the holder to special offers available at shops at the station where the user is currently located – is not permitted unless the user has given explicit consent. This is therefore an opt-in arrangement, which allows the transport companies to record and process much more data.

2.3.2 What are the arrangements for data security?

Trans Link Systems looked for a reliable chip card that had already proved itself in practice. It selected the Mifare Ultralight chip for the disposable card and the Mifare Classic chip for the anonymous and registered cards. This was despite doubts that had arisen regarding the security of these chips. Those doubts were corroborated in January 2008 when a student at Radboud University Nijmegen demonstrated that the Mifare Ultralight chip could be emulated using a gadget costing only twenty or thirty euros. In March the same year, a team at the same university discovered that the Mifare Classic chip was quite easy to hack: all that was required was a standard card reader costing ten euros and an ordinary PC.

For a long time, TLS maintained that there was nothing wrong with the security of the public transport chip card, but it did not allow the security system to be examined. It was only after demonstrations of various weaknesses in the media

that TLS revised its public position (and then only partially). Despite this, the user information provided by TLS still suggests that nothing is really wrong. In the FAQ on the www.ov-chipkaart.nl website, the question 'Can unauthorised persons transfer money from my public transport chip card?' receives the answer 'No, …'. That answer is factually incorrect.

The problems with the security measures for the public transport chip card could have been prevented if a different type of chip had been selected. At the point when TLS selected the Mifare chips concerned, other types of chip were also available but were not included in development of the public transport chip card. The Mifare chips appeared to meet the requirements set by TLS and their security weaknesses were not yet generally known. Changing the type of chip would be a costly and complicated operation. Currently, TLS is rolling out special RFID chips from manufacturer Infineon (based on the SLE66), which are essentially backward compatible with Mifare Classic, but which have improvements to keep fraudsters at bay. This is an intermediate step leading to ultimate migration to the SmartMX chip from NXP.

The security problems with the Mifare chips mean that large-scale fraud is a possibility, for example by altering the amount of money on the card at will. Theoretically, virtually all fraud will be identified by the database and manipulated cards can then be blocked. Due to a combination of technical and organisational reasons, however, the fraud detection function is not in fact foolproof and identifying fraud takes at least a whole day. As a result, 'hit-and-run fraud' remains possible.

The fact that the Mifare Classic can be hacked also means that persons with malicious intent can read out and manipulate lost or stolen cards. They can, for example, see where the holder was during his or her last ten journeys or alter the balance on the card. During a hearing on the public transport chip card before the Dutch House of Representatives, Bart Jacobs, a professor of computer security at the Radboud University Nijmegen, stated that he considered the card to be 'an open purse'.

Little is known about the security measures that protect the central database, which might be an interesting target for hackers. The extent to which the infrastructure for the public transport chip card is protected against fraud and errors on the part of the transport companies and TLS themselves is also unknown. What is clear, however, is that errors do in fact occur. At the same parliamentary hearing, Gertjan Kroon, at that time director of Amsterdam's public transport company GVB, said that some card loading terminals indicated that money had been booked onto a card when that was not in fact the case. Customers who then complained had been told that they had used the terminal incorrectly and, as far as was known, had not received a refund. That brings us to another problem with the public transport chip card, namely that holders who

have a dispute with a transport company are unable to produce the necessary evidence to substantiate their allegations. They are in fact dependent on the good will of the transport company.

2.4 The kilometre charge: technical privacy guarantees

Unlike with the public transport chip card, plans for the introduction of the kilometre charge explicitly involved consideration of technical methods for guaranteeing privacy. Two versions were developed for introducing the charge, one 'thin' and one 'fat'. In the case of the regular version, details of each journey are collected by a private service provider and passed on to the body that collects the charge, which then stores the data in a central database (Van 't Hof, Van Est & Kolman 2011). In the fat version, the data is collected within the car and then transmitted to the body that makes the charge, without any intervention by a private party.

2.4.1 A privacy-friendly design

The responsible Minister of Transport, at that time Camiel Eurlings, expressed a preference in the media for the fat version. This provides better privacy protection because only the driver himself can access data about his journeys. At the time, however, it was unclear which version would be selected. As we have already seen, the plans for the kilometre charge have since been abandoned. We will deal below only with the fat version because it is a good illustration of how technical measures can be incorporated so as to protect privacy.

The fat version of the kilometre charge makes the following functions possible:

- payment is made for travel with differential pricing applying;
- only the driver himself can access travel data that can be traced to him;
- fraud and errors on the part of the driver can be detected by the operator;
- fraud and errors on the part of the operator can be detected by the driver;
- in the event of a dispute about the bill, both the driver and the operator are able to produce the necessary evidence to substantiate their claims.

The final point in this list is a good example of the advantages of a technical measure compared to a procedural one. If the operator makes a mistake and sends the driver an inexplicably large bill, the driver is not left entirely at the mercy of the operator as regards identifying and rectifying the mistake. As we saw in the previous section, this in contrast to the case of the public transport chip card.

2.4.2 How does the kilometre charge actually work?

The driver's car is equipped with a GPS receiver that tracks where the car is travelling. Combining the journey history with a pricing table allows the bill to be drawn up by the driver's navigation system. The bill is then submitted digitally to the operator together with an encrypted version of the journey history. Car owners who do not submit a bill for a lengthy period receive a reminder; if they continue to fail to submit the bill, a penalty is imposed. If he wishes, the driver can contract calculation and submission of his bills out to a specialised company so as not to have to do the necessary work himself.

The operator can carry out checks to combat fraud by observing which cars pass a random location along the road so as to verify whether that stretch of road occurs in the journey history submitted by the cars concerned. If that stretch of road does in fact occur in the journey history, then the driver has paid for that specific road use. If it does not, a penalty will be imposed on the driver. The journey histories are encrypted in such a way that the enforcement authority can see that a stretch of road that has been checked does in fact occur but not which other stretches of road the car has been travelled on.

The fat version is a road-pricing system in which a technical measure minimises infringement of the driver's privacy (De Jonge & Jacobs 2008). The system provides a precision control tool because driver behaviour can be managed by means of differential pricing for particular times, locations, and vehicle types. Precise measurements are also recorded – who is where, when, and in what vehicle? – but they are not centrally accessible; it is only the driver himself who can access them.

2.5 A privacy-friendly public transport chip card?

The question that arises is whether it is also possible to produce a privacy-friendly version of the public transport chip card. There are two significant differences between the chip card and the kilometre charge system.

In the first place, the fat version of the kilometre charge makes use of satellite navigation for every individual driver. Such a system is not suitable for application in the context of public transport. There are a number of practical objections. The public transport traveller would need to have a device with a properly charged battery with him and that device would also need to be able to contact orientation points such as GPS satellites. It is questionable whether smartphones are sufficiently reliable for this purpose. It is also not possible to distinguish between for example a cyclist or pedestrian – who does not need to pay – and someone on a bus using the same lane or road. The design for the public transport chip card with an RFID chip with which the user checks in and out is actually not all that bad from this point of view.

The second difference concerns the use of encryption. The kilometre charge system utilises a complex 'zero-knowledge' type of encryption. 'Zero-knowledge' means that technical restrictions can be imposed on the use of information, thus allowing privacy-sensitive data to be screened from the operator while the necessary functionality – for example billing for journeys made – can still be provided (Brands 2000; Camenisch & Lysyanskaya 2002).

A zero-knowledge design is also possible for the public transport chip card, with the user still checking in and out. This version has the same privacy-friendly features as the fat version of the kilometre charge, although a central database is in fact created. The main difference to the present public transport chip card system is that zero-knowledge encryption means that travel data cannot be traced to individuals. The central database does mean, however, that the transport companies can carry out precise measurements in order to deploy their vehicles and staff more efficiently but still cannot see each individual user's transactions. This alternative design records the same details as the current public transport chip card, with the exception of the number of the card. This means that the various journeys made using the same card cannot be linked to one another or to the user.

The computing capacity required for zero-knowledge encryption is much greater than that utilised for the current public transport chip card. Until mid-2009, no commercially available RFID chips were powerful enough. When the present public transport chip card was being designed, applying zero-knowledge encryption was not an option. More secure chips did exist that were better able to combat manipulation and fraud, but there were no chips that allowed the user to travel anonymously.

2.6 Conclusions: an electronic ankle tag for every traveller?

Since the introduction of the public transport chip card, every user's travel behaviour has been recorded in detail. The data held in the central database will be retained for two to three years. That is a great deal longer, for example, than the period applying to telecommunication details stipulated in the EU's directive on data retention. The recent advent of RFID chips that support privacy-friendly technology makes it possible to introduce a privacy-friendly public transport chip card. Given the costs involved, however, heavy political and public pressure will be needed to ensure that such a card will be introduced.

In the case of the kilometre charge, a version is available that requires few if any sacrifices as regards privacy. According to the Minister of Transport, congestion and pollution can be reduced without needing to know where individual cars are located, and the technology for doing so is in fact available.

The privacy-friendly 'fat' version of the kilometre charge system is to a certain extent undermined, however, by the camera systems for automatic number plate recognition (ANPR) used by the police. These systems currently record the number plates of all cars on the motorways around the cities of Zwolle and Rotterdam. Although their effectiveness and legitimacy are still the subject of discussion, the aim of the police is to install more ANPR systems in the near future. Where cars are concerned, authorities are therefore pursuing a dual policy: while the police are registering cars on an ever-increasing scale, the Ministry of Transport is far more reserved.

Unlike with the kilometre charge, the government has set hardly any frameworks as regards public transport. The central database created with the public transport chip card has led to little discussion regarding privacy. Until recently, hardly anyone was subject to constant tracking of his or her location. That changed with the introduction of systems such as the public transport chip card and number plate registration. And because it is impossible to travel long distances unless by car or public transport, this means that the government and the transport companies can determine somebody's location at any time.

A comparison with the electronic ankle tag is almost unavoidable. Certain groups of persons convicted of a crime are permitted a degree of mobility on condition that they wear such a tag so as to allow the police or the probation service to keep track of what they are up to. Their privacy is restricted because a court has ruled that they represent a danger to other people. Large-scale recording and storage of travel data in central databases would seem to be leading to a situation in which everyone – including ordinary law-abiding citizens – are wearing the equivalent of an electronic ankle tag. The question is whether that is desirable.

Acknowledgements

This chapter could never have been written without the knowledge acquired during a large number of interviews with those directly concerned. There are too many to name but thanks are due to all of them for giving of their time and for their candour. The author was a member of the team at Radboud University Nijmegen that carried out a study of the public transport chip card, the Mifare Classic, and the kilometre charge.

3 The electronic patient record from the perspective of data protection

3 The electronic patient record from the perspective of data protection

Bart Jacobs

3.1 Introduction

Over the past few years, the Dutch government developed plans for a national electronic patient record (EPR). The purpose was to improve communication between healthcare providers and thus the quality of medical care itself. With that in mind, a national ICT infrastructure was set up giving healthcare providers access – after receiving the patient's consent – to a variety of medical data. Although development of the EPR was already far advanced, the Dutch Senate called a halt to further development in April 2011, mainly because of objections regarding security and privacy. It is currently unclear what will be done with the ICT infrastructure that has already been set up; it is possible that this will be implemented and developed further by private parties.

The present article discusses the introduction of the EPR from the perspective of information security. It deals with the architecture of the EPR, security requirements, access procedures, security risks, and the consequences of introducing the EPR for doctors and patients. The emphasis is not so much on the technology and methods but, rather, on how they are dealt with. The main conclusions of the article are that the EPR introduces new requirements for the healthcare sector as regards due care, identity checking, transparency, and accountability; besides medical advantages, it also introduces new vulnerabilities. The material is too complex to give a simple 'for' or 'against' and no attempt will therefore be made to do so.

3.2 Architecture

Three different ICT architectures are possible for a national electronic patient record, each with its own advantages and disadvantages. I shall deal successively with a central database, the possibility of decentralised storage of data, and a referral infrastructure. The term 'architecture' naturally refers in this context not to the construction of buildings and bridges but to the design of ICT systems. Broadly speaking, it refers to the structural organisation of hardware, applications, processes and data streams, along with the related organisational consequences, within companies, governments or society in a broader sense.

3.2.1 Central database

The first option for an electronic patient record involves a central database in which are stored all the records for all patients. This approach would seem to be the simplest and most obvious. However, a central database makes the system extremely vulnerable to potential misuse, failures, or overloading. Moreover, the possibility of a database containing a concentration of highly privacy-sensitive information crashing – due to malicious hackers or administrators, or simply to administration errors – constitutes too great a risk. Such a centralised approach is therefore unsuitable.

3.2.2 Decentralised storage in possession of the patient

The second option is to set up a completely decentralised architecture, with the patient holding and managing his record himself. From the point of view of privacy, this is not such a bad idea because controlling access to personal details is an essential component of the concept of privacy. Especially in countries where there is no dense network of front-line medical care, it is perfectly normal for someone who has had an X-ray, for example, to take the results home with him and then bring them along to the next consultation. In Germany, the 'Health Card' (*Gesundheitskarte*) is being introduced – a chip card on which the patient holds a large part of his medical record himself – under the motto 'the patient must be the boss of his own details' (*Der Patient muss Herr seiner Daten bleiben*). This decentralised approach does not necessarily mean that people also have to store their medical details themselves; they can also be stored on the Internet in encrypted form, with only the patient having access to the necessary cryptographic keys. The patient is therefore the sole person who can decide to provide copies of those keys to someone else, for example to ensure that they are not lost.

One basic principle of this approach is that inaccessibility of the EPR to anyone other than the patient – without the latter's consent – is an integral component of the architecture itself. Making access technically impossible in this way provides greater guarantees than if the patient's consent were to be necessary on procedural grounds; after all, procedures can easily be altered or ignored.

This decentralised architecture was not the type selected in the Netherlands. The precise reasons for this are unclear – and may perhaps merit a separate study – but they would primarily seem to have been because the patient is not considered capable of exercising sufficient care when dealing with his own details, and the medical sector did not wish to relinquish control of medical data.

The latter point already indicates that the architecture of ICT systems is closely associated with power relationships. Patients in the Netherlands have too little say. The American privacy champion Mitchell Kapor therefore rightly asserts that

'architecture is politics'. The ICT architecture selected gives a good idea of the underlying power relationships. In the Dutch plans, a form intermediate between central and decentralised storage of medical data has been selected; this will be described below.

3.2.3 National referral infrastructure

In between these two extremes of central and decentralised storage, there are a number of intermediate forms. In the Netherlands, it was decided that medical data should be managed by the healthcare providers concerned and made accessible by means of a national referral infrastructure, the National Exchange. By entering a patient's Citizen Service Number (CSN), a doctor can call up information about the patient from a colleague's computer. This makes the reliability of the EPR partly dependent on the reliability of the CSN. The healthcare provider must make absolutely sure – certainly in the case of a patient whom he does not already know – that he is entering the right CSN for the right patient. Identity checking therefore becomes part of the reliable provision of care. In actual practice, however, the importance of this is hardly appreciated; 'I'm not a policeman!', is the complaint of many healthcare providers. Nevertheless, the EPR does require healthcare providers to take on such a role.

The National Exchange infrastructure is in fact a network of connected computers within which various fragments of the patient's record are transmitted via encrypted connections. This digital exchange of medical data takes place primarily between healthcare providers, but it also makes it possible for the patient to access his own record. Healthcare providers that are connected to this National Exchange must comply with the security requirements for a 'well-managed care system' and must give patients access rights via the National Exchange. The National Exchange itself is also being developed on the basis of specific security requirements (Van 't Noordende 2010). This process is directed by the National IT Institute for Healthcare in the Netherlands (Nictiz), which operates subject to the responsibility of the Minister of Health, Welfare and Sport. We will deal below in more detail with this third version, which is generally referred to as 'the national EPR' or just 'the EPR'.

3.3 Security requirements for the EPR

What security requirements must a national electronic patient record meet? The most important conditions for it to function properly are the confidentiality, integrity, and availability of the medical data concerned. The security requirements for the national referral infrastructure are a logical consequence of these conditions.

The first condition, confidentiality, means that only authorised parties are able to read a given medical record. It is this point that is the focus of discussion regarding the threat – or supposed threat – to the patient's privacy.

Confidentiality can be compromised by such things as carelessness, leaks, or hacking. And once that confidentiality has been compromised, it can never be restored: once it has been revealed that somebody – whether a celebrity or just an ordinary person – has had psychiatric treatment, that information can never be made to disappear.

Integrity of medical data means that that data can only be altered by authorised parties, thus enabling doctors to rely on it. That integrity can be compromised if a patient's identity has not been properly determined before information is added to his record, resulting, for example, in the wrong blood group being recorded. Integrity can also be compromised if authorisation for accessing or altering the data has not been properly established. Persons with malicious intent can also deliberately damage the integrity of medical data, for example by calling in a hacker to harm a particular person or group. Damage to the integrity of data can have serious negative consequences, but can basically be rectified if it is discovered in time.

The third condition, the availability of medical records is important so as to ensure effective treatment. The more dependent healthcare providers become on electronic records, the more important it is that those records actually appear on their computer screen as and when required. If the data comes from another location via the National Exchange, it is essential for the healthcare provider to be able to rely on the correct operation of the infrastructure and on effective protection against malicious intruders.

I shall return in section 5 to the security risks associated with these conditions for an effective EPR, but will first deal in greater detail with how access to medical records is regulated.

3.4 Access procedures

Where access to the electronic patient record is concerned, a distinction needs to be made between access by healthcare providers to their patients' records and access by patients to their own records.

3.4.1 Access for healthcare providers

In order to access a patient's medical data via the National Exchange, healthcare providers make use of the 'unique healthcare provider identity pass' (the 'UZI pass'). This is read by a pass reader connected to the healthcare provider's computer. Using the pass requires authentication by means of a six-figure PIN. Healthcare providers are only permitted to access the data for patients whom they are treating, but there are no technical measures in place to determine whether that is actually the case. There are, however, a number of procedural checks and a record is kept of every time the EPR is accessed, thus making it possible to determine subsequently whether access was in fact authorised.

The UZI pass is intended to be strictly personal and non-transferable. In actual practice, however, a number of people may well utilise the same pass for the sake of convenience. This involves risks not only for the patient but also for the healthcare provider. Consultation of medical data is recorded and the records can be used, for example, if the question of liability arises. Using the UZI pass therefore requires a new kind of discipline and caution on the part of healthcare providers. It also introduces a new kind of control and liability: if someone gains unauthorised access to a patient's record using a colleague's UZI pass, he may be creating a problem for that colleague.

The government estimates that more than half a million UZI passes have been issued in the Netherlands, i.e. one for roughly every 25 adults. Not every UZI pass gives access to medical data – that depends on the authorisation associated with the role of the individual concerned, for example a doctor or nurse – but the large number of passes does mean that we all know a few people who have access to medical data. It is out of the question that every one of the half million people with access to medical data will always act properly and with due care. That is already not the case. But the EPR does give potential malicious intruders easier access to more data.

It has already been pointed out that healthcare providers must determine the identity of the patient, but the patient also has an obligation to authenticate himself. This too creates new responsibilities and liabilities for the care provider: if an uninsured person can assume my identity without that being noticed, for example, incorrect data may be entered into my record. Nationwide links mean that such errors will be propagated, making it more likely that a patient will in fact find himself confronted by them. To what extent a patient can hold a healthcare provider liable for inaccuracies that find their way into his record due to insufficient identity checks remains to be seen.

3.4.2 Access by patients

According to the Medical Treatment Agreement Act, patients have a right to be able to access their medical records. The former Minister of Health, Welfare and Sport, Ab Klink, stated that this is an essential component of the EPR and that it must be a simple matter for patients to access their medical data electronically. This access to the EPR is provided for via a more stringent version of DigiD, the government-wide authentication service, which requires the citizen to initially authenticate himself face-to-face.

People are not only given access to their medical data but also to log files that show which care providers have accessed their record. If this log information is presented transparently, it can act as an important and effective means of control. Healthcare providers then need to remember that inappropriate prying into someone's data is more likely to be noticed and lead to a complaint.

Patients themselves can also selectively adapt access rights to their record and prevent certain healthcare providers having access. One example might be if the patient's neighbour were a doctor and the patient did not want to rely on him controlling his curiosity.

3.5 Security risks

Security problems with the electronic patient record can arise in relation to confidentiality, integrity, and availability (see section 3). Availability risks are difficult to estimate at this stage and will be ignored here; that is not to underestimate their great importance. Risks regarding confidentiality and integrity will be considered jointly as forms of an authorised access.

It is a major problem if someone is able to access the database of a hospital or general practitioner's centre and inspect or alter patient records. That risk is a genuine one even without the existence of the EPR, as appeared from successful attempts at unauthorised access organised by the journalist Karin Spaink in 2005 (Spaink 2005). Introduction of the national EPR would increase this risk if it turned out to be possible to access such databases via the National Exchange. In the case of the National Exchange, however, the stringent security requirements mean that that risk would not appear to be very great. A breach of the security for the National Exchange itself would be a national disaster, however, because all the country's medical data is exchanged via the National Exchange.

The risks are far greater when it comes to the authentication of healthcare providers. They must make meticulous use of the UZI pass, not share passes or PINs, log out immediately after they have finished using the system, not forget their pass and leave it in the pass reader, etc. Towards the end of 2008, a current affairs programme on Dutch TV showed how staff of a hospital were prepared, without any pressure, to provide log-in names and passwords to strangers over the phone (NOVA 2008). A number of studies have confirmed that hospital security is not all that it ought to be. Healthcare providers have been trained to provide care but have not been properly trained as regards data protection. Major improvements are necessary. Security-related incidents – due to curiosity or ill intent – will probably be the object of much media attention, potentially tarnishing the reputation of the medical sector and the EPR.

There are also security risks when an individual patient accesses his own record via the Internet. Every person is responsible for dealing carefully with the DigiD system for authentication. Things will undoubtedly go wrong now and again, in just the same way as people unintentionally allow others to access their bank account in the context of Internet banking because they are careless or because of a computer virus. The fact that this involves individual cases means, however, that the damage will be less than when someone hacks in to a medical database.

The EPR allows patients to restrict healthcare providers' access to their records, or even to prevent it entirely. Large numbers of people will probably do this if serious security incidents occur. This 'feedback loop' can be expected to put healthy pressure on those responsible for the security of the system.

There are already numerous initiatives at local level for the electronic exchange of patient data, for example via GP centres or cooperating hospitals. These initiatives are not subject to stringent security requirements. The national EPR was intended to put an end to this by means of a nationally regulated infrastructure that would allow healthcare providers and patients uniform, verifiable access. Perhaps the strongest argument for introducing the national EPR is that it would clean up these well-intentioned, 'knocked-together' local initiatives, which have also been the object of criticism by the Dutch Data Protection Authority and the Healthcare Inspectorate.

3.6 Consequences of introducing the EPR

The electronic patient record was primarily intended to improve communication between healthcare providers. Poor communication was said to account for more than a thousand deaths annually and almost twenty thousand cases of the wrong medication being administered. The intention was that the EPR would greatly reduce these figures. Undue optimism is unwarranted, however. The EPR will not get rid of certain ingrained errors – for example nurses who cannot count and who administer the wrong dose – and it will also produce different kinds of medical errors. The most frequent computer error involves wrongly selecting the adjoining medication in the menu, i.e. when the doctor wrongly clicks on the medication located just above or below the right one. Smart software can, however, detect certain errors and inconsistencies in patient records.

The EPR might well have had its greatest impact not on the communication between healthcare providers themselves but between the healthcare provider and the patient. The latter can, after all, keep close track of what is going on in his own record, and can request an explanation or account quicker and more frequently, or even arrange for a second opinion. This forces healthcare providers to work more transparently and to adjust their attitude accordingly. They can no longer note down 'Patient is a complainer', for example, but have to make a more appropriate and respectful note to the effect that 'The patient is extremely concerned'. Greater transparency can also be ensured by installing two identical screens on the desk at the doctor's practice, one for the doctor himself and one for the patient, so that the latter can immediately see the changes that the doctor is making in his record, thus increasing his level of confidence.

3.7 Conclusions

It has become clear in recent years that incidents concerning security and privacy can make or break major ICT projects. That also applies to the electronic patient record. Besides its intended goal of improving medical care, the EPR also entails new vulnerabilities and risks, particularly as regards security, identity fraud, and the propagation of incorrect information. A successful attack on the infrastructure of the EPR can have disastrous consequences for the confidentiality, integrity, and availability of medical data. However, the greatest risk is to be found in a careless approach on the part of healthcare providers to their authentication obligations, both as regards the UZI pass and the necessary checks on the identity of the patient. At the moment, it is not reasonably possible to estimate whether the pros of the national EPR would outweigh the cons. The numerous issues raised by the EPR were reason enough for the Dutch Senate to refuse its consent to the government's plans.

Should the EPR nevertheless be introduced in the near future, it will have a dynamic of its own, one that is as yet unpredictable. Those concerned will undoubtedly see possibilities which have not so far been considered. Patients might, for example, be able to construct their own decentralised medical record, by preventing access by anyone else and saving their record to their own USB stick. Others may prefer to copy their data to Google Health. There is no point in suppressing initiatives of this kind. The most one can do is guide them in the right direction or discourage them by ensuring that the EPR is genuinely valuable for the patient and that he is therefore less likely to switch to another system. This would involve such things as enabling the patient to add data to his own medical record, for example blood pressure measurements that he has taken himself, or to communicate securely with the doctor within the electronic environment of that record.

Making the EPR secure requires transparency and constant attention and monitoring, 24 hours a day. Banks, which also work with sensitive data, also keep constant track of their Internet operations. Such transparency and monitoring are necessary to ensure confidence on the part of both healthcare providers and patients. Ultimately, it is practical experience that will need to show whether the referral architecture selected links up effectively with the existing culture and working methods of the Dutch medical sector. The decentralised version selected in Germany – utilising the above-mentioned *Gesundheitskarte* – provides the citizen with greater control; the fact that it has not been selected for use in the Netherlands gives one food for thought.

Acknowledgements

The author wishes to thank Simone van der Hof, Sjaak Nouwt, Guido van 't Noordende, and the Rathenau Instituut editors for their constructive comments.

The electronic child record: opportunities and issues

4

4 The electronic child record: opportunities and issues

Simone van der Hof

4.1 Introduction: the introduction of the electronic child record

The paper records in the context of juvenile healthcare (JHC) in the Netherlands are being converted into digital files, an operation referred to as the 'electronic child record' (ECR) or since recently the 'digital juvenile healthcare record'. This obligation is pursuant to the Public Health Act and concerns the records of all children aged up to 19 who call on the services of the counselling centre or the school doctor. The aim of the ECR is to ensure more efficient and effective juvenile healthcare, with problems with the child's upbringing and other social or health risks being identified at an early stage.

The ECR contains information on the physical, cognitive, and psychosocial development of the child, its social situation (family, friends, school) and – eventually – prenatal data. The standardised list of details – the 'basic dataset' – on the basis of which doctors and nurses collect information when they are consulted by the child and its parents amounts to some thirty pages. It is based on the paper version of the record, supplemented with certain data that doctors consider relevant. The ECR also comprises profiles indicating the extent to which youths are at risk of psychosocial problems. A child that scores high for risk factors such as divorced parents, poverty, aggressive behaviour or depression is placed in the 'red' category and requires extra attention on the part of JHC professionals. Other children are allocated to the 'orange' (medium risk) or 'yellow' (low risk) categories.

The ECR does not contain only medical data but is still considered legally to be a medical record. This means that the parents or the young person himself/herself – if over a certain age – must give consent for data to be provided to a third party. The law requires that the data contained in the ECR be retained until fifteen years after the end of the JHC relationship with the youth, i.e. from when he/she is 19. That period may be longer if circumstances require, for example so as to guarantee continuity of care. Both the parents (until the child is 12) and the youth is entitled to access the data in the ECR and to have it corrected. Access can involve the provision of a printout of the ECR or looking at the data on the computer during a consultation. Access may be refused in the interest of the child's personal privacy – for example in the case of a 15-year-old girl having an abortion – or that of one of the parents, for example in the case of divorce. In the 'Kidos' system discussed below, details such as the mother's address can be hidden on screen from the view of the father.

The original intention was to develop a national ECR, to promote uniformity and efficiency. After an unsuccessful tendering procedure, it was decided that it should be introduced by municipalities and JHC organisations, but subject to the ministerial responsibility of the Minister for Youth and Families. The ECR is still required to meet nationally determined specifications so as to simplify the exchange of information between JHC organisations. The intention is for the ECR to be gradually linked to the electronic patient record (EPR) so that general practitioners can also access it. By that time, access to the system will be by means of a special smartcard (the 'UZI pass'); for the present, however, access involves entering a user name in combination with a password.

4.2 Standard ECR or extended ECR?

The above is just part of the story. Opinions regarding the aim of the electronic child record and access to it have come to diverge: should it be solely a JHC record or should it also serve the purposes of youth welfare work in a wider sense? Information about a child's social background and psychosocial development can also be relevant to the work of the social services, schools, or police. Making the information more widely available would facilitate more effective coordination of youth care between the various organisations involved and – the reasoning goes – would make it easier to prevent abuse. This wider-ranging approach to use of the ECR is prompted by the desire to prevent tragic and sometimes fatal cases of child abuse, for example the shocking Dutch case of the three-year-old Savanna, killed by her mother in 2004 after continual ill-treatment and neglect. Children must be able to grow up in safety. To ensure that they can, various bodies within the youth care sector need to collaborate more effectively. The aim of the ECR is to ensure that all the information held about a child can be accessed throughout the sector. Policymakers therefore wish to extend the medical ECR (the 'standard ECR') that is currently under development into a youth care ECR (the 'extended ECR'), which would provide a more complete picture of the child and its social background.

The extended ECR fits in with the trend whereby there is an increasing focus on 'children at risk'. An at-risk child is one that is confronted by multiple social and individual problems and that runs the risk of dropping out of school, becoming unemployed, or becoming a criminal. Identifying and monitoring juveniles at risk is also the intention of the Reference Index for Juveniles at Risk. This is an information system that brings youth care professionals into contact with one another on the basis of risk alerts regarding juveniles up to the age of 23, for example when they come into contact with the police, drug or alcohol dependence, or child abuse. The Reference Index is intended to contribute to timely coordination and joint intervention within the context of youth care in problem cases. Like the ECR, the Reference Index is implemented locally on the basis of national standards that enable data to be exchanged nationwide. Unlike the ECR, however, the Reference Index does not involve exchanging data about children, but linking the two systems kills two birds with one stone.

The former Minister for Youth and Families, André Rouvoet, intended the ECR to be limited – in the first instance – to the field of juvenile healthcare. The technical and organisational diversity within that sector was simply too great for a wide-ranging ECR to be possible. He did not, however, exclude the possibility of the scope of the ECR being extended at a later date.

The local need for an extended ECR has since gained a momentum of its own. The four big Dutch cities – Amsterdam, The Hague, Rotterdam, and Utrecht – believe that it is in the interest of the child for the ECR to be more than just a medical record. It ought also to provide scope for data provided by social services, schools, the Youth Care Agency, mental health services, etc. The four cities claim that it is only through integration of all available data about a child that it is possible to trace (potential) problems within the family. They also consider it essential for the Reference Index and the extended ECR to be linked so as to combine risk alerts and information about the child and its background. The four cities have now made a significant investment in an extended ECR, meaning that economic considerations also play a role.

The obligation of medical confidentiality to which JHC staff are subject is a significant obstacle, however, to the exchange of data between the various different bodies, and consequently impedes the development of an extended ECR. It is only in exceptional cases, for example child abuse, that doctors – after careful consideration – are permitted to share medical data regarding patients. Doctors are, however, under increasing pressure to report abuse.

So as to illustrate what an extended ECR would involve, we will now consider some plans proposed by the youth care services in Rotterdam.

4.3 Every Child's a Winner

The extended electronic child record for Rotterdam is part of 'Every Child's a Winner', a wide-ranging action programme for children at risk. The aim of the programme is to bring about integrated cooperation between all the relevant bodies in the youth care sector. These include juvenile healthcare service, education sector, welfare sector, Youth Care Agency, youth care providers, juvenile mental health organisation, Child Care and Protection Board, police, prosecution service, and juvenile courts. The aim of Every Child's a Winner is to identify risks and prevent problems at an early stage.

Since 2008, the ECR has been operational – as 'Kidos' – in the healthcare sector in Rotterdam. The system records all relevant data on a child, including risk profiles, from as soon as its mother becomes pregnant. The city's policy is to ensure 100% participation. Consideration has been given to an obligation to appear, subject to penalties, so as to compel parents to make use of the juvenile healthcare system.

Kidos is administered by the Regional Health Service but youth care professionals will be given access to the information database via the Centre for Family and Children. The latter is a partnership comprising the counselling centre, the Regional Health Service and the Youth Care Agency. It is also intended to be the 'hub' at the centre of the city's youth care system. Furthermore, Kidos is linked to Rotterdam's Reference Index in order to filter out potential at-risk children from the system. In the future, data on children will be entered that is provided by the education system (the pupil information management system and the socio-educational services), the juvenile mental health organisation, and the youth care system, thus providing a complete picture. The intention is that this should form the basis for differentiation in the number of contacts with parents and children. Children at risk will be the subject of more contacts than those for whom the system indicates no problems.

4.4 Opportunities and issues

The electronic child record facilitates information processes within the juvenile healthcare sector and beyond. The nationwide infrastructure will make it a simple matter to transfer digitised records between the various JHC organisations. This will reduce the risk of a child 'disappearing' when the family moves to a different town or city. The ECR also is also meant to reduce the administrative burden when – after the link has been effectuated to the electronic patient record (EPR) – wider ranging referral options become available within the healthcare sector. Digitising information processes in the youth care sector is also intended to improve coordination of work processes and to simplify earlier identification of problems affecting children and juveniles. The introduction of digital records in the youth care sector is a feature within a broader trend towards the information society, and would consequently seem to be no more than a logical step in the modernisation of this policy field.

However, the process of digitising paper records is not without less beneficial consequences for children. Introduction of the ECR is associated with greater data intensity within the youth care/healthcare sector. Not only does it become possible to record more information about a child, but an increased number of organisations can more easily access that information and the records held by different organisations can be more easily linked. In the case of the extended ECR, the intention is for data to be shared more widely so as to acquire a more complete picture of the child. More information does not necessarily mean, however, that the quality of care will be better. Greater data intensity can obfuscate just what data is relevant and what is not. Healthcare providers will need to look for the proverbial 'needle in a haystack'. Digitising the child record can also produce more problems regarding interpretation and consequently errors, for example if the data involved is specific to a particular context but is utilised by a number of different organisations within the youth care sector. Aiming for a complete picture of the child can also lead to care

avoidance on the part of parents. There have been various media reports about highly educated parents who refuse to fill in psychosocial questionnaires for the school doctor because of a lack of confidence regarding the ECR.

Digitising data also opens up the way to using risk profiles. It is no longer merely the intention to track a child's development by periodically recording data; the child record is also used for advanced analysis of the child and its social environment. Based on a series of risk parameters, estimates are made of the likelihood that an individual child will be the subject of physical and – above all – psychosocial developmental problems. The aim of risk profiling is to ensure that potential problem children are identified at an early stage.

Based on their risk profiles, children are assigned to a particular risk category and labelled accordingly (see the 'yellow', 'orange', and 'red' categories referred to above). This means that the focus is shifted from the individual child to the type of child. It is not inconceivable that such risk categorisation will come to determine the approach that carers take vis-à-vis the child. The label that is assigned can therefore have a stigmatising and even discriminatory effect, and can lead to unjustified distinctions being made in the way children and their parents are treated. Attention needs to be paid to the long-term consequences of such stigmatisation. The fact that the child record will be retained for a long period can lead to the 'sins' of somebody's youth still influencing his or her later life because of the way he or she will be assessed or treated by the authorities (and perhaps by others too). Moreover, the limits applying to the use of this data are often only vague.

Digitising the child record alters the relationship between the child and the care professional, meaning that the child comes to be represented more frequently by a dataset or an associated risk profile. The use of risk profiles can create a reality of its own that is entirely separate from the actual individual. This is sometimes referred to as an 'abstracted identity'. As long as that identity accords with the 'real' identity, there is not really any problem. Matters become different if the registered identity does not develop – or does not develop sufficiently – along with the reality within which the child lives, or if it contains incorrect information. It may be difficult for the child or parent concerned to ensure that data or profiles are corrected if they are utilised within a chain and take on a life of their own within that chain. The 2008 annual report entitled *De burger in de ketens* [The Citizen in Chains] by the Dutch National Ombudsman reveals how someone may find himself confronted by major problems if he or she is registered incorrectly within such an information chain (Nationale ombudsman 2009). Moreover, it is unclear in many cases just which body one must approach when something has gone wrong. The ombudsman mentions the youth care sector as an example of an extremely complex organisation, with the Reference Index alone involving 24 referring bodies.

Data confidentiality is also a problem. We have already pointed out that the duty of confidentiality to which medical professionals are subject can impede the exchange of data within the youth care sector. Just how this matter is dealt with in the context of the Rotterdam project is unclear. It is also not inconceivable that care professionals may keep sensitive information out of the record so as not to harm the relationship of trust that they have with the child or the parent. Reference can also be made to the tendency (see above) of certain groups of parents to refuse to collaborate with wide-scale psychosocial screening.

Confidence in the system can also be eroded because of the central role allocated to technology. The ECR can be allocated a controlling effect due to the use of standard settings, menus, or other working methods laid down in the software which restrict the professional autonomy of the carer. A carer who is required to assess a child on the basis of a standardised checklist will be unable to record anomalous findings and may overlook other matters. The central role of ICT technology also makes the ECR vulnerable as regards security risks, for example careless use of passwords and unauthorised intrusion into the system. Those risks are more significant the more sensitive their data, and the ECR certainly does involve sensitive data.

4.5 The interests of the child?

But however one views it, the important question is to what extent the electronic child record contributes to the interests of the child as regards its being able to develop within a safe environment and to become a healthy, happy, and responsible citizen. Promoting the welfare of children – in addition to protecting society against children who have gone off the rails – is an important aim of the version of juvenile healthcare that we are discussing. But it is often unclear just how the interests, needs, and rights of children and their parents actually play a role. They are seldom made specific in the plans for the ECR.

The plans for the extended ECR hardly mentioned the legal conditions within which it is intended to operate, and this, at the very least, puts the legitimacy of the developments at risk. Both the Dutch Senate and the Data Protection Authority have emphatically referred to fundamental objections regarding the confidentiality of data and the privacy of children and their parents. It is also striking that no special guarantees have been laid down in formal legislation regarding the administration and use of the ECR in general, as has been done, for example, in the case of the electronic patient record (EPR). At the moment, development of the ECR would appear to be concerned more with speed than with caution.

The ECR is very much a technology-driven solution to the great diversity of psychosocial and health problems. It is questionable whether this is the most effective approach to the problems confronting the youth care sector. Nor is

it clear what the long-term consequences are of the chosen approach – for example the long data-retention period – and how the potentially negative effects on children can be obviated.

4.6 Conclusions

It is relevant to clarify what needs exists within the youth care sector and how the electronic child record can meet those needs. Within the discussion regarding the ECR, various different aims are entwined: more efficient juvenile healthcare, improved coordination within the juvenile care sector, prevention of child abuse, and early identification of children who are at risk. Whether the ECR is in all cases the most suitable means of achieving those aims is unclear.

More attention also needs to be paid to the choices made in designing the ECR. Collecting more information about children and the social environment in which they grow up does not necessarily mean that the quality of care will be better. It is even questionable whether identifying potential 'problem children' on the basis of risk profiles in itself risks missing the target. Specifically, the result might be an unworkably large number of at-risk children – or at least potentially at-risk children – with carers being unable to identify the genuine problem cases or having too little time to provide the necessary support. Many problem cases are already known to youth workers. The principle of selectivity – 'select before you collect' – suggests that one should specifically collect data on these problem cases so as to provide tailor-made care.

It is also questionable whether one should in fact keep close and continuous track of children and young people. Does that still enable parents to allow their children to grow up freely and uninhibitedly? Do children still have the opportunity to acquire wisdom through experience?

It is also relevant for all those involved – carers, children, and parents – to know what data is being collected, what that data is being used for, and how errors in records and profiles can be rectified. Parents and children should be given independent access to the ECR so as to simplify inspection. Such measures would increase confidence in the system.

5 Customer profiles: the invisible hand of the Internet

5 Customer profiles: the invisible hand of the Internet

Mireille Hildebrandt and Niels van Dijk

5.1 Introduction: e-commerce

Data is the new currency of the information society. In February 2010, The Economist devoted a supplement to the 'monstrous quantity of data' that is now available. As pointed out by Ayres (2007) in *Super Crunchers*, we are no longer dealing with thousands or millions of data, but with billions of data that can be stored at little expense and searched through rapidly. Pariser (2011) gives the example of Acxiom, a company specialising in marketing service and technologies, which holds some 1500 'data points' on 96% of American households and another half million individuals. This involves not only data deliberately provided but mostly data that is leaked, for example surfing and clicking behaviour. In order to still see the wood for the trees in this avalanche of data, sophisticated computer techniques have been developed for pattern recognition. This is called 'data mining', and the patterns can be used as consumer 'profiles'.

Data mining techniques are applied in various contexts. Banks use profiling for preparing credit ratings or to detect fraud or money laundering. Forensics uses profiles to solve crimes or to draw up risk profiles for potential criminals. Employers can use profiling to monitor employees for fraudulent behaviour or to estimate their skills and suitability for particular work.

In this article, we will focus on profiling in the commercial sector and specifically on the use of customer profiles on the Internet. This forms part of the broader development of e-commerce. It is important to distinguish here between individual profiles – which are the result of mining a particular individual's data – and group profiles, which result from pattern recognition at an aggregate level. We will look mainly at the way the latter are utilised by the industry, with what motives, and how this may affect consumers. We will conclude by briefly considering the legal and technical instruments that could counter undesirable consequences.

5.2 Marketing and customer loyalty

In the field of marketing, attempts to approach the customer date back to the 1970s. Instead of advertising campaigns aimed at the 'average consumer', efforts were made to subdivide the market into segments, utilising such factors as address, family, gender, age, education, and income. A segment refers to a type of consumer with particular features and needs; each such type can be the object of a specific offer. This approach has its limitations, however. The market segments are relatively static and stereotypical, being based on general geo-demographic data.

The exponential growth of computing storage capacity has made available a vast amount of data about individual people. In the online world of the Internet, people continually leave behind digital traces of themselves, which can be retrieved by means of cookies, web bugs, and other techniques. Similarly, mobile devices such as phones and laptops make a wide range of data available regarding the user's location and communication activity. This profusion of data is a goldmine for the commercial sector. When combined with powerful profiling techniques, it generates an unprecedented source of knowledge about individual and aggregate behaviour patterns (Hildebrandt and Gutwirth 2008).

Initially, this avalanche of data produced a surfeit of advertising – i.e. spam – but companies have since turned to more specific offers by means of targeted advertising. Marketing is focusing more and more on identifying the inferred preferences of (potential) customers, and is seemingly becoming increasingly clever in doing so thanks to the use of advanced data mining techniques that can reveal profitable patterns in consumer behaviour. The resulting 'knowledge' of the customer is no longer based on the assumptions of marketing agencies or on what customers themselves say about their preferences in the context of focus groups or interviews; instead, it is based on what they *actually do* online and often also offline. The thinking behind this is that the aggregated behaviour of a customer provides a better prediction of future purchasing behaviour than the information that customers provide about themselves. The company with the best data mining techniques will therefore be best able to key in to customers' wishes and preferences – even where a customer may not even be aware of them. A positive result from the customer's point of view is that he or she will no longer be troubled by irrelevant offers.

5.3 What is the purpose of customer profiling?

The primary purpose of customer profiling is to bring about improved coordination between a company's range of products and services and the needs of customers and potential customers. Customer profiling is intended to increase the effectiveness of advertising, allow offers to be targeted more precisely, and boost customer loyalty. All this forms part of what is now referred to as 'customer relationship management' (CRM), which focuses on acquiring and retaining as many lucrative customers as possible. Customers who generate little income for the company or who may fail to pay for their purchases are excluded as far as possible. Profiling is indeed also used to assess the creditworthiness of customers.

Another function is that of price discrimination: how much is a consumer prepared to pay for a given product or service? Price discrimination is a regular and basically legal practice that can generate extra profits for a company. In an

'ideal market', tailoring the price to the wishes of individual consumers can lead to a win-win situation because the price is then precisely coordinated with the customer's needs. In practice, however, price discrimination is often based on an information deficit: if the customer had known that he or she could purchase a given service more cheaply elsewhere, he or she would not have bought it. The trouble that the customer would have to go through to discover this is an advantage for the seller, who has an interest in ensuring that this situation continues. The Internet is highly suited to this kind of price discrimination. To a certain extent, price comparison sites can alleviate the customer's information deficit, but it is not always clear what the interests of the owners of such sites actually are (Stone 2010). Moreover, the sites are another potential goldmine as regards customer details that can be mined and sold on to other companies, which will have adverse effects on the customer's privacy.

5.4 How does customer profiling work?

Profiling is utilised to identify potentially interesting customers, offers that are likely to interest those customers, the price they are prepared to pay, their readiness to switch to a different brand, or the likelihood that they will remain a customer. A good example of such profiling is Google Analytics, one of the major players in the Web statistics market. This application merits more detailed consideration here because it is used by numerous companies and provides a good example of the various different types of customer profiling.

Google Analytics makes it possible to keep detailed track of what kind of users arrive at a given site and from which other site or search engine. It also tracks how long they remain at the site, what they click on, how often they return, etc. This data is acquired by installing software on the site of the website owner that is using Google Analytics and on the computers of users of that website. Google Analytics generates statistical relationships and overviews that enable the website owner to optimise the design of its website and to earn money from the clicking behaviour of visitors. The latter involves auctioning advertising space around specific keywords. Companies bid for this advertising space if they believe that their products or services will interest visitors to sites that utilise the keyword concerned. The highest bidder gets the opportunity to advertise and pays a per-click charge to the owner of the website. The company can also analyse how much income its advertising ultimately generates, so that it can then focus on the most lucrative sites.

In order to understand how a Web statistics application such as Google Analytics actually works, we need to distinguish between various different types of profiles (Custers 2004). Firstly, there are group profiles; these are derived from data of large numbers of individuals, their behaviour, and the context within which they display certain behaviours. One example is market segmentation. Based on such features as an individual's postal code, online surfing and purchasing behaviour, the use of search terms, statistical inferences can be drawn regarding the customer's future behaviour, in particular purchasing behaviour or credit risks. To the extent that firms such as Acxiom or Experion have access to data that correlates with health risks, they infer highly sensitive information. Their inferences could be based, for example, on online purchases of medication, the use of search terms such as 'depression' or ' intestinal cancer', or visits to websites run by patient associations. The inferences drawn have a market value for life insurance or health insurance companies. The fact that these group profiles are probably derived from anonymised data implies that the EU's Data Protection Directive is not applicable and cannot prevent their being sold.

A group profile may be correct at the aggregated level of the market segment concerned. However, because we are dealing with statistical relationships, group profiles are not automatically applicable to individual persons. That is a familiar problem in the field of epidemiology: the fact that a group displaying certain features has a 1 in 24 risk of developing breast cancer does not indicate which individual out of any given 24 will actually develop it. A company that applies group profiles to individuals can therefore easily get things wrong. Nevertheless, because large numbers are involved, the application will in all likelihood be profitable in the long run.

In addition to group profiles, we distinguish individual profiles, which are derived from data on a single individual. Recording and analysing the steady stream of data on somebody's online and offline behaviour – for example surfing, downloading and uploading, e-mailing and chatting, 'friending' in online social networks, blogging, and the use of search terms – will reveal patterns that provide detailed information on that person's interests and preferences, on her daily comings and goings and on her specific public and private life.

Combining an individual profile with group's profiles can provide a general insight into an individual's recurring activities, risk of illness, accidents or other kinds of harm, tax avoidance or other contraventions, and a ranking of her personal preferences and capabilities. This can include such various aspects as the newspaper she prefers to read, how her income is likely to develop, what sort of underwear she wears, the films she likes to watch, and how much she is prepared to spend on a car, at the funfair, or at the ballet. It goes without saying that such individualised profiles are worth their weight in gold. The industry's frequent mantra of 'free content' – for example a free online newspaper or webportal – is based on this ability to record and analyse online behavioural data and in fact confirms that there really is no such thing as a free lunch.

5.5 Undesirable consequences

As we have seen, applying group profiles to individuals often produces incorrect relationships. One undesirable consequence of this is that the inclusion or

exclusion of someone in a group profile will often be incorrect. Depending on the specific context, this can involve disadvantages both large and small for an individual customer: the person concerned may not receive certain offers, may need to pay a higher insurance premium or indeed be refused insurance. We will consider three undesirable consequences that may arise even if the inferred correlations are in fact correct: invisible infringements of privacy, unfair exclusion, and lack of due process (Zarsky 2002–2003).

5.5.1 Infringement of privacy

In the world of ICT, privacy is often defined in terms of the protection of personal data. That is in fact a rather poor definition. Protecting personal data is actually only one way of protecting privacy. In our view, privacy is a broader concept, neatly expressed by Agre and Rotenberg: in the information society the right to privacy is '...the freedom from unreasonable constraints on the construction of one's own identity' (Agre and Rotenberg 2001, p. 7). 'Identity' here means not a collection of personal data but the way in which someone shapes his or her own identity and develops it in relation to other people. This extends to someone's picture that others – including businesses – create.

Let us assume that my keyboard behaviour suggests that I have an increased risk of developing Parkinson's disease, for example, or that my circle of friends on Facebook implies that I am probably gay (Jernigan and Mistree 2009). It is undesirable for other people to acquire such sensitive information – and potentially act on it – without my being aware of this.

However, the use made of this kind of information can in fact go even further. Let us assume that my surfing and clicking behaviour are recorded without my actually being identified, for example because my keyboard and mouse behaviour mean I am recognised as being one and the same person in *terms of this behaviour*. My name, street address, and IP address (which is generally considered to be personal data in the sense of the EU's Data Protection Directive) are not required for this recognition, meaning that it is not clear whether the data protection legislation actually applies. The individual profile thus created is subsequently matched with various group profiles, from which it is possible to conclude, for example, that I am about to become a vegetarian. That information is then sold on to a nationwide supermarket chain from which I order my groceries online. Based on Web statistics, the supermarket chain calculates the probability that I will not in fact become a vegetarian if I am offered some free meat products next time I place an order. In this way, the supermarket chain will attempt to influence my preference for vegetarian products. This could also be done by placing individualised banners on websites that I frequently visit, referring to scientific research that sheds light on the negative health effects of a meat-free diet. It may well be that these offers and advertorials will lead me to decide to continue to eat meat.

This kind of manipulation is a greater infringement of my autonomy – and by association my privacy – then the simple fact that some of my personal details are known to other people. In the example given, information regarding my preferences is in fact being generated and utilised behind my back. Based on anonymised group profiles that I know nothing about, I am being categorised and enticed into certain purchasing behaviour. Indeed, my preferences are being manipulated by means of targeted interventions that I am not aware of. This seems to equate with a kind of subliminal manipulation.

5.5.2 Unjustified exclusion

In the age of data mining, unjustified exclusion is particularly problematical because it is invisible. When considering job applications, employers can utilise software that generates extensive profiles of candidates based on information that is publicly available on, or invisibly mined from, the Internet. This could be seen as an infringement of privacy if the candidate is assessed on the basis of information that she considers to be part of her private life. Moreover, based on such profiling, prohibited factors could be used for the assessment. Profiling may reveal, for example, that a female candidate is probably pregnant or suffering from a certain disease, despite these being matters that the employer is not permitted to ask about during her job interview. The fact that such profiling takes place behind the candidate's back also makes it difficult – if not impossible – to protect oneself against exclusion.

5.5.3 Lack of due process

Due process is a principle of criminal law that requires justice authorities to respect the procedural rights of a defendant. In the context of criminal law, a defendant is entitled to fair treatment and must be able to challenge decisions or actions taken in relation to him or her. Important aspects of due process are transparency and the possibility to require an independent determination of guilt. It enables the defendant to contest the charges and invoke principles such as privacy, fair play, or non-discrimination. In a more general sense, due process refers to our capability to contest actions or decisions that affect the opportunities and the risks we encounter. In this broader sense due process is not restricted to the context of the criminal law, but regards our capability to challenge the way in which major players restrict the freedom of the citizen.

Invisible profiling is problematical because one cannot challenge something that remains concealed. Although the EU's Data Protection Directive enshrines various rights regarding transparency, it is no easy matter to actually assert and enforce them. Article 12 of the Directive gives a person the right to 'knowledge of the logic involved in any automatic processing of data concerning him'. Currently, however, it is not feasible for a consumer to find out how he or she has been profiled. The recent upheaval about Facebook's refusal to provide access to the personal data they have in store is a telling example. Even if the company concerned were to be prepared to provide the relevant information,

the consumer does not have the facilities for checking whether that information is in fact accurate. Moreover, the preamble (Recital 41) to the Data Protection Directive provides that the right to know how one has been profiled must 'not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software' and perhaps even the profiles themselves (Van Dijk 2009 and 2010). This is exactly the point made by Facebook.

5.6 Conclusions: a need for control and feedback

As regards the positive aspects of customer profiling, we must necessarily be brief. E-commerce offers new and promising opportunities to contribute to prosperity and well-being, but utilising those opportunities requires greater attention for the position of the consumer. Individual consumers are hardly aware of what data is collected on the Internet and what is done with it. It is important for national and European legislators to provide effective protection against the undesirable consequences of customer profiling as indicated above (see also Hildebrandt and Koops 2010). The European Union's 2009 'Cookie Directive' obliges Member States to introduce an opt-in regime for the installation of cookies with a view to collecting data on online behaviour for such purposes as targeted advertising. To that end, the Dutch legislature has added a new Section 11.7a to the Telecommunications Act requiring that the customer consent to his/her data being mined in this way. That consent must be acquired unambiguously and prior to a cookie being installed. The pressing question in this context is how this process of consenting will be organised in actual practice: a browser setting allowing generic consent for all websites will no longer be sufficient, but constantly recurring requests for consent would be awkward and irritating, and will undoubtedly lead to people just giving generic consent or refusal, simply in order not to be bothered any further.

Analysis of customer profiles shows however, that the real problem is not so much that of collecting one's online behavioural data; rather, the core of the problem is the lack of transparency regarding the consequences of doing so. What is particularly important is the question of what kind of profiles we are matched with and what consequences will ensue.

That problem can be tackled by incorporating effective control by the customer and feedback for the customer into the very software and hardware that make customer profiling possible. Control here requires that it is both technically possible and practically easy to exclude or anonymise data. A variety of 'privacy enhancing technologies' (PETs) are now available (Borking and Raab 2001, Dolinar et al. 2009) for these purposes.

Feedback means that the customer can gain insight into the consequences that others attach to her online behaviour. This can be achieved, for example, by obliging companies to clarify why they decide whether or not to make certain offers available to a customer. The customer must also be able to easily check

the accuracy of the information on the basis of which such decisions were taken. To that end, 'transparency enhancing technologies' (TETs) must be developed. If I can see that I have been profiled as somebody who intends to stop smoking, I will be able to 'interpret' the offers of free cigarettes as an attempt to prevent me from doing so. The substance underlying the concept of autonomy is thus restored. If I can see that I have been categorised as a defaulter because my postal code has been combined with an incident concerning an unpaid bill from years ago, I must be able to contest this categorisation. That would be due process 'in action'.

Insight into the processes involved in customer profiling is a condition for the individual consumer to be able to exercise her rights. Only in this way will consumers be enabled to deal more effectively with the flow of details they generate, as they increasingly shift their commercial activities to the Internet.

The downside of the Schengen Information System

6

6 The downside of the Schengen Information System

Michiel Besters

6.1 Introduction

When the internal market within the Schengen Area was established in 1995, the internal borders were removed between Belgium, France, Germany, Luxembourg, the Netherlands, Portugal, and Spain. From that point on, the external borders of the Schengen Area have been the main control location for persons and goods travelling into or out of the Schengen Member States. Lifting the border controls between the individual Member States has made it necessary to impose measures to maintain public order and security within the Schengen Area. Those measures were set out in the Convention Implementing the Schengen Agreement (1990), one of which involves the introduction of an information system to support collaboration between the police and judicial authorities of the Member States, namely the Schengen Information System (SIS).

This article will describe the development of the Schengen Information System. It will consider how the system registers individuals, the legal position of those individuals, supervision of the functioning of the system, and the technical and organisational problems that arise. Development of the SIS cannot be viewed in isolation but needs to be seen in the broader context of the digitisation of EU migration policy (Besters & Brom 2010; Broeders 2011). Besides the SIS, various other databases are being developed and implemented – for example Eurodac and the Visa Information System – so as to control flows of migration. Given its pioneering role, the SIS can act as a kind of litmus test.

The SIS registers people and goods that must be refused entry to the Schengen Area or that are being sought by a Schengen Member State, for example undesirable aliens, missing persons, stolen cars, or stolen identity documents. Registration means that an 'alert' is entered into the SIS. The SIS currently includes more than 35 million such alerts, for more than 29 million identity documents, four million vehicles, and one million persons (Council of the European Union 2011). Almost 80% of the persons registered are undesirable aliens. These include persons who are not subjects of an EU Member State and therefore required to hold a visa, and who have exceeded the period during which they are permitted to stay.

The number of Schengen Member States has increased considerably. When the Scandinavian countries acceded to the Schengen Agreement in 1996, the SIS had to be extended because its technical capacity was insufficient at the time for the new Member States to be integrated. It was decided that a second-generation SIS (SIS II) should be developed. This would not only allow new Member States to join but would also make possible new technical functions. When it became clear that SIS II would not be ready before the millennium, it was decided that the capacity of SIS should be expanded so as to in any case give the Scandinavian countries access to the system. This temporary solution is referred to as 'SIS I+'. The necessity of developing SIS II became even more apparent in 1999 when a number of provisions of the Schengen Agreement (the Schengen acquis) were integrated into the Treaty on European Union. The external borders of the Schengen Area consequently became the same as those of the European Union, meaning that all EU Member States need to be able to access the SIS.

The original intention was for SIS II to be available by 2006, at the point when the various Eastern European countries joined the EU. Delays in developing the system meant, however, that this has not been possible. A temporary technical adaptation of SIS I+ was intended to provide a solution, namely SISone4all, the version of the system that is currently in operation. Compilation of SIS II was again postponed in 2009 until at least 2013. As the former Dutch Interior Minister, Guusje Ter Horst, remarked: 'I wouldn't say that it [i.e. the current system, MB] has just been knocked together, but it's less advanced than is actually possible.' (ANP 15 January 2009).

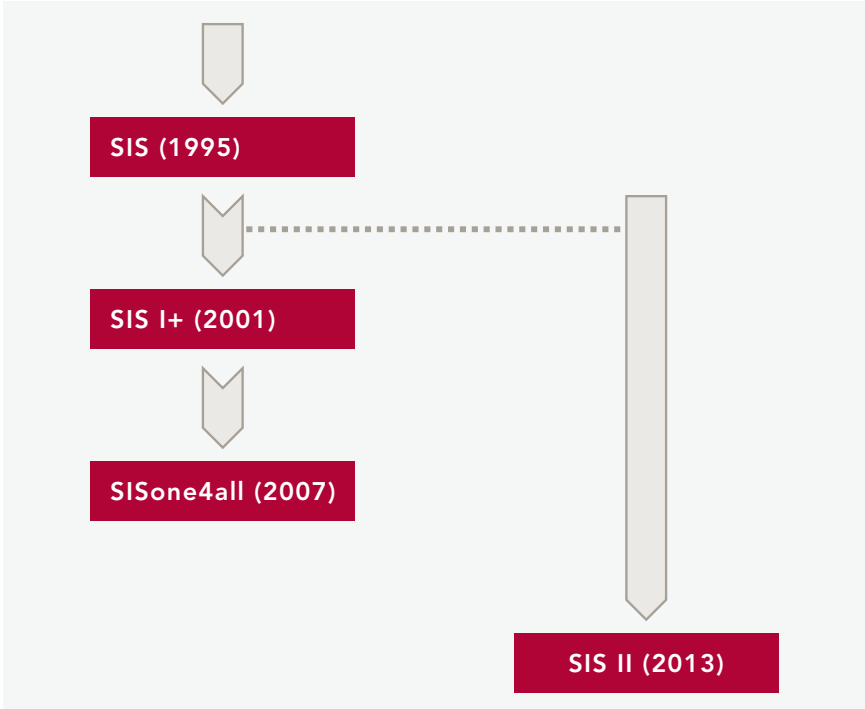

Figure 1: Chronology of the various versions of the SIS

The accession of new Member States has made implementation of the system and political decision-making increasingly complex. Joanna Parkin, researcher at the Centre for European Policy Studies, argues that a lack of political control at EU level is a significant complicating factor in this regard (Parkin 2011). This means that development of the first and second-generation SIS is pretty much a Sisyphean labour. The diffuse political decision-making has resulted in a large quantity of information: proposals by the European Commission, decisions adopted by the Council of the European Union, and reports and studies by various working parties. This enormous quantity of information makes it difficult to gain a clear picture of the developments regarding the first and second-generation SIS. This led in 2003 to serious criticism by the European Parliament, which said that SIS II was 'very opaque, difficult to follow even by experts and completely incomprehensible for normal people' (European Parliament 2003).

6.2 Alerts regarding individuals

The SIS has five categories of alerts regarding individuals: (1) extradition, (2) refusal of entry to the Schengen Area, (3) missing, (4) witness to or convicted of a crime, and (5) a suspect or a threat to the State. Depending on the kind of alert, personal details are recorded and also the reason for registration, the measures to be taken, and whether the person concerned is, for example, armed or violent. About one million alerts are entered, altered, or deleted each day.

The SIS is a 'hit–no hit' system. When a person is checked at the border or within the Schengen Area and is found to be registered in the system, the system generates a 'hit'. This can lead to the individual concerned being arrested or deported, or to goods being seized. In 2008, the SIS generated more than 120,000 hits.

The decision to include an alert regarding an individual or item in the SIS is taken by the police and judicial authorities of the Member States. In the Netherlands, for example, that decision can be taken by the Immigration and Naturalisation Service. The domestic legislation of the Member State is decisive when assessing when an alert rises to 'Schengen level'. In Spain, for example, failing to comply with one's obligation to pay alimony or child support is a criminal offence and can result in registration in the SIS. This is in contrast to the Netherlands, for example, where failure to meet that obligation is a civil matter.

The decision by a Member State to declare someone to be an undesirable alien means that all the Members States are required to prevent that person entering the Schengen Area. This can have drastic consequences for the person concerned. If that declaration is issued by the Dutch Minister of Justice, for example, the person concerned may be excluded for decades.

6.3 Architecture

The SIS consists of two components, a central component (C.SIS) located in Strasbourg and a national component (N.SIS) located in the Member States. The Member States are responsible for registrations in their national systems. There are a total of more than half a million terminals within the Schengen Member States with access to the SIS. So as to make the information from a Member State's system available to other Member States, the N.SIS is synchronised with the central system. The Member States' systems therefore constitute the active components of the first-generation SIS.

In the case of SIS II, a different relationship between the central and national systems has been selected. In SIS II, data is entered directly into the central database via a national interface. This is also based in Strasbourg, with a backup system in Sankt Johann im Pongau (Austria). The national systems are a kind of conduit. Member States can also decide to save a copy of the data within their national system. The emphasis of SIS II is consequently more on the central system.

When SIS II was being developed, a flexible architecture was chosen so as to make the system viable for the long term. The architecture was designed in such a way that the technical possibilities as regards new functions are already incorporated into the system. These latent functions can then be activated pursuant to a joint decision by the Member States. This solution has been chosen so that construction of SIS II will not be blocked because of the negotiations between the Member States on those new functions. The architecture incorporates five new functions:

- wider access for national and international security and investigation services such as Interpol, Europol, and Eurojust;
- biometric identification through the entering of fingerprints into a supplementary database;
- new categories of alerts: terrorism suspects, hooligans, and abducted children;
- alert linking, for example linking of criminals to terrorism suspects;
- linking to the Visa Information System in which people are recorded who submit a visa application.

National SIRENE agencies (Supplementary Information Request at the National Entry) have been set up to support the SIS. These are the human link within the SIS. Their task is to monitor alerts that are entered into the system. A SIRENE agency can also be requested to provide additional information to the police and judicial authorities of other Member States.

6.4 Legal position of individuals

Registration in the SIS can have serious consequences for the individual concerned, for example if he or she is declared to be an undesirable alien. Attention to such persons' legal position is therefore very important. From that perspective, the functioning of the SIS is open to criticism. Interpretation of the criteria for an alert regarding an individual by the Member States is a problem, for example, because it leads to a legal inequality within the EU. A report by the Netherlands Court of Audit shows, for example, that there were major differences shortly after the introduction of the SIS in the Netherlands between the 25 regional police forces regarding application of the criteria for alerts regarding individuals (House of Representatives 1996–1997a). In addition, a study of national data protection authorities commissioned by the Joint Supervisory Authority of Schengen shows that there are also major differences in interpretation between Member States (Joint Supervisory Authority of Schengen 2005, 2007, 2009a, and 2009b).

One example of this is the way the German authorities label persons who have been refused political asylum as undesirable aliens. France's Conseil d'État ruled in 1999 that this kind of categorisation was illegal. Under the Convention Implementing the Schengen Agreement, persons may only be registered as undesirable aliens if they are persons from outside the EU who constitute a genuine danger to public order and security in a Member State, or who are illegal immigrants. The mere fact that somebody's request for asylum has been rejected is not covered by this criterion. Reports by the German data protection authorities show, however, that in 2004 the German police and judicial authorities were still designating those who had been refused political asylum as undesirable aliens in the SIS.

It is questionable whether the introduction of SIS II will improve harmonisation of the criteria for alerts regarding individuals. The British human rights organisation JUSTICE does not have very high hopes in this respect (House of Lords 2007). JUSTICE bases that opinion on the disparity between the proposed and the definitive rules for SIS II. In the original proposal, it was stated that the criteria for registering an alert needed to be harmonised. In the regulation as ultimately adopted, this harmonisation requirement has been downgraded, with reference being made only to 'consultation regarding harmonisation must be continued'.

There is also a second reason why attention needs to be paid to the legal position of individuals. There are in fact gaps in the legal protection for people who are registered. In the first place, undesirable aliens are not notified of the fact that they have been registered in the SIS. In the Netherlands, they are told that they have been declared 'undesirable' but not that they had been registered in the SIS; they only become aware of this if they wish to re-enter Europe (Nationale ombudsman 2010). The second point is associated with the first: exercise of the right of inspection, correction, and deletion by registered individuals. Where the exercise of these rights is concerned, the Convention Implementing the Schengen Agreement refers to the domestic law of the Member States. According to the lawyer Evelien Brouwer, however, effective procedures for contesting one's registration are often lacking (Brouwer 2008).

Complications frequently arise when someone decides to exercise his right of inspection, correction, or deletion. The Convention states, for example, that the ruling by a court in a given Member State is binding for all Member States. In practice, however, this is often merely wishful thinking. There have been a number of cases in which a Dutch court found that the alert for an individual entered by the Spanish authorities was unlawful and that it should be deleted. This was only actually done, however, after the intervention of the Dutch Data Protection Authority, which contacted its counterpart in Spain.

6.5 Supervision and control

There is also a lot to criticise in the way the SIS functions as regards supervision and control. In the Netherlands, it is the Immigration and Naturalisation Service that is responsible for most alerts regarding individuals, namely aliens who must be refused entry to the Schengen Area. During checks at the border, undesirable aliens are held by the Royal Netherlands Military Police, which then submits an alert proposal to the IND. A study by the Dutch National Ombudsman has shown that the IND virtually always accedes to the Military Police's proposal without itself considering the facts of the case (Nationale ombudsman 2010). As a result, even a minor mistake – for example exceeding the period during which one is permitted to stay by only a few days – can lead to someone being registered in the SIS.

For all other registrations of individuals, the responsible authority in the Netherlands is the prosecution service. The Public Prosecutor decides on the basis of the underlying file whether registration complies with the criteria set forth in the Schengen Agreement. A study by the Dutch Data Protection Authority has shown, however, that the underlying documentation is not always available, meaning that it is not possible to check whether a registration is in fact legitimate (College bescherming persoonsgegevens 2008).

Data management within the SIS has also been criticised. The design for the Dutch national system for SIS I did not provide for overviews to be produced of alerts that had been entered, that were outstanding, or that needed to be withdrawn. As the Netherlands Court of Audit found in its 1997 report, this meant that the system offered insufficient options for preventing file corruption and for evaluating the effectiveness of the system (House of Representatives 1996–1997a). The report led to the necessary facilities for effective data management being implemented in 1999.

Similar problems also occur at European level. Since the SIS was introduced, a number of reports have been published irregularly and via a variety of channels. According to criticism by the European Parliament, this approach leads to an atmosphere of secrecy regarding the information, something that hampers democratic control of how the system functions (European Parliament 2003). At the moment, annual statistics are in fact published by the EU but only as concerns the central system. Reporting therefore remains incomplete and incorrect.

The European Parliament has repeatedly argued for the introduction of an agency to conduct strategic management of the SIS and other large-scale European information systems such as the Visa Information System. An agency of this kind would be intended to make the functioning of the information systems more transparent and increase democratic control of them. In 2009, the European Commission published ambitious proposals for such an agency, which would not only be responsible for operational management of databases but would also become a centre of expertise. The European Data Protection Supervisor (EDPS) responded positively to the Commission's proposals, but recommended caution: an agency should only be set up if its duties and responsibilities were clearly defined. According to the EDPS, that was not the case in the Commission's proposals (European Data Protection Supervisor 2010).

6.6 The future of SIS II

The importance of completing the introduction of SIS II has become ever more pressing. Development of SIS II has been subject to considerable delay, however, due to uncertainty regarding funding, problems during the tendering phase, and negotiations regarding new functionality for the system. It would seem that history is repeating itself: the first-generation SIS struggled with comparable problems. Recent developments during the testing phase for the SIS II have led to the Council of the European Union and the European Commission referring to a genuine crisis.

A number of problems were identified during a test of SIS II in 2008. Data from the national and central components turned out not to correspond, alerts had disappeared or had been duplicated, and the central system was unable to cope with the volume of data entered. The biggest problem seems to be the capacity of the central system, which was designed to deal with 15 million alerts. Currently, however, SISone4all already contains more than 35 million alerts, a figure that will only increase due to the participation of the new Member States. A progress report on SIS II in 2009 indicated that the accession of the latter meant that the central system needed to be able to continue to function without a hitch with up to 60 million alerts (Council of the European Union 2009).

Various measures have been implemented in order to advert the crisis with SIS II. As a precaution for the eventuality that SIS II is a failure, an alternative scenario has been drawn up. In addition, external IT consultants have been brought in to produce a diagnosis of SIS II. That diagnosis is moderately positive: with some repairs and improvements, it is probably possible to rescue the design for the system. Despite this positive diagnosis, it has nevertheless been decided that the emergency plan should be further elaborated, thus creating the impression that the Commission and the Member States are still not convinced that things will work out well with SIS II.

The delays mean that the increasing costs are becoming all the more relevant. Development of the central system for SIS II will be financed from EU funds. The cost involved up to 2013 will amount to more than EUR 140 million. The cost of developing the national systems will be covered by the Member States themselves. Up to the present, the cost for the Netherlands amounts to some EUR 21 million, whereas the original estimate was EUR 14 million. This is because the delay caused by the problems during the testing phase cost the Netherlands an additional EUR 7 million for developing its national system. In addition, there are the costs involved in keeping the present system operational; the Dutch Interior Ministry estimates these at EUR 3 million (Computable 2009).

Despite all these problems, a new version of the SIS remains a necessity, not only to keep the promise made to the new Member States but also in the interests of the 'old' Member States. For the present, it has been decided to continue with the initial design for SIS II. The thinking here is that so much money has already been put into SIS II that it would be a pity to cease development. It remains to be seen whether this was the right political decision. Will SIS II – which has already devoured so many millions of euros – collapse under its own weight and will significant expenditure be necessary to implement an emergency plan? Or will SIS II succeed in bootstrapping its own way out of the morass?

6.7 Conclusions: a 'SISyphean' labour

Removal of the interior borders within the Schengen Area has led to a clear necessity for European information systems such as the SIS with which the police and judicial authorities can exchange information. As we have seen, however, development of the SIS has been anything but trouble-free. From the very beginning, the system struggled with teething troubles. Since then, the increased number of Schengen Member States and the planned functional expansion have only served to put development under further pressure. Besides technical and administrative problems, the SIS has to deal with gaps in the legal position of registered individuals. Supervision of how the system functions also leaves something to be desired.

Given the above issues, the question that arises is whether a database of the size and complexity of the SIS can in fact function properly. At the very least, one can conclude that a large-scale European database has its limitations.

If no account is taken of those limitations, then a database like the SIS is pretty much doomed to be – in the words of a former Dutch MP – a 'rickety old jalopy' (House of Representatives 1996–1997b). Given the ambitions regarding digitising European migration policy, that is a worrisome diagnosis.

Acknowledgements

I would like to express my thanks to the following persons who helped me with my 'SISyphean' labour. In random order: Evelien van Beek (Dutch Data Protection Authority), Petra van Dorst (Dutch National Ombudsman), Peter Michael (Council of the European Union), Richard Rinkens (European Commission), Dirk Hoogenboezem, Susan Lasschuit-Lavalaye, Chris Michel, Wijnanda van der Zwan, Wally Ruytenbeek, Judith Hoogesteger, and Peter Tazelaar (National Police Services Agency), Wilbert Schel (Ministry of the Interior and Kingdom Relations), Dennis Broeders (Scientific Council for Government Policy), Joanna Parkin (Centre for European Policy Studies), Geert Munnichs and Mirjam Schuijff (Rathenau Instituut).

7

Dynamics of the Municipal Personal Records Database

7 Dynamics of the Municipal Personal Records Database

Ellen Boschker, Peter Castenmiller, Arre Zuurmond

7.1 Introduction

Governments have always kept records of their subjects. The onward march of information and communication technology (ICT) in the twentieth century has had a major impact on such records and has greatly increased their size and quality. The function of those records has also changed, with some of them taking on the function of a basic register, i.e. a database intended to be an authentic source of information regarding people and property in the context of data management by public authorities and related organisations. In the Netherlands, the Municipal Personal Records Database, the Land Register, and the Trade Register function as such authentic registrations. These basic registers together form an information system that is meant to facilitate the exchange of data between public bodies, and thus to improve the quality of the public services.

Discussion of basic registers generally concerns optimising their design, with the convenience of the citizen being primary. Unfortunately, this means that the wider political and social significance of basic registers is relegated to the background. In this essay, that significance is discussed on the basis of the Municipal Personal Records Database. Based on an historical sketch, we will show that basic registers are not only necessary for the government to function optimally but also have great significance for the constitutional state and for society in general. We will argue that the use of basic registers involves a tension between control and emancipation. Basic registers can be deployed as tools with which the government can control society but can also act as a means of emancipation.

Our article is structured as follows. In the opening section, we introduce as our example the modernisation of the Municipal Personal Records Database in the Netherlands. We then set out the key concepts dealt with in the essay, namely control and emancipation. Section 4 sketches the historical development of the municipal database. That historical sketch clarifies the importance of registers for the constitutional state and for society in general as well as the tension that exists between emancipation and control. We then go on to describe current developments, including the important role played by computerisation. In the final section we summarise our findings and make recommendations for modernising the Municipal Personal Records Database.

7.2 The Municipal Personal Records Database

As pointed out in our introduction, the Municipal Personal Records Database is a component in a system of basic registers. Basic registers contain details of all individuals, businesses and institutions, and are of major importance for the proper functioning of government.

The Municipal Personal Records Database was introduced in the Netherlands on 1 October 1994. It is managed by a registration agency that is part of the Ministry of the Interior and Kingdom Relations. The register can be described as '…a group of computerised municipal databases that are connected to one another and to other public authorities by means of a data communication network' (Lütter & Van Troost 2008, p. 21 [our translation]).

This definition comprises two essential elements of the Municipal Personal Records Database. Firstly, the municipality incorporates the personal records into a computerised system, which comprises all general personal details and changes in them, from birth through to death. An electronic personal list is created for every member of the Dutch population, comprising the following details:

- civil status (name, gender, data birth, place of birth, personal details of parents, marital details, registered partnership, children, and death);
- details of children and parental authority;
- nationality;
- right of residence (in the case of aliens);
- the municipality where someone is registered and his/her address within that municipality;
- details of residence in and departure from the Netherlands (in the case of people who remain here only temporarily);
- registration numbers for the person registered and for his/her parents, spouse (or ex-spouse) or registered partner and children;
- the Citizen Service Number for the person registered and the above-mentioned relatives;
- use of the surname of the partner (or ex-partner).

The second essential element of the Municipal Personal Records Database is that messages are exchanged via an electronic communication network with other municipalities and other organisations, for example in the case of a change of address or notification of death. The database is an 'authentic' basic register for all government bodies (and quasi-governmental bodies) that require personal details to perform their duties. This involves hundreds of organisations, for example the Tax Administration, the Social Insurance Bank, and pension funds. All public-sector bodies must utilise the Municipal Personal Records Database as the basis for personal details. It determines, for example, whether someone receives support from local or national government. Someone will only receive the statutory old-age pension if the data in the municipal database

indicates that he or she in fact qualifies. When somebody dies, a message is sent from the register to the Social Insurance Bank, which stops payment of his or her pension. The Municipal Personal Records Database is therefore the source of information regarding personal details.

Early in 2001, the ad hoc Modernisation Advisory Committee for the municipal databases gave the starting signal for modernising the Municipal Personal Records Database. According to the committee, it should be possible to consult the register online. Users should have access 24 hours a day and 7 days a week from every municipality in the Netherlands (Lütter & Van Troost 2008).

7.3 Control and emancipation

The modern state is based on bureaucracy as its organisation form. A modern bureaucracy requires systems of standardised registration in order to identify and contact citizens and to collect information about them. The authorities require this information in order to exercise 'control'. From the perspective of the citizen, the relevant registers can also acquire an emancipation function. We will explain both aspects below.

Our view of the modern state is to a large extent based on the bureaucracy theory of the German sociologist Max Weber (1922|1978). Weber studied bureaucracy as a rational form of organisation. He considered bureaucracy as the ultimate form of rational administrative organisation. In his opinion, this could be seen, on the one hand, as positive because it is only in that way that organisations can function rationally, carefully, and impartially. On the other hand, Weber also understood – and foresaw – that there are hazards implicit in far-reaching bureaucratisation. Without political guarantees, there is a danger that bureaucracy will become highhanded and out of control. Bureaucracy is thus both a condition for democracy and a threat to it. In other words, Athens can lead to Orwell.

In normal usage, the term 'control' often has the latter, negative connotation; for us, however, that is not the case, or rather: not necessarily. As Weber indicates, the control aspect of identification and registration is essential for bureaucracy to function. Information in the Municipal Personal Records Database can, for example, enable the authorities to ensure that people comply with their obligation to pay taxes. The Trade Register makes it possible to determine whether an organisation that presents itself as a business actually is one; it is only then that market parties can do business with one another on a basis of mutual good faith. The Land Registry provides a guarantee that a given item of property really does belong to the party that puts it up for sale or rent. These examples show that a system of basic registers makes society manageable.

The emancipatory aspect of a system of personal records does not receive much attention, despite registration and documentation being essential if people are to matter in a complex, large-scale, modern world. There are countless (negative) examples to illustrate this, one of them the position of people in developing countries. There are still large numbers who have no access to education because the State does not recognise them as citizens. It is true that international treaties and UN charters guarantee everyone certain rights, but without proper registration – without the necessary 'official papers' – it is a difficult matter to actually enjoy those rights, for example the right to vote and the right to education or healthcare. Without a system of personal records, no one is free to travel (because he/she does not have a valid travel document such as a passport), to set up a business (because he/she cannot register with the trade register or the land register), or to vote (because he/she is not on the electoral roll). In other words, someone in this situation is unable to exercise the rights of a free individual. This emancipatory dimension is also the basis for the principle that 'Every child shall be registered immediately after birth and shall have a name' enshrined in the United Nations International Covenant on Civil and Political Rights (1966). In short, a system of registration documents someone's existence and gives him/her access to social and political rights.

As we will argue below, the use of a system of registers involves a continuous tension between control and emancipation. That tension is linked to the relationship between the citizen and the authorities. The position of the authorities is strengthened if the system is focused primarily on control. If, however, a great deal of attention is paid to the exercise of one's rights, registration in fact strengthens the position of the citizen (Caplan & Torpey 2001). Like Weber, we would argue that there needs to be a balance between these two aspects so as to ensure that society remains manageable but at the same time to prevent bureaucracy becoming highhanded.

7.4 Development of the Municipal Personal Records Database

This section outlines the historical development of personal records databases. We hope to clarify the tension between control and emancipation that is inherent to the system of registration.

7.4.1 Development of the first registers

In the sixteenth century, a growing need began to be felt for regulation against the background of increasing trade, urbanisation, the introduction of the money-based economy, and population increase – in other words a more complex society. That need was felt both by rulers – who wanted a more efficient system for levying all kinds of taxes from their increasingly wealthy subjects – and by the subjects themselves, who needed rules and guarantees in the business transactions between them. The same need was felt by the ecclesiastical authorities, which wished to maintain their grip on the moral conduct of their followers. Church registers of baptisms, marriages, and births

were introduced in order to combat such abuses as bigamy, incest, unmarried cohabitation, and marriages involving minors.

In order to be able to levy taxes, every district from the late Middle Ages on had its own tax register comprising information about taxation on homeownership (hearths, fireplaces, and chimney money), landholdings and capital, and inheritance. This illustrates the control aspect of registration. However, registration also involved emancipatory aspects. The rights assigned to cities from the thirteenth century on guaranteed a certain measure of independence to their citizens vis-à-vis the arbitrary will of temporal rulers. In order to invoke these rights, one needed to be registered as a burgher. A burgher was entitled to live within the gates of a city with city rights. In fact, it was only people who could support themselves financially and contribute to the prosperity of the city who qualified as burghers, whether or not in return for payment (Holthuizen-Seegers & Wens 1993).

7.4.2 Establishment and exercise of freedoms

Until the sixteenth century, the emphasis in registration was on the control aspect of identification and registration, in particular with a view to levying taxes. It was primarily in the sixteenth century – certainly in the Netherlands – that city rights and the privileges of cities and their inhabitants became a political issue as part of the resistance to the Habsburg rulers Charles V and his son Philip II. In the sixteenth and seventeenth centuries, the emancipatory aspect became increasingly significant in Europe. One feature of this period were the increasing endeavours – primarily in England and France – to ensure that the citizen was protected against the power of the king. Such classic freedoms as freedom of speech and freedom of property were formulated and propagated with growing force.

According to Bovens (1998), it was in this period that the liberal layer of the constitutional state was formed, which offers the citizen protection against the power of the government. With the establishment of ownership relationships, the rising middle class and large landowners could safeguard their economic freedoms and business interests against the 'almighty', capricious, and all-too-demanding monarch. The establishment of ownership rights emancipated the rising middle class and made further economic development possible (Bovens 1998; Hoof & Ruysseveldt 1996). Certainly, it was no easy matter to wrest these rights from the king. A striking example is given by the way legitimacy was found for the Dutch revolt as being a defence against the King of Spain's violation of city rights and privileges. It took the Eighty Years' War to enforce recognition of the fact that those rights had been violated. In England, this conflict found expression in a struggle lasting decades between the King and the House of Commons, with the latter gradually succeeding in depriving the King of his privileges. In France, it took until almost the end of the eighteenth century before the monarchy was violently ousted.

7.4.3 Introduction of the registry of births, marriages and deaths and the population register

In the nineteenth century too, we can discover both the emancipatory and control aspects of identification and registration. In the extensive empire of Napoleon, centralised administration and uniform legislation were indispensable in order to govern. This required information regarding the size and structure of the population, which made it easier to enforce compulsory military service and to make the levying of taxes more efficient. In 1811, Napoleon introduced the register of births, marriages and deaths for most of the Netherlands, with the church's records of these events being transferred to the government (Holthuizen-Seegers & Wens 1993).

The droit citoyen was introduced along with the register of births, marriages, and deaths. This development was extremely important for the emancipation of the citizen, giving people equal status before the law and vis-à-vis one another. Free individuals were recognised as such. In France and the Netherlands, this meant, for example, that the Jewish community could integrate into and participate in society (Caplan & Torpey 2001). Registration meant that political rights such as the right to vote and to demonstrate could be exercised. The democratic layer of the constitutional state was formed (Bovens 1998).

The nineteenth century saw the start of the present Municipal Personal Records Database. In 1815, a constitutional monarchy was proclaimed and the Kingdom of the Netherlands came into being. In 1828, the municipal register became a state matter, replacing the ten-yearly censuses. Initially, pre-bound registers were used; in other words, entries were written in ink in a volume that was already bound. Later, the system switched to loose-leaf family cards. The advantages of a loose-leaf system were that it was easier to read and that it was possible to produce the original and a duplicate simultaneously using carbon paper. In 1938, it was decided that each municipality should set up a system with a separate card for each individual. The card gave the personal details of the person concerned – surname and forename, nationality, date and place of birth, position within the family, occupation, and changes of address – and often also the names and details of the parents and children (Centraal bureau voor genealogie 2009).

7.4.4 Extremes of emancipation and control

The twentieth century saw various extremes in the tension between control and emancipation. On the one hand, there were the horrors of the Nazi regime and on the other the development of the welfare state. Memories are still fresh of the far-reaching assistance that the Dutch municipal registers and identification obligation gave to the German occupiers during the Second World War in tracking down people who went underground, members of the resistance, and Jews. It became all too clear during the War that recording identity details can have perverse consequences.

By contrast, the emancipatory aspect finds powerful expression in the welfare state. This took shape in the form of basic social rights such as the right to social security benefits, education, and a pension. The growth in the range of tasks of government also led to an explosive increase in the number of registrations. Expansion of the education system, for example, required registers of children subject to the compulsory education obligation; the healthcare system required an overview of employees with health insurance; and the pension system required a similar overview of those entitled to a pension. Data was also collected for the purpose of administering social security benefits, various one-off benefit payments, and housing benefits (Holthuizen-Seegers & Wens 1993).

However, the welfare state also featured control – in fact to a far-reaching extent. In striving to serve every citizen effectively, it was necessary to construct large-scale personal records databases. That process involved a risk of over-bureaucratisation, with 'clients' becoming nothing more than a file number. That risk had already been foreseen by Weber, who believed that in the modern world the freedom of the individual was under threat from a suffocating bureaucracy, with people becoming imprisoned in an 'iron cage'.

7.4.5 The advent of the computer

The development of the welfare state produced an explosive growth in the use of personal data. This was compounded by the increasing use of computers, which greatly facilitated the work of the civil servants tasked with registering personal details. By the end of the 1970s, a large number of Dutch municipalities had computerised their register. However, updating of the various files within the municipality continued to be carried out separately. In 1984, the State Secretary for Internal Affairs announced a new approach to the system of municipal registers, namely the Municipal Personal Records Database, which by 1994 had become reality. The age of the computer and the introduction of the latter meant that personal details could be processed, altered, added to, consulted, and applied more efficiently and effectively.

7.5 Current developments: ongoing computerisation

Modernisation of the Municipal Personal Records Database and more recently the introduction of the Citizen Service Number and the Digital Identity system have shaped today's e-government. The modernised Municipal Personal Records Database is intended to enable the authorities to operate and cooperate more efficiently, and to improve their service delivery (www.bzk.nl). The necessary electronic communication between the various government bodies themselves and with the citizen is being effectuated on an ever-increasing scale.

The focus is primarily on the technical perfection and more efficient structure of government. Prins and Ham (2008, p. 10) argue that the pursuit of efficiency has become dominant: 'We are now striving solely for efficiency, we perform

our duties in an entirely standardised manner, and technological methods have become goals in themselves' [our translation]. The possibilities opened up by ICT have served only to reinforce this pursuit of efficiency. The onward march of computerisation also has a major impact on the quantity of data collected. Initially, data was recorded primarily in order to facilitate the implementation of the increasing volume of legislation and regulations. In their study, Schermer and Wagemans (2009) state, however, that personal details are currently recorded for virtually all of the processes and actions within our information society.

Computerisation also reinforces the control dimension, whereby the equilibrium between government and citizen threatens to be disrupted. Zuurmond (1994) argues that the 'iron cage' of classical bureaucracy is increasingly being replaced by a 'virtual fortress'. Electronic databases have become not only more comprehensive but also less flexible than the old-fashioned card index. The computer has taken up a position between the civil servant and the citizen, and leaves even less scope for personal interaction and for 'exceptional' cases.

Computerisation makes the registering of data simpler and at the same time more normal, meaning that more data is being recorded than ever before. In the period from 1998 to 2000 alone, the number of databases held by Dutch public authorities and quasi-governmental organisations increased ten-fold, from about 3,500 to 30,000 (Schermer & Wagemans 2009). As we have seen, the Municipal Personal Records Database alone is already used by hundreds of different organisations, and files held by a given body are increasingly linked via reference indexes and access facilities such as Suwinet and the electronic child record. The authorities are consequently obtaining an increasingly detailed picture of the citizen. From the perspective of the authorities, the citizen is in fact becoming increasingly transparent.

7.6 Dynamics of the personal records database

As we saw in the previous section, recording identities has come to be part of an apparently unquestioned and automatic administrative routine. For many people, their initial contact with an authority involves – as the first formal action – the entering of their name and address details, either on the spot into a registration system or after being called up from the existing system. It has become a matter of course for the citizen to be requested to have his or her 'client number' or Citizen Service Number ready when he or she wishes to utilise a service provided by the authorities. However, that 'matter of course' is not without its consequences.

We have argued above that registering individuals has an impact on the relationship – i.e. the power relationship – between government and citizen. According to Caplan & Torbey (2001), identification is a primary source of interaction and communication between them. This can serve not only control

purposes – for example levying taxes – but also protect the citizen against arbitrariness on the part of those wielding power. Registers of personal details are also one of the foundations of the development of our democratic state subject to the rule of law and the exercise of classic political and social rights. Such registers are therefore not merely a paper or electronic matter but are pre-eminently a political matter. Viewed in that light, the Municipal Personal Records Database can also be seen as part of the modern constitutional state, in which the power of the government is regulated and limited. After all, the database records not only taxpayers but also voters and those entitled to receive social security benefits.

We have also seen that in the course of the twentieth century advancing computerisation has radically changed the way registers are used. It is striking that this 'modernisation' is seen mainly as a technical matter, focusing on improving efficiency and effectiveness. This one-sided focus on efficiency threatens to tip the balance between emancipation and control towards the latter. Caplan and Torpey (2001) describe the continuous tension between control and emancipation as a game of cat and mouse between the State and the citizen. Their provisional conclusion is that even if the result of that game is never entirely clear in advance, it is so far the cat – i.e. the State – that has the advantage (Caplan & Torpey 2001, p. 7). The balance in the relationship between state and citizen threatens to be disturbed by an excess of bureaucratisation and control-oriented thinking, which leads above all to new dependencies on the part of the citizen. That danger is only reinforced by continuing to implement the modernisation of registers such as the Municipal Personal Records Database solely in terms of efficiency and technology rather than also recognising the importance and possibilities that modernisation offers for emancipation.

7.7 Conclusions: in search of an equilibrium?

For the current discussion, it is important to continue to emphasise the emancipatory aspect of registers and to develop sufficient guarantees for a new equilibrium between government and the citizen. This raises the question of how one can reinforce the position of the citizen vis-à-vis the State. The State's still increasing information superiority over the citizen demands a new system of checks and balances. We consider the protection of privacy to be an important component of those checks and balances, although it is primarily of a defensive nature. It fails to do sufficient justice to the emancipatory potential that has always characterised civil registers. Our intention is specifically to focus attention on the possibilities that modernising registers opens up for the further emancipation of the citizen. To conclude, we wish to mention a number of 'opening moves' within this discussion. For that matter, we make no pretension at this stage to conjure up a 'winning variant' onto the chessboard. In our recommendations, management by the citizen of his or her own personal details is central.

Management in this context means – to put it briefly – that the citizen gains insight into the way the State is processing his or her personal details and can influence this. Management by the citizen goes further than merely being shown what data is collected and processed, and compliance with the statutory obligations regarding the provision of information. In fact – and above all – it involves a certain level of control by the citizen of his or her data and the ability to influence how that data is processed – data that forms the basis for decisions taken by others (i.e. the State) that may have an impact on his or her life (N2L/Zenc 2002).

Insight into how one's data is processed depends above all on the transparency of that processing and the knowledge that the citizen has of the fact that processing is taking place. Openness and transparency are also important preconditions for management of his or her personal data by the citizen. To a large extent, this involves the obligations and associated rights for the individual involved that are enshrined in the Dutch Data Protection Act, for example the right to inspect and correct one's data. Often, however, the right to inspect and correct is not an 'active' right. In general, the citizen is not in a position to inspect the data immediately but must submit a written request. The www.mijnoverheid.nl website is an exception, while it enables the citizen to inspect certain data that the government has collected on him or her. For the time being, this involves data held in the Municipal Personal Records Database and the Digital Client Dossier and by the Road Transport Agency, and the Land Registry. In addition to this, the authorities could add an annex to each decision, giving the data for the applicant on which that decision is based. This would be an expression of active openness and would give the applicant the possibility of checking whether the authorities had perhaps made use of incorrect data. It would prevent the citizen needing to undertake a virtually hopeless Odyssey through officialdom in order to have his or her personal situation corrected.

However, achieving an equilibrium between state and citizen requires above all that the latter has a greater influence on the processing of data that matter to him. The Data Protection Act does not offer any options for this; the citizen cannot, after all, alter his details himself. Where the Municipal Personal Records Database is concerned, www.mijnoverheid.nl should offer the citizen more options for altering certain data, for example whether a woman wishes to be addressed by her maiden name. Another possibility is to enable citizens to request income support facilities on the basis of their own personal details.

Our intention in giving these examples is to show that the registration of personal details does not necessarily need to be aimed solely at increased efficiency. Registers can also be constructed in such a way that it is easier for the citizen to make changes to his or her details or to qualify for certain rights. Files can be linked to one another, thus clarifying, for example, whether or not someone is making use of income support facilities. Both the State

and the citizen can benefit from this. It is therefore precisely the developments in ICT that offer excellent opportunities for strengthening the position of the citizen. The rights and obligations dealt with in the previous sections can therefore also be supplemented by information rights for the citizen and information obligations for the State (see also Bovens 1998). With the aid of ICT, new checks and balances can be added, meaning that the mouse is no longer entirely at the mercy of the cat.

Bibliography

Databases on display: lessons from Dutch experiences

Algemene Rekenkamer (2007). *Lessen uit ICT-projecten bij de overheid. Deel A.* [z.p.]

Automatisering Gids (2010). 'Plan elektronische overheid dreigt faliekant te mislukken'. 12 February 2010.

BB Digitaal Bestuur (2010). 'De zeven gevaren van datahonger'. March 2010.

Commissie-Brouwer (2009), *Gewoon doen, beschermen van veiligheid en persoonlijke levenssfeer.* The Hague: Dutch Government.

Considerati (2009). *Onze digitale schaduw. Een verkennend onderzoek naar het aantal databases waarin de gemiddelde Nederlander geregistreerd staat.* Amsterdam: Considerati.

Senate (2009-2010a). *Verslag van een rondetafelgesprek.* Vergaderjaar 2009-2010, 31 466, F.

Senate (2009-2010b). *Verslag van de expertbijeenkomst over het elektronisch patiëntendossier van de vaste commissie voor Volksgezondheid, Welzijn en Sport/ Jeugd en Gezin van de Eerste Kamer op woensdag 9 december 2009.* Vergaderjaar 2009-2010, 31 466, E.

Hildebrandt, M. & S. Gutwirth (eds.) (2008). *Profiling the European Citizen. Cross-Disciplinary Perspectives.* Dordrecht: Springer.

Hof, C. van 't, R. van Est & F. Daemen (eds.) (2011). *Check in/Check out. The Public Space as an Internet of Things.* Rotterdam: Rathenau Instituut/NAi Publishers.

Leenes, R. (2010). *Harde lessen. Apologie van technologie als reguleringsinstrument.* Tilburg: Tilburg University.

Munnichs, G. (2009). Startnotitie *Expertmeeting elektronisch patiëntendossier (EPD).* The Hague: Eerste Kamer der Staten-Generaal/ Rathenau Instituut.

Nationale ombudsman (2009). *De burger in de ketens. Verslag van de Nationale ombudsman over 2008.* The Hague: Nationale ombudsman.

NRC Handelsblad (2007). *'Stad zegt of u seksuele voorlichting moet geven'.* 1 November 2007.

Vedder, A. et al. (2007). *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw.* The Hague: Rathenau Instituut.

www.iederkindwint.nl. http://www.iederkindwint.nl/#pagina=1006.

The public transport chip card and the kilometre charge: an electronic ankle tag for travellers?

Bakker, J. (2011) *'Alle OV-chipdata wordt eerder vernietigd'.* Webwereld, http://webwereld.nl/nieuws/107445/alle-ov-chipdata-wordt-eerder-vernietigd.html

Brands, S. (2000). *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy.* Cambridge, Massachusetts: MIT.

Camenisch, J. & A. Lysyanskaya (2002). 'A Signature Scheme for Efficient Protocols'. In:Conference proceedings *Security in Communication Networks*, pp. 268-289.

College bescherming persoonsgegevens (2008). *Brief aan Staatsecretaris van Verkeer en Waterstaat Mevrouw J.C. Huizinga-Heringa (kenmerk z2008-01411).* 6 November 2008.

Jonge, W. de & B. Jacobs (2008). 'Privacy-friendly Electronic Traffic Pricing via Commits'. In: Conference proceedings *Formal Aspects in Security and Trust*, pp. 143-161.

Hof, C. van 't, R. van Est & S. Kolman (2011). 'Networked Cars'. In: Hof, C. van 't, R. van Est & F. Daemen (eds.) (2011). *Check in/Check out. The* Public Space as an Internet of Things. Rotterdam: Rathenau Instituut/NAi Publishers, pp. 135-167.

Winter, B. de (2008). '7 jaar centrale opslag OV-reisgegevens niet nodig'. In: *Webwereld.nl*, 17 November 2008.

The electronic patient record from the perspective of data protection

Noordende, G. van 't (2010). *A Security Analysis of the Dutch Electronic Patient Record System.* Technical Report UVA-SNE-2010-01. Amsterdam: University of Amsterdam.

NOVA (2008). Elektronisch patiëntendossier part 1.12 November 2008 (http://www.youtube.com/watch?v= ahkcA1PH7Mw).

Spaink, K. (2005). *Medische geheimen. De risico's van het elektronisch patiëntendossier.* Amsterdam:Nijgh& Van Ditmar.

The electronic child record: opportunities and issues

Nationale ombudsman (2009). *De burger in de ketens. Verslag van de Nationale ombudsman over 2008.* The Hague: Nationale ombudsman.

Customer profiles: the invisible hand of the Internet

Agre, P.E. & M. Rotenberg (eds.) (2001). *Technology and privacy: The new landscape.* Cambridge, Massachusetts: MIT.

Ayres, I. (2007). *Super crunchers: why thinking-by-numbers is the new way to be smart.* New York: Bantam Books.

Borking, J.J. & Ch.D. Raab (2001). 'Laws, PETs and Other Technologies for Privacy Protection'. In: *Journal of Information, Law and Technology,* 2001 (1).

Custers, B. (2004). *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology. Nijmegen:* Wolf Legal Publishers.

Dijk, N. van (2009). 'Intellectual Rights as Obstacles for Transparency in Data Protection'. In: Deuker, A. (ed.), *Mobile Marketing in the Perspective of Identity, Privacy and Transparency.* FIDIS deliverable. 11 December 2009.

Dijk, N. van (2010). 'Auteursrecht in Profielen'. In: *Computerrecht*, Issue 2, pp. 53-61.

Dolinar, K. et al. (2009). 'Design Patterns for a Systemic Privacy Protection'. In: *IARIA International Journal of Advances in Security*, no. 2, pp. 267-287.

Hildebrandt, M. & S. Gutwirth (eds.) (2008). *Profiling the European Citizen. Cross-disciplinary Perspectives.* Dordrecht: Springer.

Hildebrandt, M. & B.J. Koops (2010). 'The challenges of Ambient Law and legal protection in the profiling era'. In: *Modern Law Review*, 73(3), pp. 428-460.

Jernigan, C. & B.F.T. Mistree (2009). 'Gaydar: Facebook friendships expose sexual orientation'. In: *First Monday*, 14(10).

Pariser, E. (2011). T*he Filter Bubble. What The Internet Is Hiding From You*. Penguin Viking.

Stone, B. (2010). 'Sure, It's Big, but is that Bad? Google'. In: *New York Times*, 21 May 2010.

The Economist (2010). *'Data, data everywhere. A special report on managing information'*, 27 February 2010.

Zarsky, T.Z. (2002-2003). '"Mine Your Own Business!": Making the Case for the Implications of the Data Mining or Personal Information in the Forum of Public Opinion'. In: *Yale Journal of Law & Technology*, 5(4), pp. 17-47.

http://www.zdnet.com/blog/facebook/facebook-releasing-your-personal-data-reveals-our-trade-secrets/4552

http://www.zdnet.com/blog/facebook/europe-versus-facebook-the-law-protects-program-logic-not-data/4608?tag=content;siu-container

The downside of the Schengen Information System

Brouwer, E. (2008). *Digital Borders and Real Rights. Effective Remedies for Third-Country Nationals in the Schengen Information System.* Leiden/Boston: Martinus Nijhoff.

College bescherming persoonsgegevens (2008). *Brief aan Minister van Justitie. Afronding onderzoek artikel 99 SUO*. 20 March 2008.

Computable (2009). 'Vertraging SIS II kost ministerie miljoen extra'. 22 januari 2009 (http://www.computable.nl/artikel/ict_topics/overheid/2843704/1277202/vertraging-sis-ii-kost-ministerie-miljoen-extra.html).

Council of the European Union (2009). *Report on the further direction of SIS II*. Doc. no. 10005/09, 20-05-2009.

European Data Protection Supervisor (2010). 'Opinions'. In: *Official Journal of the European Union*,C 70. 19 March 2010.

European Parliament (2003). Report with a proposal for a European Parliament recommendation to the Council on the second-generation Schengen Information System (SIS II). A5-0398/2003.

House of Lords European Union Committee (2007). *9th Report of Session 2006-07. Schengen Information System II (SIS II). Report with Evidence*. HL Paper 49. London: The Stationary Office Limited.

House of Representatives (1996-1997a). *Rapport Nationaal Schengen Informatie Systeem*. Vergaderjaar 1996-1997, 25 200, nos. 1-2.

House of Representatives (1996-1997b). V*erslag van een Algemeen Overleg*. Vergaderjaar 1996-1997, 25 200, no. 6.

Joint Supervisory *Authority of Schengen (2005). Article 96 Inspection. Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 96 alerts in the Schengen Information System*. 20 June 2005.

Joint Supervisory Authority of Schengen (2007). *Article 99 Inspection. Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 99 alerts in the Schengen Information System*. 18 December 2007.

Joint Supervisory Authority of Schengen (2009a). *Article 97 Inspection. Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 97 alerts in the Schengen Information System*. 13 October 2009.

Joint Supervisory Authority of Schengen (2009b). *Article 98 Inspection. Report of the Schengen Joint Supervisory Authority on an inspection of the use of Article 98 alerts in the Schengen Information System*. 13 October 2009.

Nationale ombudsman (2010). *Toegang verboden. Onderzoek naar de opname van vreemdelingen in het Schengen Informatie Systeem en de informatievoorziening hierover.* Rapportnummer 2010/115. The Hague: Nationale ombudsman.

Dynamics of the Municipal Personal Records Database

Bovens, M.A.P. (1998). *De digitale rechtsstaat, beschouwingen over informatiemaatschappij en rechtsstaat.* Utrecht: Utrecht University

Caplan, J. & J. Torpey. (2001). *Documenting individual identity. The development of state practices in the modern world.* Princeton: Princeton University Press.

Centraal bureau voor genealogie (2009). Persoonskaarten en persoonslijsten (http://www.cbg.nl/download/cbg_nl_persoonskaarten_200901.pdf).

Holthuizen-Seegers, G.H.J. & M.C.C. Wens (1993). *Persoonlijk gegeven, grepen uit de geschiedenis van bevolkingsregistratie in Nederland.* Amersfoort: Bekking.

Hoof, J. van & J. van Ruysseveldt (1996). *Sociologie en de moderne samenleving. Maatschappelijke veranderingen van de industriële revolutie tot in de 21ste eeuw.* Amsterdam: Boom.

Lütter, G. & R. van Troost (2008). *De dataloods en zijn machinekamer. Inleiding tot de GBA.* Deventer: Kluwer.

Net2Legal Consultants/Zenc (2002). *De betrokkene betrokken.* Onderzoek in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Directie Informatiebeleid Openbare Sector. [z.p.]

Prins, C. & M. Ham (2008). *In de greep van de technologie, Nieuwe toepassingen en het gedrag van de burger.* Amsterdam: Van Gennep.

Schermer, B.W. & T. Wagemans. (2009). *Onze digitale schaduw.* Amsterdam: Considerati.

Weber, M. (1978|1922). *Economy and society: an outline of interpretive sociology.* Berkeley: University of California Press. Translation of Weber, M. (1922). Wirtschaft und Gesellschaft.

www.bzk.nl. http://www.bzk.nl/actueel/nieuws--en/@117129/modernisering-gba.

Zuurmond, A. (1994). De infocratie, *Een theoretische en empirische heroriëntatie op Weber's ideaaltype in het informatietijdperk.* The Hague: Phaedrus.

Background to this study

This study makes use of six case studies concerning the utilisation of databases. The following topics were selected:

- the public transport chip card and the kilometre charge;
- the electronic patient record;
- the electronic child record;
- customer profiles on the Internet;
- the Schengen Information System;
- Municipal Personal Records Database.

In selecting these topics, consideration was given to a spread across a number of different fields and a mix of public and private databases, with attention also being paid to the use of databases within the EU. The selection was also partly determined by the background interviews held with ten experts at the start of the project (for their names, see Appendix 1). The selection naturally remains to a certain extent arbitrary. We might also have selected case studies regarding the 'smart' energy meter, the central storage of biometric passport details, the National Debt Information System, the Electronic Education Record, or the tremendous growth of social networking sites such as Hyves or Facebook – to mention just a few other examples. The variety of subjects involved already indicates how widely use is made of digitised data files.

The cases have been described without applying too strict a framework. Instead, we utilised a list of points for consideration as a guideline for the authors (for the instructions to the authors, see Appendix 2). Each case has its own special features and casts a somewhat different light on the way databases function.

In the essay 'Databases on display', the editors Munnichs, Besters, and Schuijff present the main outcomes of the case studies. In doing so, they have made use of the results generated by a meeting of experts at the Rathenau Instituut on 19 March 2010 at which earlier versions of the case studies were discussed (for a list of participants at the meeting, see Appendix 3). Responsibility for the content of the essay rests of course entirely with the authors.

About the authors

Michiel Besters
Michiel Besters graduated in philosophy at Tilburg University. Since October 2010 he has been working towards his doctorate in the philosophy of law at the university's Faculty of Humanities. In his dissertation, he is developing a political concept of security, applying this within the context of the European Area of Freedom, Security and Justice. From September 2008 to October 2010, he was a researcher at the Rathenau Instituut, working on projects in the field of medical technology and security technology.

Ellen Boschker
Ellen Boschker's field is public administration. She graduated cum laude from Radboud University Nijmegen, specialising in good governance. Given that background, she has a long-term interest in the relationship between citizen and State. As an adviser with Zenc, she promotes forceful administration and a strong society. Ellen Boschker is an expert on key registers.

Peter Castenmiller
Peter Castenmiller studied political science at the University of Amsterdam, receiving his doctorate in 2001 with a dissertation on the relationship between the citizen and local government. He is an expert in the field of the functioning of public administration. As an adviser with Zenc, he combines an understanding of the structure and functioning of public administration with a number of practical positions in the public domain. In addition to working at Zenc, Peter Castenmiller is an associate professor at the BAZN Academy of Administration, focusing on the topic of 'Administrative Strength and Innovation'.

Niels van Dijk
Niels van Dijk studied law in Amsterdam and philosophy in Amsterdam and Barcelona. He is currently engaged in doctoral research at Vrije Universiteit Brussel in the context of the research project on Law and Autonomic Computing. A mutual transformation process. His research focuses on the confrontation and interaction between new information technologies and law in the field of intellectual property rights and data protection.

Mireille Hildebrandt
Mireille Hildebrandt is Professor of Smart Environments, Data Protection and the Rule of Law at Radboud University Nijmegen's Institute for Computer and Information Sciences (ICIS). She is also a senior lecturer in the theory of law at Erasmus University Rotterdam and a senior researcher at the Centre for Law, Science Technology & Society (LSTS) at Vrije Universiteit Brussel. In the context of her work at LSTS, she coordinated the subproject on profiling technology within the European Commission's FP6 research programme on the Future of Identity in the Information Society (FIDIS) and, with Serge Gutwirth, edited Profiling the European Citizen. Cross-Disciplinary Perspectives (Springer 2008). With Antoinette Rouvroy, she edited Law, Human Agency and Autonomic Computing. The philosophy of law meets the philosophy of technology (Routledge 2011).

Simone van der Hof
Simone van der Hof is Professor of Law and the Information Society at Leiden University. Her research in recent years has concentrated on the ways in which citizens' digital identities are being used by the state for a variety of purposes – for example the provision of public services, policy-making, combating crime and fraud – and how this impacts relationships between citizens and government. She also studies consumers and online privacy (policies) as well as regulatory issues regarding the online risks to children and young people, such as cyberbullying and online grooming.

Bart Jacobs
Bart Jacobs is Professor of Computer Security at Radboud University Nijmegen. He graduated in mathematics and philosophy. His publications involve both theoretical research and practical work with direct relevance to society: electronic voting, biometric passports, the public transport chip card, and 'smart' electricity meters. He makes fairly regular appearances in the media to discuss these and other issues. Bart Jacobs is a member of the National Cyber Security Council.

Geert Munnichs
Geert Munnichs has worked at the Rathenau Instituut since 2002 as a senior researcher and, since 2010, as a department coordinator. In addition to the Databases on Display project, his work in recent years has concerned security and privacy, animal welfare, and nutrition and health. After studying environmental sciences, philosophy, and history at Wageningen University, he took his doctorate at Groningen University with a dissertation on Public Discontent and Public Credibility. Democratic Legitimacy in a Post-traditional Society [Publiek ongenoegen en politieke geloofwaardigheid. Democratische legitimiteit in een ontzuilde samenleving] (2000).

Mirjam Schuijff
Mirjam Schuijff is a researcher at the Technology Assessment department of the Rathenau Instituut. She studied philosophy and public administration in Nijmegen. Besides her research on the use of databases, she is investigating the use of technology for human enhancement and developments in the neurosciences.

Wouter Teepe
Until August 2009, Wouter Teepe was a researcher with the Digital Security group at the Radboud University Nijmegen, where he was one of those who revealed the cryptographic weaknesses in the Mifare Classic chip used in the Dutch public transport chip card. His contribution to this book is based on that background. Wouter Teepe studied artificial intelligence at Groningen University, where his doctorate involved a dissertation on the design and analysis of cryptographic solutions to a number of common privacy problems. He currently works at the Crypto & High Security business unit of Fox-IT in Delft.

Arre Zuurmond
Arre Zuurmond studied public administration at the University of Amsterdam. Since 1989, he has been researching the use of computerisation within public administration. In 1994, he was awarded his doctorate cum laude with a dissertation entitled The Infocracy [De Infocratie]. In 2000, Arre Zuurmond set up his own consultancy firm, Zenc, where he focuses on administrative innovations and the role of ICT. As a partner at Zenc, he advises ministries, provinces, and municipalities on organisational structuring and information provision.

Appendix 1: Background interviews

Sjaak Brinkkemper, Professor of Information and Software Systems, Utrecht University

Paul ´t Hoen, Chairman of the Advisory Board, ICT Regie

Bart Jacobs, Professor of Computer Security, Radboud University Nijmegen

Hadewych van Kempen, Senior Information Adviser, Ministry of the Interior and Kingdom Relations

Jacob Kohnstamm, Chair of the Dutch Data Protection Authority

Martijn Kriens, independent ICT consultant

Ronald Leenes, Scientific Director of TILT, Tilburg University

Johan Louwers, Oracle consultant, Capgemini Outsourcing

Corien Prins, Professor of Law and Informatisation, Tilburg University and member of the Scientific Council for Government Policy

Arre Zuurmond, Zenc and member of the board of the Rathenau Instituut

Appendix 2: Instructions to authors of case studies

The following guidelines are intended for authors of the case studies for the Databases on Display project. They are not intended to constitute a strict framework and the list is not exhaustive. Not every aspect is equally relevant to every case study. Emphases may also shift in the course of the work in the light of interaction between the project coordinators and the authors.

Key questions

The key questions for each case study are:
- What choices have been made as regards the architecture of databases?
- What consequences (intended and unintended) do those choices have?
- What alternative choices are possible?
- Do the consequences require the original objectives to be reconsidered?

Relevant aspects of case studies

Introduction
- What were the reasons for introducing the database/information system?
- What is the objective, i.e. what is the system intended to do?

Design
- What data is recorded?
- What processing, exchange, linking, and analysis of data takes place?
- How long is data retained?
- Which parties have access to the data?
- What are the arrangements for data security?
- What controls are there on the entry, quality, processing, access to, and deletion of data?

Operation in actual practice
- Is the system practicable from the point of view of the professionals involved?
- Does the system work effectively, i.e. does it actually contribute to achieving the objectives?
- What risks arise? These include such things as interpretation problems because data is taken out of context, false links, misinterpretation due to file corruption, or identity theft.

- What effect does the system have on the work of the professionals involved?
- Are the controls on the entry, quality, processing, access to, and deletion of data sufficient?

Position of the citizen
- What effect does the system have on the position of the citizen (as a customer, client, patient, etc.)?
- What provisions are there as regards the right to inspect and correct data? What control options are open to the citizen? Are these sufficient?
- Who can the citizen approach if something goes wrong?
- Does the citizen have an opt-out option?

Wider issues
- What effect does the system have on existing power relationships?
- Can the data be used for other purposes? Have these additional possibilities being taken into account when designing the system?
- Does profiling lead to 'social sorting' and to conventional, 'desirable' behaviour on the part of the citizen?

Alternatives
- What alternative design choices are possible? What are their consequences?
- What would happen if no database/information system were introduced?

The case study on the Municipal Personal Records Database was discussed in detail with the authors because it differs from the other cases.

Appendix 3: Participants at expert meeting Rathenau Instituut 19 March 2010

Michiel Besters, researcher at the Technology Assessment department, Rathenau Instituut

Guus Bronkhorst, head of the cluster for Information Policy for Key Government Facilities, Ministry of the Interior and Kingdom Relations

Frans Brom, head of the Technology Assessment department, Rathenau Instituut

Alex Commandeur, head of the Public Sector Supervision department, Dutch Data Protection Authority

Egbert Dommering, Professor of the Theory of Information Law, Institute for Information Law (IViR), University of Amsterdam

Bart Jacobs, Professor of Computer Security, Radboud University Nijmegen.

Ronald Leenes, Professor of Regulation by Technology, Tilburg University

Xander van der Linde, Burgerlink adviser, ICTU

Geert Munnichs, coordinator at the Technology Assessment department, Rathenau Instituut

Matt Poelmans, director of Burgerlink, ICTU

Who was Rathenau?
The Rathenau Instituut is named after Professor G.W. Rathenau (1911–1989), who was successively professor of experimental physics at the University of Amsterdam, director of the Philips Physics Laboratory in Eindhoven, and a member of the Scientific Advisory Council on Government Policy. He achieved national fame as chairman of the commission formed in 1978 to investigate the societal implications of micro-electronics. One of the commission's recommendations was that there should be ongoing and systematic monitoring of the societal significance of all technological advances. Rathenau's activities led to the foundation of the Netherlands Organization for Technology Assessment (NOTA) in 1986. On 2 June 1994, this organization was renamed 'the Rathenau Instituut'.

Does the electronic child record reduce the rate of child abuse? Does the Schengen Information System improve the way the external borders of the EU are guarded? And what do companies do with the personal data about customers that they collect on the Internet?

Computer systems are storing more and more information about us. Governments and businesses use that information to increase efficiency or improve communication. But do databases do what they are supposed to do? What about the security of all that information? How reliable is it? And how can people exercise control over information about them?

Based on six case studies, *Databases* comes to some disconcerting conclusions. The use of databases turns out to involve all kinds of risks that are often not given the attention they deserve. These risks are linked to the architecture – or design – of databases. As a result, the promises of ICT are at risk of turning into threats. The study shows that other design choices are possible that give a more important role to the position of the patient, citizen, or consumer about whom data is collected.

ISBN 978-90-77364-41-3