

SUMMARY

Privacy Law is Code.

About the deployment of privacy enhancing technologies

John Borking

© 2010 J.J.F.M.Borking

The title of the book is inspired by Lessig's adage: 'Code is Law'. This dissertation deals with two issues. On the one hand it explores whether information systems that safeguard privacy can be used preventatively on the other hand it investigates whether privacy-enhancing technologies (PET) can be implemented in information systems. In eight chapters I have tried to find an answer to the following problem definition: *how can personal information of citizens in information systems be protected that effectively, that people can (continue to) be assured (trust) that their personal data are not collected, processed, stored and circulated unlawfully by the party responsible (the controller) and the processor, both in the sense of the European Union Directive 95/46.*

Within the context of the problem definition this dissertation discusses six research questions, which have been enumerated in chapter 1, that will produce the answer to the problem definition. The first research question deals with the legal requirements of the Directive 95/46/EC; Research question 2 deals with the negative effect of the surveillance state on privacy; The third research question investigates the privacy threats; The fourth research question explores the concept of privacy enhancing technologies (PET); Research question 5 investigates the possibilities for constructing information systems which are privacy safe and research question 6 deals with the adoption obstacles for the deployment of PET.

Chapter 1

The analysis of today's environment provokes the first research question. It shows that in post-industrial countries such as the United States, Canada, Australia, Japan and the member states of the European Union, information and communication systems are used which collect, store, exchange, (re) use, identify, analyze and monitor data of persons in an increasingly sophisticated manner.

From the environment analysis in this chapter it also becomes clear that citizens (e.g. inhabitants, patients, hotel guests, passengers, students, buyers on the internet etc.) fear that the authorities, the business world and other organizations are misusing their personal data. This concern is fostered by the existence of a growing number of information systems that can be linked to data bases via internet or other networks and can automatically and freely exchange (personal) data. The more personal data that is available, the greater the risk of identity theft by malicious persons who appropriate and misuse personal data of citizens without their permission.

Citizens and consumers are not in a position to check what is happening to their personal data and to whom they are being distributed. It goes without saying that they want to have control over and keep check on the use of their personal details. However, in actual practice it proves to be very difficult for citizens and consumers to assert their rights in the field of the protection of personal data. Intrusive technologies increasingly put pressure on the personal domain (an invisible sphere surrounding

each human being and that becomes perceptible when other people are trespassing) and the informational privacy. Without technical resources, this situation will deteriorate sharply in the coming ambient intelligence (AMI) environment. AMIs are electronic environments, which are sensitive and receptive to the presence of people.

Chapter 2

The law protects our individual privacy and our personal data. This chapter explores the terms 'privacy', 'personal domain', 'identity' and 'personal data'. Subsequently, the general fundamentals with respect to personal data that form the basis of privacy protection are mapped out. These general fundamentals are worked out in the privacy realization principles, laid down in Convention 108 of the Council of Europe, the OECD directives and in the EU Directives 95/46 and 2002/58 and which have been explained in this chapter. In this respect the views of the 'Article 29 working Party' and a number of relevant rulings of the European Court for Human Rights and the European Court of Justice are also considered. The privacy realization principles (the starting points for effectuating privacy protection that are discussed in chapter 2) have direct consequences for the development and technical specifications of information systems. This for example concerns the principles of data minimization, purpose binding and transparency (the supply of information and access rights) and data protection. As a result of the first research question seven legal requirements for privacy safe information systems have listed. Chapter 2 points out that the EU data retention directive 2006/24 has consequences for the protection of privacy. It puts a number of critical comments with respect to the EU privacy directives.

Chapter 3

Before going into the privacy threats in the field of the information systems, this chapter examines the risk-monitoring society that has resulted in an increase in privacy violations. Also it elucidates a number of social developments, which seem to be conducive to the erosion of privacy. Particular attention is paid to various surveillance (criminal investigation) technologies such as data warehousing, data mining, video cameras, biometrics and localization (e.g. via cell phones). The authorities and trade and industry employ these technologies in order to offer services but also to combat terrorism, crime and fraud. Are '9/11', the directive 2006/24/EC or any legislation derived from this directive responsible for the crumbling of our privacy? The answer to that question of 'guilt' is negative. Chapter 3 argues that the deeper cause for the anti-terrorism legislation does not directly lie in the attacks carried out all over the world during the past six years but in the gradual development of our network society. That society has increasingly put the emphasis on risk analysis. In order to guarantee collective security in society as much as possible, a form of surveillance has emerged which is supported by ICT. Panoptic technology will increasingly be used to monitor people. Because the sensors (RFIDs) surrounding us are getting smaller all the time, surveillance by the authorities and the business world will become more and more imperceptible (particularly in AMI environments) for individuals. It remains to be seen to what extent individuals and groups in such a surveillance society can make their own decisions as regards the level of exposure to surveillance and to what extent they can limit the personal data that is collected and used. To a layman surveillance systems are often too technical to be understood. They invisibly and as a result imperceptibly merge into the day-to-day structures and systems of society: at the workplace, at home, at school, whilst travelling and whilst using telecommunication. The risk surveillance society creates social sorting and

information apartheid. Special offers with discounts for example are not given to people from underprivileged areas because people living there have no purchasing power or they are considered poor credit risks. The second research question results in the conclusion that in our surveillance society our privacy is at risk if the surveillance is executed with non-privacy protective information systems.

Chapter 4

This chapter stresses the point that in order to be allowed to process personal data and to be able to build privacy protection into information systems, it will be necessary to carry out a privacy risk, impact or threat analysis. In doing so, not only an assessment from a security technical point should be made but legal issues should also be considered. From article 17 of EU directive 95/46 it cannot be concluded otherwise that privacy risk analysis or treat analysis *ex ante* is a *sine qua non*. However, organizations widely ignore this statutory requirement as if this obligation would not exist. An investigation conducted by KPMG in 2004 shows that 95 percent of all Dutch organizations is acting contrary to the Personal Data Protection Act (Wbp) in the processing of personal data and that privacy is violated on a large scale.

Privacy risk analyses and threat analyses bring to light the dangers in the collection, exchange and circulation of personal data for the individual person and the data processing organizations. The European privacy directives and the national legislation of the EU member states engrafted onto those directives set out a standard of protection of personal data that ensures that those risks will be covered. Chapter 4 considers the third research question and raises seven risk analysis and risk management methods, such as i.e. the method of the 'Registration Chamber' (presently Dutch Data Protection Authority: 'College Bescherming Persoonsgegevens') to determine the risk class with respect to a specific form of processing of personal data. In addition it deals with the privacy impact analysis (PIA) developed by the Treasury Board of the Canadian authorities, the privacy threat analysis containing the pentagonal approach developed in the European PISA project and the privacy threat ontology, which was first applied in 2007 in the Norwegian PETWEB project. It is important to conduct a privacy risk or privacy threat analysis in which circumstances are taken into account as much as possible. Often security experts from actual practice list the potential privacy violations and the relative threats and risks. This is not considered preferable; an ontological specification of threats would be more suitable. From the privacy risk and threat analyses that have been investigated it becomes clear that personal data can best be protected if they have been anonymized or have been separated from other data. This means that the personal data are actually being processed but that the identifying personal data are immediately unlinked from the other personal data. The research question results in 14 generic privacy threats.

Chapter 5

This chapter explores the fourth research question dealing with the substance and implications of the privacy enhancing technologies concept (PET) and examines how PET can contribute to the protection of personal data in information systems. In addition it investigates the role reserved for the Identity Protector (IDP) and how privacy realization principles can be converted into a program code. In this chapter a number of important draft elements in combination with privacy enhancing technologies that can be used in the development of systems in which privacy is secured are discussed. The PET concept may theoretically be seen as a significant

complement to the existing legal framework and its implementation as far as organization is concerned. PET can ensure that organizations do not use personal data or minimize their use or process them in accordance with the statutory provisions. As a result the protection of privacy by the parties responsible does not become an empty shell. Moreover PET enables citizens and consumers to keep a check on the processing of their personal data that consequently increases their confidence in the lawful processing of data. Research discussed in this chapter shows that the privacy of citizens and consumers can be safeguarded in an increasingly effective manner. There is an ever-growing need to develop adequate technological means to protect the individual privacy. After all, in the near future more and more transactions will be carried out not only directly between people but also increasingly directly between information systems, software agents, intelligent sensors and robots. This chapter also discusses the tools to protect personal data, such as encryption, rule-based privacy management systems, data tracking, sticky policies and privacy ontologies.

Chapter 6

On the basis of a number of models, this chapter deals with information systems with enhanced privacy that has been realized successfully in different sectors of society. In this chapter four examples are worked out in which the design principles and techniques of chapter 5 have been applied. These four examples demonstrate that personal data of individuals can be protected properly technically without endangering the functionality of the information systems. The PET concept, as part of the data architecture, plays an important role in the protection of personal data. In order to protect the personal data of individuals effectively, PET needs to form part of the data architecture. This generally involves a fundamental revision of the architecture, especially as regards the internal relations of the components and the connections with the environment of the system. The integration of PET in newly to be developed systems is a realistic option. PET is most effective in the collection of personal data, because privacy will then be protected at source. The meta-search machine Ixquick, discussed in this chapter, demonstrates this. As shown by the example of the Veldwijk-Meerkanten hospital, with the use of PET, sensitive medical data (personal data) can be protected extremely well during processing and storage. More complex systems such as the National Trauma Information System (NTIS) and the Victim Tracking and Tracing System (ViTTS) could not exist without PET. PET can also be used effectively in the circulation of data because PET prevents the unlawful linking of data. The PISA project demonstrates that PET is able to adequately protect personal data in network environments despite the complexity to build in and uphold privacy legislation in systems.

Organizations as yet make little use of privacy management systems that force data to be processed in conformity with privacy rules. The Privacy Incorporated Software Agent (PISA) project is an advanced application in this respect and provides knowledge that may be used in an ambient intelligence environment. The answer to fifth research question whether privacy safe information systems can be built successfully, is affirmative.

Chapter 7

Here has been examined the sixth research question why privacy secured architectures is scarcely implemented and PET is hardly used. It analyses the organizational and economic impediments to the adoption of PET, among others on the basis of case studies. It becomes clear that organizations are influenced by a large number of

factors in their decision whether or not to implement PET. If the positive adoption factors would be utilized, organizations would be able to implement PET in their information systems much faster on a large scale. This particularly applies to organizations with large information intensity and which on account of their organization strategy have a great need to protect personal data and to be financially and operationally capable of doing so.

In order to implement PET, the organization needs to have a certain degree of maturity. The chapter deals with this issue in further detail. Whether PET can be applied within an organization depends on the maturity of said organization in the field of Identity & Access Management (IAM) and privacy protection. In chapter 7 the progress of these processes and the decision-taking moment to implement PET are outlined in three related S-curves. Business models to invest in PET do not exist. Investment in PET requires a positive business case demonstrating the financial feasibility of PET. For that reason a number of methods are discussed in this chapter to calculate the cost-effectiveness of investments including the Return On Investment method containing a specific investment formula for PET (ROI-PI) and the Net Present Value formula. Empirical information on privacy incidents in the European Union is not available, making it impossible to assess the consequences of such incidents properly and rendering the calculations on return inaccurate. A compulsory disclosure and recording of the loss or theft of personal data, as provided for in the proposed amendment of the EU- directive 2002/58, will ensure that this information will be available in the future.

Chapter 8

This study ends with a number of concluding observations and produces ten recommendations. This chapter returns to the investigation issues in chapter 1 and presents a number of recommendations based on the positive adoption factors for PET from chapter 7. In addition to the supply of information, the role of the Data Protection Authorities (DPAs) is of vital importance for the implementation of PET in information systems. The DPAs, such as the CBP (Data Protection Authority) in the Netherlands should not adopt an *ex post* attitude (handling complaints and carrying out checks afterwards) but actually adopt an *ex ante* attitude (rendering pre-emptive advice). They should be deploying their technological experts as PET consultants. On the basis of analyses of privacy risk, privacy threat or privacy impact (PIAs) they could assess whether the information systems to be implemented comply with privacy legislation and if necessary they could advise the use of PET. However, expertise on PET applications is scarce. For that reason it would be advisable for a PET expertise centre to be set up. In order to implement PET successfully in new information systems, the book recommends a specific PET step-by-step plan. The chapter concludes with proposals for a number of amendments of the EU directive 95/46 necessary for the improved protection of personal data. As a result citizens and consumers may become more confident that their personal data will be processed in accordance with their privacy preferences and the rules and regulations. The PET measures incorporated in information systems will enable them to protect themselves more effectively against privacy violations in the coming AMI world.

The research of today shows that we can build privacy safe information system (the *how* in the problem definition), but these systems need to be equipped with a certificate (privacy seal) declaring that the system warrants the privacy safe processing of personal data, and these systems have to be deployed on a large scale in society in order to generate the general *trust* of the citizens. However if there is the

lack of political imperative to protect our privacy adequately with PET and if we continue the use of privacy unsafe information systems in our risk-surveillance society, then great dangers for our privacy is at hand.