Chapter IV
Practical Privacy Assessments

Thejs Willem Jansen
Technical University of Denmark, Denmark

Søren Peen
Technical University of Denmark, Denmark

Christian Damsgaard Jensen
Technical University of Denmark, Denmark

ABSTRACT

Governments and large companies are increasingly relying on information technology to provide enhanced services to the citizens and customers and reduce their operational costs. This means that an increasing amount of information about ordinary citizens is collected in a growing number of databases. As the amount of collected information grows and the ability to correlate information from many different databases increases, the risk that some or all of this information is disclosed to unauthorised third parties grows as well. Although most people appear unaware or unconcerned about this risk, both governments and large companies have started to worry about the dangers of privacy violations on a major scale. In this chapter, we present a new method of assessing the privacy protection offered by a specific IT system. The operational privacy assessment model, presented here, is based on an evaluation of all the organisational, operational and technical factors that are relevant to the protection of personal data stored and managed in an IT system. The different factors are measured on a simple scale and the results presented in a simple graphical form, which makes it easy to compare two systems to each other or to identify the factors that benefit most from improved privacy enhancing technologies.A standardised assessment of the privacy protection offered by a particular IT system; serve to help system owners understand the privacy risks in their IT system as well as help individuals, whose data is being processed, to understand their personal privacy situation. This will facilitate the development and procurement of IT systems with acceptable privacy levels, but the simple standard assessment result may also provide the basis for a certification scheme, which may help raise the confidence in the IT system's ability to protect the privacy of the data stored and processed in the system.

INTRODUCTION

Existing research into privacy enhancing technology (PET) has provided few answers to many of the real questions that governments and large companies are facing when they try to protect the privacy of their citizens or customers. Most of the current work has focused on technical solutions to anonymous communications and pseudonymous interactions, but, in reality, the majority of privacy violations involve careless management of government it-systems, inadequate procedures or insecure data storage. In this chapter, we introduce a method that helps system developers and managers to assess the level of privacy protection offered by their system and to identify areas where privacy should be improved. The method has been developed in the context of government IT systems in Europe, which has relatively strict privacy legislation, but we believe that the method may also apply to other government systems, non-governmental organisations (NGOs) and large private companies. With the privatisation of many state monopolies, such as telecommunications and railroads, in many countries and the increasing number of public/private partnerships, the distinction between the public and private sector has grown increasingly fuzzy.[1] For the purpose of clarity in our discussions, however, we have decided to use the vocabulary from government systems, so we discuss the relationships between governments and citizens instead of companies and customers.

Governments are increasingly relying on information technology to provide enhanced services to the citizens and reduce the costs of the public sector. This means that an increasing amount of information about ordinary citizens is collected in an increasing number of government databases. As the amount of collected information grows and the ability to correlate information from many different databases increases, the risk that some or all of this information is disclosed to unauthorised third parties grows as well. Although most citizens appear unaware or unconcerned about this risk, governments have started to worry about the dangers of privacy violations on a major scale. If the government is not seen to be able to treat information about its citizens securely, these citizens will be reluctant to provide timely and accurate information to the government in the future. Many of the same factors are relevant in the relationship between companies and their customers, so both governments and large companies have realised that protecting the privacy of their citizens and customers is necessary if they are to reap the benefits of the information society in the future.

The benefits of collecting and storing information about citizens in electronic databases is an increasing level of efficiency in administrative systems and convenience for the citizens, because it provides government agencies with faster and easier access to relevant data and improves their ability to combine sets of personal data from different systems. This allows improved services at reduced costs, for example, the Inland Revenue Service in Denmark has reduced the number of employees from around 14,000 to around 9,000 in the past decade, while the amount of information that is being processed about each citizen has increased. The sheer volume of data collected by different government IT systems, however, makes it increasingly difficult for anyone to obtain an accurate picture of all the personal information that may be available in government databases. Moreover, it also makes it difficult to determine which persons, institutions or private companies that have access to the data.

There have been an increasing number of incidents, where personal information has been released to unauthorised third parties, either through carelessness or through negligent administrative procedures. Financial News reports that JPMorgan Chase recently lost a container with a backup tape that includes the account information and social security numbers of some 47,000 of their Chicago-area clients according to Financial