2009

Data Privacy

MBA Team Assignment - MBA 664

Sebastian Leinmueller
Birgit Hainzlmaier
4/13/2009

Table of Contents

1. Introduction

In a world where the possibility of collecting, storing and conciliation of large pools of data is widely available, data privacy becomes a critical issue. Identity theft, which is the use of personal information to illegally access existing financial accounts, open fraudulent accounts, or obtain credit cards in other people's names (Lee 2001), happened 258,427 times nationwide (Coakley 2009, 1). About 500,000 to 750,000 credit fraud cases are registered every year (Lee 2001). Obviously, it has become an easy task to abuse personally identifiable data or to trace a person due to installed public surveillance cameras, information provided by social networks, and credit card information. In response, many states developed legislative strategies to ensure a person the right of control over all data in connection with his or her identity. However, the extent of data privacy safeguarded by the state significantly varies among different counties.

The purpose of this work is to outline differences and similarities in the extent of data privacy in the United States and Europe. In the first chapter of this work, a brief section about the history of data privacy will lead to a comparison of data privacy regulations between the United States and Europe. After that, different types of technical tools and standards for protecting personally identifiable data are illustrated. Additionally, areas of concern are pointed out at the end of the first chapter. Consecutively, data privacy is examined and compared by means of two examples: the social network website Facebook and public surveillance cameras. Therefore, the second chapter takes Facebook into detailed consideration. It briefly outlines the technical environment that enables 200 million active users (Facebook 2009) to use Facebook's services and applications. Subsequently, it is described how the data are collected and who is authorized to access the data. Once being entered in the system, it is illustrated how those data are currently used or abused. The second chapter of this work concludes with potential risks and problems. After that, chapter three provides insight in the technical environment of public surveillance cameras. Furthermore, the collection by public surveillance cameras and authorization of data is taken into consideration. After that, chapter three concludes by an overview of how the data are used or abused and potential problems and risks are identified.