Chapter 4
The Right to Privacy and the Protection of Personal Data in a Digital Era and the Age of Information

William Bülow
Royal Institute of Technology, Sweden

Misse Wester
Royal Institute of Technology, Sweden

ABSTRACT

As information technology is becoming an integral part of modern society, there is a growing concern that too much data containing personal information is stored by different actors in society and that this could potentially be harmful for the individual. The aim of this contribution is to show how the extended use of ICT can affect the individual's right to privacy and how the public perceives risks to privacy. Three points are raised in this chapter: first, if privacy is important from a philosophical perspective, how is this demonstrated by empirical evidence? Do individuals trust the different actors that control their personal information, and is there a consensus that privacy can and should be compromised in order to reach another value? Second, if compromises in privacy are warranted by increased safety, is this increased security supported by empirical evidence? Third, the authors will argue that privacy can indeed be a means to increase the safety of citizens and that the moral burden of ensuring and protecting privacy is a matter for policy makers, not individuals. In conclusion, the authors suggest that more nuanced discussion on the concepts of privacy and safety should be acknowledged and the importance of privacy must be seen as an important objective in the development and structure of ICT uses.

DOI: 10.4018/978-1-4666-0891-7.ch004

INTRODUCTION

In our modern day society, more and more of our interactions with other parties, be it friends or official agencies, take electronic form. Sharing personal information by using social networking sites or declaring one's income taxes on-line is ever increasing and there are few signs that this development will decrease in the near future. The speed and relative ease of conducting on-line transactions has in many ways improved our lives by increasing availability of e-services, saving time and effort. However, the rapid increase of electronic transmission, storing and sharing of personal data is not without risk. There are numerous ways one's identity can be stolen, personal data abused or enclosed to unintended parties. In this context, the need for privacy is considered one of the main ethical issues in relation to developments and applications of Information and Communication Technologies (ICT) (see e.g. Johnson, 2004; Stamatelos, 2007). There is a growing concern that too much data containing personal information is stored by different actors in society and that this could potentially be harmful for the individual. Not only is information about individuals shared voluntarily in the above-mentioned examples, there has also been an increase of other technologies, such as RFID-tags and CCTV cameras in various context, including workplace and public spheres. In this context, information about our habits and whereabouts can be stored and shared without our active use of e.g. e-services. Information like this, collected by different sources can be combined and aggregated, making very detailed descriptions about individuals more easily created than before. When aggregating information it is possible to extract new information and knowledge about individuals that extend beyond the literal bounderies of the orginal purpose of gathering the information. Situations like this are sometimes refererd to as re-purposing, where the original purpose that the informaiton was collected for changes into something else without the expressed consent of the individual. One example of this can be the use of biometrical data, such as DNA, originally collected for medical purposes, in attempting to solve a crime. In situations where different types of information from a variety of related or unrelated sources is combined, privacy is often used as a value that can—and perhaps even should be—compromised if the end result of combining stored data is beneficial for society, such as, increased security for all law-abiding citizens. For example, imagine that a country has problems with hate crimes towards a minority ethnic group. It would be possible to monitor an individual that frequently visits websites for national extremism, to keep track on the credit card purshases for any suspicious transactions, track the persons movements by GPS or the use of so-called smart cards with RFID-tags used in public transportation and finally catch the person meeting with other suspicious individuals by using CCTV and, hopefully in the end, preventing another attack. Here, clearly it can be argued that the extended use of ICT can be beneficial to society at large. There are instances however, where this clear connection between increased surveillance and public safety is not visable, but sensitive personal data is instead combined and shared in ways that are not beneficial. For example, by checking out my Facebook statuses for the past years, in combnation with an investigation on my shopping habits can reveal that I only buy special kinds of food, combined with a scrutiny of the RFID tags on my library books show that I read books on clinical depression and taken together with a copy of my bank statements,that reveal that I have regularly made payments to a psychiatrist for the past two years as well as a divorce lawyer. This, in combination with my medical data relating to possible drugs I take and how many days I have been on sick-leave, can reveal more information about me than I would want to share with any person or potential employer. Often, as citizens, we are asked to trust the institutions or commercial agents that handle our personal data