Chapter 1
Privacy Enhancing Technologies for Information Control

Martin Gilje Jaatun
SINTEF ICT, Norway

Inger Anne Tøndel
SINTEF ICT, Norway

Karin Bernsmed
SINTEF ICT, Norway

Åsmund Ahlmann Nyre
SINTEF ICT, Norway

ABSTRACT

Privacy Enhancing Technologies (PETs) help to protect the personal information of users. This chapter will discuss challenges and opportunities of PETs in a business context, and present examples of currently available PETs. We will further study the Platform for Privacy Preferences (P3P), and discuss why it so far has failed to deliver on its promise. Finally, we provide our advice on further research on privacy preferences, and conclude with our conviction that businesses need to take a progressive stance on providing privacy to their customers.

INTRODUCTION

Privacy is a fuzzy concept with many definitions, one of which is "the right to be let alone" (Warren & Brandeis, 1890). This particular definition seems to have lost much of its validity, however, as we in modern society base so much of our existence on interaction with others over the internet. This is in particular true for us as consumers, as increasingly businesses assume that we will use the internet for both purchases and user support.

Privacy Enhancing Technologies (PETs) comprise a broad collection of tools and processes that help protect the privacy of end-users. PETs range from mechanisms that prevent disclosure of personal information, via ways of hiding location information, to methods for anonymous communication.

To the casual observer it might seem that most businesses have been more interested in privacy-

DOI: 10.4018/978-1-61350-501-4.ch001

invasive technologies than privacy-enhancing technologies, in that businesses have wanted to learn as much as possible about their (potential) customers, in order to deploy more targeted advertisements, sales projections and production planning. On the "dark side" of the business spectrum, this has led to the development of spyware that monitors individual computer users, but retailers have also looked into the possibility of exploiting RFID tags on merchandise to harvest information on their customers (CASPIAN, 2006).

To this day, most consumers seem oblivious to privacy concerns, and their behavior is usually not motivated by such concerns; to the contrary, most people seem overly free with their personal information, particularly in the context of online social networks such as Facebook (2011) and LinkedIn (2011). However, as advances in data mining techniques are progressing, the vast amounts of data available to businesses are bound to be recognized as a concern by consumers, and a backlash is imminent.

It has been said that online businesses instead of establishing a trust relationship with their customers, rather focus on avoiding *distrust* (Clarke, 2008), and that this is mainly achieved through how they treat the personal data of their customers – in many cases, the more personal data a business demands from a customer, the more the distrust increases. In this context, it would seem that organizations that facilitate the use of Privacy Enhancing Technologies in their interactions with their customers should have a business advantage. Many businesses tend to collect personal information about their customers as a matter of course, regardless of whether they actually need this information. This could potentially end up as a liability for a business, since in many jurisdictions, storing personal information requires informed consent, and forces the business to abide by privacy legislation.

The obligation to inform users of privacy practices is commonly resolved by using a comprehensive and high-level description of an organization's privacy policy (Guarda, 2009). In the digital world, privacy policies have become the main instrument for service providers to explain how users' personal data are collected, used, disclosed, and managed. Unfortunately, due to their complexity, difficult language and sheer length, users tend to neither read nor understand the policies prior to acceptance (Berendt, Günther, & Spiekermann, 2005). Vila et al. (2003) show that market forces are actually counter-productive to use of privacy policies when effort is required by users to verify a policy. This is an argument for more automated processes.

As the 20th century was drawing to a close, the Platform for Privacy Preferences (P3P) (W3C, 2006) emerged as an innovative privacy-enhancing concept, based on the transformation of textual privacy policies into machine-readable instructions for computers. A main motivation for the P3P project was to make it easier for users to understand privacy policies and make well-informed decisions on how to interact with services that collect personal data (Argyrakis, Gritzalis, & Kioulafas, 2003). Central to its vision was the privacy agents that allowed the user to specify what was acceptable and not, in terms of information sharing, and let the agent compare the user's privacy restrictions with the intentions of the web site that he was visiting. P3P is considered one of the most significant efforts to help web users control the sharing of their personal information. Later on in this chapter we will discuss its background, history and uptake, criticisms and technical obstacles, and explain the main reasons for its failure.

Strictly speaking, one may be reluctant to categorize approaches such as P3P as PETs, since they are more concerned with informing users about how their personal information will be (ab)used than actually protecting the users (often against themselves). It is important to consider P3P as a concept, however, as it primarily has relied on individual websites (i.e. businesses) for deployment, and the current verdict is that for the most part, this must be considered a dismal failure.