Chapter IX
Avoiding Pitfalls in Policy-Based Privacy Management

George O.M. Yee
NRC Institute for Information Technology, Canada

Larry Korba
NRC Institute for Information Technology, Canada

ABSTRACT

The growth of the Internet is increasing the deployment of e-services in such areas as e-commerce, e-learning, and e-health. In parallel, the providers and consumers of such services are realizing the need for privacy. The use of P3P privacy policies on Web sites is an example of this growing concern for privacy. Managing privacy using privacy policies is a promising approach. In this approach, an e-service provider and an e-service consumer each have separate privacy policies. Before an e-service is engaged, the provider’s policy must be “compatible” with the consumer’s policy. However, beyond compatibility, the policies may face pitfalls arising from improper specification, misapplication, and improper maintenance (e.g. failing to keep a personal privacy policy up-to-date). This can result in the lost of privacy and even lead to serious safety issues in certain cases. This chapter gives examples of how such pitfalls can arise and suggests ways to avoid these pitfalls.

1. INTRODUCTION

1.1 The Privacy Problem

The rapid development of the Internet has been accompanied by a growth in the number of e-services available to consumers. E-services, and in particular, web services, are available for banking, shopping, learning, healthcare, and Government Online. However, each of these services requires a consumer’s personal information in one form or another. This leads to concerns over privacy. Indeed, the public’s awareness of potential violations of privacy by online service providers has been
Avoiding Pitfalls in Policy-Based Privacy Management

growing. Evidence affirming this situation include a) the use of P3P privacy policies (P3P, 2002) by web server sites to disclose their treatment of users' private information, b) the enactment of privacy legislation and directives by major jurisdictions as a sort of owners’ “bill of rights” concerning their private information, and c) the appointment of privacy commissioners or officials who can assist the consumer in addressing violations of privacy (Canada has a federal privacy commissioner as well as provincial level privacy commissioners). In order for e-services to be successful, privacy must be protected. An effective and flexible way of protecting privacy is to manage it using privacy policies. The objectives of this chapter are a) to show that such use of privacy policies can lead to pitfalls and b) to propose ways to eliminate or mitigate these bad outcomes. This work is based on Yee & Korba (Oct. 2005).

1.2 Approaches for Solving the Privacy Problem

Various approaches have been used to protect personal information, including data anonymization (Iyengar, 2002; Kobsa & Schreck, 2003) and pseudonym technology (Song et al., 2006). Approaches for privacy protection that are in the research stage include treating privacy protection as an access problem and then bringing the tools of access control to bear for privacy control (Adams & Barbieri, 2006), treating privacy protection as a privacy rights management problem using the techniques of digital rights management (Kenny & Korba, 2002), and considering privacy protection as a privacy policy compliance problem, verifying compliance with secure logs (Yee & Korba, 2004). This work is concerned with the latter approach, i.e. the management of privacy using privacy policies. In this approach, the e-service provider and e-service consumer each has a privacy policy that stipulates how personal information is to be handled. The consumer’s policy states how the personal information about the consumer is to be handled by the provider, for example, what the information can be used for, how long the provider can retain the information in its possession, to which parties the information may be disclosed, and so on. The provider’s policy states how the provider will handle the consumer’s personal information, in terms of the same ways of handling information as in the consumer’s policy. Naturally, the e-service can only proceed if both policies agree with each other. Once this agreement is reached, privacy protection relies on the provider upholding the agreed upon privacy policy.

1.3 The Privacy Policy Pitfalls Problem

The use of privacy policies in privacy management can have pitfalls or unexpected negative outcomes. Pitfalls can arise from a) how the matching of policies between consumer and provider was carried out, b) improperly specified policy content, c) whether or not the consumer privacy policy was a good fit for the e-service, and d) whether or not the privacy policy was properly maintained or kept up-to-date. For example, a policy allowing a drug prescription to be given to a provider is unlikely to be a good fit if the provider’s service sells books instead of drugs. In such a scenario, a pitfall could arise if the provider inadvertently discloses the prescription to an individual who is not to receive such information according to the consumer’s wishes (e.g. a mother who the consumer would not wish to worry, if the prescription was for a serious illness).

1.4 Map to the Chapter

The rest of this chapter is organized as follows. Section 2 discusses recent privacy legislation, and further explains what we mean by e-services and privacy management, application, and maintenance. Section 3 explains privacy policies, including their specification, application, and