Chapter I

Exercising the Right of Privacy

Scott Flinn, National Research Council Canada, Canada

Scott Buffett, National Research Council Canada, Canada

Abstract

This chapter discusses privacy from the perspective of the consumer of e-services. It proposes a technique for risk management assessment designed to help consumers evaluate a situation to identify and understand potential privacy concerns. The technique centers around a series of questions based on common principles of privacy protection. The chapter discusses how a consumer can understand exposure risks and how information can be controlled and monitored to mitigate the risks. It also proposes a method for assessing the consumer’s value of personal information, and a mechanism for automated negotiation is presented to facilitate fair, private information exchange. The authors believe that these or similar techniques are essential to give consumers of e-services meaningful control over the personal information they release. This forward-looking chapter provides a foundation for developing methods to empower users with control over their private information.

Copyright © 2006, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.
Introduction

In a transaction or relationship in which there is an expectation of privacy, the roles of the parties involved are generally not symmetric. In the simplest case, one party (which we will call the sender) discloses information to another (the receiver). More generally, one or more senders will disclose information to one or more receivers. We also refer to senders as relying parties because they must rely on receivers to keep information in confidence. Widely recognized privacy principles (such as those of the CSA Model Code introduced in the next section) can be interpreted from both perspectives. For the receiver, they define a duty of confidentiality. For the sender, they define a right of privacy that is primarily concerned with the sender’s ability to exercise control over the exposure of sensitive information.

The privacy concerns relating to a direct relationship between parties are often spelled out in legal agreements or legislation. In these cases, it may be clear to relying parties what their exposure is and how to manage it. In many cases, however, relationships may be informal, indirect, or complex multi-party relationships. In these circumstances, the situation is much less clear for senders.

This chapter focuses on senders who must manage their exposure in these complex situations. It outlines a vision for privacy management from a sender’s perspective that has three major components. The ultimate objective is to assist senders in making good decisions regarding the trade-offs between the potential costs and benefits of disclosing sensitive information.

First, senders must be aware of the potential privacy risks they face as they conduct their business online. What are they? How likely are they? What are the associated costs? What incentives balance the risks? We discuss these and other questions, and introduce a decision process based on a risk management approach.

Second, senders must have the means to limit their exposure, obtaining benefits in proportion to the value of the information they reveal. We discuss the valuation of personal information from both the senders’ and receivers’ perspectives and describe in detail a protocol for negotiating equitable exchanges.

Third, senders should have some degree of direct control over their personal information following its release. We review the challenges this goal presents and discuss techniques to address it.

Each of these components has implications for the architecture and design of e-services, which we will highlight throughout the discussion.

This chapter is very much a forward-looking one. It is important to recognize that privacy is an ill-defined concept, meaning many different things to different people. In a recent article on the meaning of privacy, Daniel Solove put it this way: “Privacy is a concept in disarray. Nobody can articulate what it means” (Solove, 2006). The comment is especially relevant for this chapter with its focus on individuals who may each have their own conception of privacy. It is therefore unrealistic to expect to find turn-key technologies capable of ensuring end-user privacy today. In this regard, any potential solution is necessarily forward-looking. The proposals in this chapter are not yet widely deployed.