Chapter XI

Legislative Bases for Personal Privacy Policy Specification¹

George Yee, National Research Council Canada, Canada
Larry Korba, National Research Council Canada, Canada
Ronggong Song, National Research Council Canada, Canada

Abstract

The growth of the Internet has been accompanied by a proliferation of e-services, especially in the area of e-commerce (e.g., Amazon.com, eBay.com). However, consumers of these e-services are becoming more and more sensitive to the fact that they are giving up private information every time they use them. At the same time, legislative bodies in many jurisdictions have enacted legislation to protect the privacy of individuals when they need to interact with organizations. As a result, e-services can only be successful if there is adequate protection for user privacy. The use of personal privacy policies to express an individual’s privacy preferences appears best-suited to manage privacy for e-commerce. We first motivate the reader with our e-service privacy policy model that explains how personal privacy policies can be used for e-services. We then derive the minimum content of a personal privacy policy by examining some key privacy legislation selected from Canada, the European Union, and the United States.

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

The rapid growth of the Internet has been accompanied by a proliferation of e-services targeting consumers. E-services are available for banking, shopping, learning, healthcare, government services, and many other areas. However, each of these services requires a consumer’s personal information in one form or another. This leads to consumer concerns over unwarranted leakage, storage, and/or exploitation of their private information. Indeed, consumer savvy regarding their rights to privacy is increasing. In Canada, recent federal privacy legislation known as the Personal Information Protection and Electronic Documents Act (PIPEDA) (Government of Canada) has forced businesses to seek consumer permission before collecting personal information. Similar legislation exists in the European Union (European Union, 1995) and in the United States for healthcare (U.S. Government). In this light, e-services must respect consumers’ personal privacy if they are to be successful.

A promising solution for management of private information in e-services is to employ consumer personal privacy policies, that is, a consumer expresses his/her privacy preferences in a personal privacy policy. Once the e-service provider agrees with this privacy policy, it is then the provider’s responsibility to comply with it. These are the basic tenets of our e-service privacy policy model (explained in the section E-Service Privacy Policy Model [EPPM]) to motivate the need for personal privacy policies). However, what should go into the personal privacy policy? In this work, we answer this question by examining privacy legislation from Canada, the European Union, and the United States. (Although we could have looked at privacy legislation in other countries as well, we settled on these three because our audience is expected to be mostly from these regions and thus be subject to privacy legislation from them). The result is the minimum personal privacy policy, that is, one that contains the necessary elements to satisfy privacy legislation, but one that can contain extra privacy provisions according to consumer wishes. We shall indicate what some of these “extra provisions” could be.

Policy-based management approaches have been used effectively to manage and control large distributed systems. As in any distributed system, e-services may also use a policy-based framework to manage the security and privacy aspects of operations. For privacy policies, there are related works such as P3P (W3C), APPEL (W3C, 2002), PSP (Carnegie Mellon University), and EPAL (IBM), which are languages for expressing privacy preferences in policies. Web sites use P3P to divulge their privacy policies to consumers. APPEL is a specification language used to describe a consumer’s privacy preferences for comparison with the privacy policy of a Web site. PSP is a protocol in the research stage that provides a basis for policy negotiation. EPAL is a markup language for privacy preferences. These works are not necessary for the purposes of this chapter. They only serve as illustrations of what has been done in the related area of capturing privacy preferences in a form amenable to machine processing. Our work differs from P3P, APPEL, PSP, and EPAL in that we look at privacy legislation and other regulations in order to derive a core set of privacy attributes that are required by law in the content of a consumer personal privacy policy, rather than be concerned with expressing preferences in machine processable form. In fact, the example personal privacy policies we give in this chapter are expressed in English. Therefore, we are not