Semiautomatic Derivation and Use of Personal Privacy Policies in E-Business

George Yee & Larry Korba
National Research Council Canada, Canada

ABSTRACT

The growth of the Internet has been accompanied by the growth of Internet e-business services (e.g., electronic bookseller services, electronic stock-transaction services). This proliferation of e-business services has in turn fueled the need to protect the personal privacy of e-business users or consumers. We advocate a privacy policy approach to protecting personal privacy. However, it is evident that the specification of a personal privacy policy must be as easy as possible for the consumer. In this paper, we define the content of personal privacy policies using privacy principles that have been enacted into legislation. We then present two semiautomated approaches for the derivation of personal privacy policies. The first approach makes use of common privacy rules obtained through community consensus. This consensus can be obtained from research and/or surveys. The second approach makes use of existing privacy policies in a peer-to-peer community. We conclude the paper by explaining how personal privacy policies can be applied in e-business to protect consumer privacy.

Keywords: automatic generation; e-business; privacy; privacy policy; privacy rights

INTRODUCTION

The rapid growth of the Internet has been accompanied by an avalanche of e-business services targeting consumers. E-business services (or “e-services” — we use these terms interchangeably) are available for banking, shopping, stock investing, and health care, to name a few. However, each of these services requires a consumer’s personal information in one form or another. This leads to concerns over privacy.

In order for e-business services to be successful, privacy must be protected. In a recent U.S. study by MasterCard International, 60% of respondents were concerned with the privacy of transmitted data (Greer & Murtaza, 2004). An effective and flexible way of protecting privacy is to manage it using privacy policies. In this approach, each provider of an e-service has a privacy policy specifying the private information required for that e-service. Similarly, each consumer of an e-service has a privacy policy specifying the private infor-
mation he or she is willing to share for the e-service. Prior to the activation of an e-service, the consumer and provider of the e-service exchange privacy policies. The service is only activated if the policies are compatible. Where the privacy policy of an e-service consumer conflicts with the privacy policy of an e-service provider, we have advocated a negotiations approach to resolve the conflict (Yee & Korba, 2003a, 2003b). However, where do these privacy policies come from? Providers, in general, have sufficient resources to come up with their privacy policies. Consumers, on the other hand, need help in formulating privacy policies. In addition, the creation of such policies needs to be as easy as possible or consumers would simply avoid using them. Existing privacy specification languages such as P3P and APPEL (W3C APPEL, 2002; W3C Platform, n.d.) that are XML-based are far too complicated for the average Internet user to understand. Understanding or changing a privacy policy expressed in these languages effectively requires knowing how to program. What is needed is an easy, semiautomated way of deriving a personal privacy policy. In this paper, we present two semiautomated approaches for obtaining personal privacy policies for consumers and explain how the policies are used to protect consumer privacy.

The “Specification of Privacy Policy Content” section examines the specification of privacy policies by identifying some attributes of private information collection. The “Semiautomated Derivation of Personal Privacy Policies” section shows how personal privacy policies can be semiautomatically generated. The “Privacy Management Model” section presents our privacy management model, which explains how personal privacy policies can be used to protect consumer privacy. The “Discussion and Related Work” section discusses our approaches and presents related work. The paper ends with conclusions and future research.

SPECIFICATION OF PRIVACY POLICY CONTENT

Privacy Legislation and Directives

In Canada, privacy legislation is enacted in the Personal Information Protection and Electronic Documents Act (PIPEDA; Department of Justice, n.d.) and is based on the Canadian Standards Association’s Model Code for the Protection of Personal Information (Canadian Standards Association, n.d.), recognized as a national standard in 1996. This code consists of ten privacy principles that for convenience, we label as CSAPPs. Data privacy in the European Union is governed by a very comprehensive set of regulations called the Data Protection Directive (European Union, 1995). In the United States, privacy protection is achieved through a patchwork of legislation at the federal and state levels. However, privacy has been recognized as a constitutional right and there has existed a highly developed system of privacy protection under tort law for the past century (Industry Canada, n.d.).

Requirements from Privacy Principles

In this section, we identify some attributes of private information collection or personally identifiable information (PII) collection using CSAPPs as a guide. Note we use private information and PII inter-
Collaborative Commerce
www.igi-global.com/chapter/collaborative-commerce/4748?camid=4v1a