Chapter 13
A Privacy Agreement Negotiation Model in B2C E-Commerce Transactions

Murthy V. Rallapalli
IBM and Stevens Institute of Technology, USA

ABSTRACT

This article presents an alternate approach to effectively address the way privacy agreements are initiated through web services. In this new framework, the consumer and the service provider can mutually negotiate on the privacy terms. It contains a privacy model in which the transaction takes place after a negotiation between the service provider and the web user is completed. In addition, this framework would support various negotiation levels of the agreement lifecycle which is an important aspect of the dynamic environment of a B2C e-commerce scenario. A third party trusted agency and a privacy filter are included to handle privacy information of the web user. The author seeks to raise awareness of the issues surrounding privacy transactions and the potential ongoing impact to both service providers and clients as the use of web services accelerates.

INTRODUCTION

Privacy agreements are invariably a one-sided agreement with the service provider asking the web user, “Unless you accept it, you can go no further with this transaction”. In this scenario as shown in Figure 1, the customer has no choice but to click on ‘I agree’ to proceed further with the transaction. If the web user chooses not to agree to the terms, the application will not allow the web user to go any further. The agreement is just a good gesture on the part of the service providers. However, lately, it has become a privacy weapon where service providers impose their version of the privacy policies with no room for any type of negotiation. Today, every individual who conducts e-commerce transactions on the web is guaranteed to part with certain private information in order to complete the transaction. This leads to concerns that privacy information being collected may be misused by the collecting organizations or businesses. For a secure e-commerce transaction...
experience with minimal risk, it is important to build customer confidence with service providers, particularly, when these service providers collect privacy data. Figure 1 is an example of a typical privacy agreement. Service providers leverage web services to present such privacy policies of the service provider’s organization.

Privacy agreements (similar to Figure 1) presented to the customer state what the organization would do with the personal information. However, simply presenting a privacy policy to the web user does not guarantee the protection of personal information of the customer. A verbal promise through this type of agreement has very little legal ground to hold the service provider responsible for any privacy data misuse (Powers, 2002). There is a need for something more secure; a more formal (legally binding) than what is currently provided in a privacy agreement today.

Today’s privacy agreements are notorious for being a one-sided agreement presented by the service provider to the service consumer. The service providers dynamically revise their privacy policies as well to accommodate new business strategies, changes to laws and regulations. Another concern is what happens to this collected data. In many situations it is being bought back by various industries and corporate information systems. Consider institutions such as banking, insurance, telecom and how they are leveraging this personal data to customize products and minimize fraud, which may lead to discriminatory trends. Worse is that these trends may even be automated (Davis, 2000). For example tracking people through mobile phone roaming may indicate that they drive frequently through low income neighborhoods and thus may be categorized as high risk for car insurance. People purchasing cigarettes online could be categorized as higher risk for health problems by insurance companies which result in increases in health premiums. This type of data mining is often used to create separate “categories” of people. As organizations collect more and more personal information, everyday behavior will be aggregated by corporations and governments to augment social control (Newman, 2009). The fundamental point of entry into the collector’s archives is through web transactions. It is when a web user logs on, and if the privacy data is being controlled, then data aggregation will also be controlled.

In this paper, I propose a framework where the consumer and service provider interactively decide on privacy terms. The framework develops

Figure 1. A privacy agreement presented to the customer