Chapter VII
Online Personal Data Licensing: Regulating Abuse of Personal Data in Cyberspace

Yuh-Jzer Joung
National Taiwan University, Taiwan

Shi-Cho Cha
National Taiwan University of Science and Technology, Taiwan

ABSTRACT

We propose a new technical and legal approach, called online personal data licensing (OPDL), for responding to concerns about the privacy of personal data. Unlike traditional privacy-enhancing technologies that typically aim to hide personal data, OPDL enables individuals to concretize their consent to allow others to use their personal data as licenses. Service providers must obtain licenses before legally collecting, processing, or using a person's data. By allowing individuals to issue their own licenses and to determine the content of the licenses, OPDL brings the control of personal data back to their owner, and ensures that the use of the data is strictly under the owner's consent. In contrast, most Web-based service providers today use passive consent, which usually results in situations in which users have inadvertently given the providers the authorization to use their personal data. Besides, users generally do not have information on who still owns a copy of their data, and how their data have been, or will be, used.

INTRODUCTION

Personal data have been used for many different purposes in cyberspace. For example, in customer relationship management (CRM) and one-to-one marketing, service providers collect their customers' data and use them to understand the customers' wants, goals, and needs, so as to improve their quality of service and the customers' loyalty and lifetime value (Hanson, 1999).

An unfortunate problem, however, is that most people are not aware of who has collected their personal data, who has used that data, for what purposes, and who still holds a copy of the data. In fact, the advances in the Internet and information technologies, although allowing personal data to be efficiently collected and processed, have at the same time turned cyberspace into a hotbed for data abuse, for example, e-mail spamming (Cerf, 2005; Peeger & Bloom, 2005), and credit card fraud (Walia, 2006).

To face these new challenges, many countries have enacted laws to regulate abuse of personal data in cyberspace, for example, the Australian Privacy Act (Australian Government, 1988), the British Data Protection Act (British Government, 1998), the Personal Information Protection and Electronic Document Act of Canada (Canada Government, 2000), the German Federal Data Protection Act (German Government, 2001), and so forth. Moreover, the European Parliament and Council passed the European Union's Directive 95/46/EC, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, in 1995 (European Union, 1995). It requires the member states of the EU to put their national legislation in line with the provisions of the directive. Transmission of personal data to non-EU countries that do not meet its standard for data protection is prohibited. Because of the stricture on cross-border flows of personal data in the Directive and the emergence of well-networked global policy communities, laws on personal data protection in different countries are progressively toward a convergence (Bennett, 1997). That is, although the words of personal data protection laws may be different in different countries, they usually follow some basic principles.

However, even though some basic principles have been established, the current Internet architecture does not easily allow abuse of personal data to be discovered and proved. This is because Internet service providers are usually required to obtain a user's consent when his/her data are to be collected and processed. For example, the EU Directive stipulates that personal data can be processed only if the owner (the *data subject*) has unambiguously given his/her consent (European Union, 1995). There are many types of consent, such as *oral/verbal, written, proxy, passive*, and so forth (University of Washington, 2006). Obviously, written consent can provide the strongest power of evidence, especially when disputes occur. Considering the dynamics of cyberspace and the flow of information, however, it is very inefficient and inconvenient for users and service providers to proceed with written consent. Therefore, passive consent is generally allowed and adopted in many countries. To obtain a passive consent, a Web site simply discloses its practices about personal data at its site. If one continually uses the site's services or even registers as a member of the site, then this will be considered as an indication that consent has been given to the site.

A problem with passive consent is that it is very hard for users to prove that the sites have used their personal data in accordance with their understandings. To see this, suppose that when a person registered as a member of an online shopping site, the privacy policies of the site did not express an intention to collect its users' transactional behaviors. Some days after, the site decided to do so for, say, one-to-one marketing. The site did not actively inform its users about this decision, but only modified (perhaps silently) its disclosed privacy policies. If the person later discovers that the site has collected his personal data without his consent and decides to make a complaint against the site, he needs to prove that the modified privacy policies are *not* the ones he saw when he registered at the site. Clearly, this complaint is hard to make a case, as the user may not have enough evidence to support him.

To make cyberspace more "regulable" (Lessig, 2000) without sacrificing efficiency, we propose *online personal data licensing* (OPDL) (Cha & Joung, 2002). Our goal is to build a privacy protec-