A Generic Privacy-Enhancing Personalization Infrastructure

Yang Wang and Alfred Kobsa

Donald Bren School of Information and Computer Sciences
University of California, Irvine, U.S.A.
{yangwang,kobsa}@uci.edu

Abstract. Respecting users' privacy is a key challenge for building personalized systems. We have designed a generic privacy-enhancing personalization infrastructure that allows system designers to express privacy constraints at design time and enables system enforcement of privacy constraints at runtime.

1 Introduction

As personalization emerges as a mainstream practice for web sites, privacy issues only get heightened. A recent example is Facebook Open Graph. Open Graph is an innovative technology that gives its users "instant" personalized experience in Facebook partner sites (e.g., cnn.com and yelp.com) without users logging in these sites [1]. Despite its appeal, it also "ratchets up privacy concerns" [2]. To reconcile privacy and web personalization, two main types of privacy constraints need to be taken into consideration in designing and implementing web-based personalized systems: regulatory privacy requirements set out by various privacy laws and regulations [3], and users' personal privacy preferences/needs [4].

2 Infrastructure Functionalities

We have designed a generic privacy-enhancing personalization infrastructure that: (1) supports system designers to graphically express privacy constraints, their interdependencies as well as their impacts on the personalized system at design time, (2) allows end users to set their personal privacy preferences and to see how the personalized system operates in accordance with their current privacy settings, and (3) enables run-time dynamic enforcement of the privacy constraints in the system.

To our best knowledge, all three features above are novel in personalized systems. See [5] for a more comprehensive review of related work in this area.

2.1 Support System Designers to Express Privacy Constraints

System designers of privacy-enhancing personalized systems need to capture two domain models: (1) a system model representing the system features/components and their interdependencies, and (2) a privacy model expressing the privacy constraints, their interdependencies, and the impacts of these privacy constraints on the system features.

We use the notions of change sets and relationships as the underlying constructs to represent the two domain models [6]. A change set is an individually-identifiable set of changes from a base version of a system. A particular version of the system can be composed by mixing and matching different change sets. Relationships are constraints that govern the system composition from change sets. Relationships among change sets are constructed using logic operators such as AND and OR. We design four types of change sets in our modeling tool: feature change sets and relationships which are used to model the software model, preference change sets and country change sets which are used to model the privacy model, and mapping change sets which are used to connect the two models.
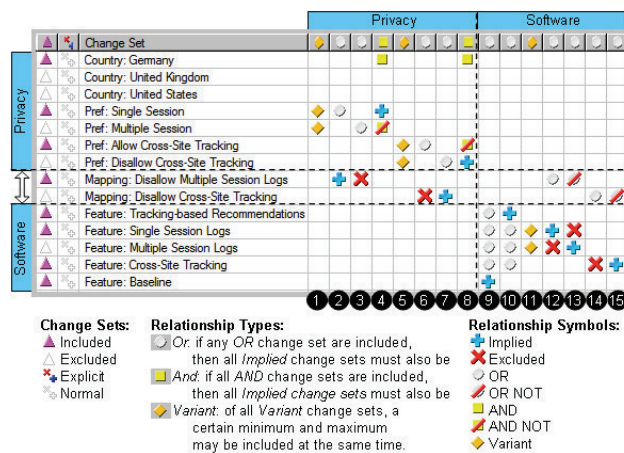

Fig. 1. Modeling System Domain, Privacy Domain, and Their Interdependencies

Figure 1 illustrates the usage of our modeling tool for a personalized system. Each row represents a change set and each column to the right of the "Change Set" column represents a relationship. The two domain models remain independent, interconnected only through the common mapping change sets. This approach makes the two models less coupled and thus easier to model and manage. This tool also makes it straightforward to track which country and what specific privacy constraints have been supported. This would make both internal and external audits easier.

2.2 Support Users to set Privacy Preferences and See Consequences Instantly

This infrastructure also enables users to express their privacy preferences with regard to a personalized system. More importantly, users can see immediately the consequences of their privacy changes/settings in terms of how the underlying personalized system might change (e.g., certain system components get turn on or off). Figure 2 shows an example of this functionality. The upper part contains the privacy options that a user can specify, while the lower part lists the usage of personalization components according to the current privacy settings.
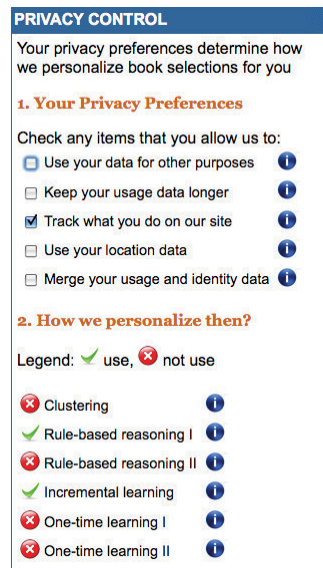
Fig. 2. Privacy Control Tool for Users

2.3 Enforcement of Privacy Constraints at Runtime

Internally, each personalization component is associated with a Boolean guard. The current privacy settings are translated as values that are used to evaluate these Boolean guards. A personalization method would be turned on if its Boolean guard is evaluated to be true, and vice versa [7].

References

1. Facebook: Open graph protocol. http://developers.facebook.com/docs/opengraph (2010)
2. Shuler, P.J.: Facebook's open graph ratchets up privacy concerns. http://www.npr.org/templates/story/story.php?storyId=126183577 (2010)
3. Wang, Y., Chen, Z., Kobsa, A.: A Collection and Systematization of International Privacy Laws, with Special Consideration of Internationally Operating Personalized Websites. (2006)
4. Teltzrow, M., Kobsa, A.: Impacts of user privacy preferences on personalized systems: a comparative study. In: Designing personalized user experiences in eCommerce. Kluwer Academic Publishers (2004) 315–332
5. Wang, Y., Kobsa, A.: Technical solutions for Privacy-Enhanced personalization. In: Intelligent User Interfaces: Adaptation and Personalization Systems and Technologies. IGI Global, Hershey, PA (2009) 353–376
6. Wang, Y., Hendrickson, S.A., van der Hoek, A., Taylor, R.N.: Modeling PLA variation of Privacy-Enhancing personalized systems, San Francisco, CA (2009) 71–80
7. Wang, Y., Kobsa, A. In: Respecting Users' Individual Privacy Constraints in Web Personalization. Berlin - Heidelberg - New York: Springer-Verlag, Corfu, Greece (2007)