

# PRIVACY BY AGREEMENT

Dora Galvez-Cruz & Karen Renaud

*Department of Computing Science, University of Glasgow  
17 Lily bank Gardens, G12 8RZ. Glasgow, Scotland, UK*

## ABSTRACT

Privacy is a very important issue for web users, but many don't fully understand the implications of privacy violations. They easily disclose their private data in exchange for few benefits without being aware of the risks of sharing their private information. One of the main reasons for this careless disclosure could be the lack of control that the users think they have over their own data. To solve this there have been several attempts to guard the user's privacy, with most effort concentrated in health related applications. This work presents a different approach to the preservation of privacy, focusing on e-commerce, an agreement by which the users can select how much and which particulars of their personal information is to be disclosed before using the e-commerce web site, allowing them to browse the e-store even if they decide not to disclose any information. This proposal's aim is to generate mutual benefits both for customers and for retailers. This work builds on the success points of other privacy proposals, avoids their reported pitfalls and delivers a new approach to ensuring the protection of privacy while facilitating personalisation of e-commerce.

## KEYWORDS

E-Commerce, personalisation, privacy.

## 1. INTRODUCTION

The study of shopping as phenomena has captivated the attention of researchers. Investigations range from physical (i.e. the ergonomics of a store) to subjective such as identifying what elements influence the customer's decision to buy items. Underhill (Underhill 2000) has developed an empirical observational method which he uses to determine the optimal ergonomics of a store, determining the location of the goods and the combination of colours, for example. The position of the merchandise on the shelves has been found to be particularly important.

On the other hand, other studies show that shopping is not only a physical reaction to the location of goods within stores, since customers are influenced by other factors as well. For instance the context of the shopper is also relevant; a mother might buy cheap goods for herself while spending much more on her items for her children (Miller 1998). We can therefore make a distinction between *necessity* shopping and *desire* shopping. Necessity shopping leads customers to buy the goods they really need, while the latter satisfies a desire, fashion or mood. Retailers expect more income from desire shopping than from necessity (Casino 2001).

There is a definite move away from brick-and-mortar traditional shopping to the use of e-commerce. Knowledge of previous shopping experiences and of individual customer behaviour and needs in traditional shopping can be used to successfully adapt e-commerce to meet their needs. It's very likely that brick-and-mortar customer behaviours could be mapped to e-commerce. For instance, window shopping is beginning to appear in e-commerce (Germain 2005). Therefore, other successful practices in brick-and-mortar shopping could be adapted to e-commerce and might improve the customer's shopping experience, guarantee customer loyalty and increase profits. E-commerce delivers many advantages to customers, including special delivery, 24 hour shopping and personalisation. Because of these advantages and the convenience of the use of e-commerce it has carved itself a significant niche in the Internet (Kelly 1998). Whereas we have discussed e-commerce from the customer's perspective, it also offers new opportunities for retailers in matching offered goods to the individual customer. This is done by means of personalisation. There are, however, some concerns about the use of personalisation.

The following section focuses on personalisation, and the issues that personalisation brings to privacy. Section 3 mentions the efforts related to preserve privacy, while section 4 presents this paper's proposal for ensuring user privacy. At the end of this paper, a scenario is presented which motivates the use of the privacy agreement.

## 2. PERSONALISATION

E-commerce is still a new technology and commercial area. In 1998, the OECD (COOPERATION & DEVELOPMENT 1999) reported 1995 as the start of e-commerce, and from this early stage the predications about its future development were optimistic due to wide-scale adoption of the Internet. Major e-commerce stores increased in popularity. The evolution of e-commerce is reflected in the e-customers' behaviour. These behaviours involve better informed customers (sometimes better than the retailers) who search for the best options discovered through the Internet and compare before any purchasing (Economist 2004). However, some practices such as customers abandoning the "shopping cart" just before the purchase, and window shopping, reflect traditional shopping behaviour (Germain2005).

In general, personalisation is based on obtaining customer preferences and characteristics. These characteristics are used to derive a set of rules. The elements matching those modelled rules are presented to the user, facilitating a more focused and easy navigation through the site.

One of the main characteristics of personalisation is the way it adapts to the individual customer's preferences, according to seasons and fashions and previous shopping behaviour. Hence e-commerce is an area of computer science that is constantly evolving. Personalisation has proven to be a key in the success of certain e-commerce sites, as in the case of Amazon.com, and some authors are trying to get the attention of other retailers due to the potential of this mechanism (Kasanoff 2001).

Even though personalisation is an important facet of e-commerce, it shouldn't be overestimated; it is just one part of the front end that the customer perceives, but it needs the support of the rest of the company's infrastructure to guarantee customer satisfaction.

We can obtain the customer's profile in two main ways, collaboratively or via observation. In the collaborative method, the customer is asked to provide their preferences either by filling in a form or by selecting from interactive elements on a screen. The observational method tracks the customer's activities during their web session and this data is collected and stored. These data are the basis of a further analysis that will generate the rules that will eventually become the key to the layout the information that will be presented to the customer.

No matter which method is used to personalise e-commerce, to be successful both methods require the use of the customer's personal information, but the way that this information is collected or the subsequent use of the information has raised one major issue in personalisation: privacy, which will be discussed in the following section.

## 3. PRIVACY

The need for privacy can be traced back to 1890 (Warren & Brandeis 1890) where the 'right to be let alone' is argued. From that date onwards there have been several attempts to install privacy as a basic human right and to create laws to protect individual privacy.

Maslow proposes a hierarchy of needs (Ventegodt, S., J. Merrick, and N. J. Andersen 2003). These needs are divided into five levels with more basic needs appearing at the lowest levels. The upper level needs cannot be met unless the lower level needs are met. While Maslow's first level deals with the physiological needs, the second level deals with security, which includes privacy. Hence, if privacy is a basic human need and laws are being created to protect it, the issues that puzzle researchers are the reasons behind the apparent thoughtless disclosure of personal details. Studies have found that users disclose their private data in exchange for something of little value (Acquisti 2004). Sometimes the user's private data are misused by companies. There is also a distinct reluctance by customers to read web site privacy policies (Vila, Greenstadt & Molnar 2003).

Many groups have tried to address these privacy concerns:

- Anonymity: Provide a different IP address, so the web page cannot trace the previous web page visited (Glater 2006)
- Creation of an image of the user: This intent was used in ubiquitous computing to hide the user's presence within an awareness system (Lederer, Hong, Dey & Landay 2004)
- Creator of licenses: Creates and negotiates licenses (Huang 2005)
- Creator of privacy policies: an application that can create, implement and monitor the compliance of privacy policies (Brodie, Karat, Karat & Feng 2005)
- Council of Europe: "Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data" (of Europe 1981)
- P3P: "Defines the syntax and semantics of P3P privacy policies, and the mechanisms for associating policies with Web resources" (Cranor, Dobbs, Egelman, Hogben, Humphrey, Langheinrich, Marchiori, Presler-Marshall, Reagle, Schunter, Stampley & Wenning 2006)

The low use of these options might well be due to the high technological expertise and high level of privacy awareness that is required in order to motivate their use.

Allowing users to control the disclosure of their own data has presented some problems, such as the users requiring extra help and revealing their information to their assistant. The next section presents an improved mechanism for maintaining the customer's privacy while supporting personalisation.

## 4. PRIVACY-ENHANCED PERSONALISATION

Both retailers and customers can benefit from the e-commerce experience with an agreed personalisation feature offered by the company and real personal information voluntarily disclosed by the customer. By agreeing on the level of disclosure, the customers maintains control over their privacy and will know exactly what information the retailer is storing about them.

To set up this agreement, the customer will supply personal information and shopping context according to their privacy preferences. Using this information, the retailer will give the customer access to specific personalisation features rewarding the confidence displayed by the customer and the degree of information disclosure. Penalties will apply to both parties in case of fraudulent activity.

The PLA (*Personal Level Agreement*) captures the details of this agreement process. The design of the PLA is based on two important privacy initiatives: P3P and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (Cranor et al. 2006)

The first is related to the syntax and semantics of privacy policies, their location and access. The second is related to the content, handling, sharing, uses and storage of the information that should be kept from the customers, including the information's physical location.

Therefore, the PLA integrates recent research findings concerning privacy in the form of a system that handles the customer's privacy and allows a customer to be in control of his or her own privacy. The design and implementation of the PLA are presented in next section.

### 4.1 PLA DESIGN AND IMPLEMENTATION

In order to facilitate the agreement process the customer accesses e-commerce sites via a third party web site, called the "Alter-Ego Website", which allows customers to choose one of three different levels: *Bronze*, *Silver* and *Gold* to access different e-commerce sites. Bronze (the third level) would be almost anonymous and few personalisation features would be offered, the anonymity of this level would be lost only at actual purchase, where the store receives the customer's credit information and delivery address. Records of the purchases are kept only for legal purposes.

Silver (the second level) requires disclosure of a few more information in exchange for extended personalisation features, while Gold (first level) requires full customer disclosure and allows the site to store shopping context. The store then delivers all the available personalisation features and thereby rewards the customer's loyalty.

The following is a scenario best showing the flexibility and uses of the PLA. A mother does her regular e-grocery shopping on a store that implements the PLA. She uses Gold level taking advantage of all the

facilities that the store offers. The store keeps a record of her previous purchases and can offer suggestions based on them. She then buys her youngest son a number of football-related gifts for his birthday and uses the context feature that tells the site not to include football in order to provide her with recommendations, but she would like football recommendations in a yearly calendar reminding her of the proximity of the son's birthday and reminding her the items that she already bought so she doesn't buy them again. One weekend, she has to do the shopping for her husband's office meeting and she doesn't want all the alcohol and meat to affect her vegetarian recommendation

## 5. CONCLUSION

This paper presents a new perspective to the preservation of privacy while personalising e-commerce, discusses the importance of personalisation and argues that privacy is personalisation's Achilles' heel. It enumerates privacy-related research efforts, proposes a pre-settled agreement between the e-commerce store and the customer where the customer discloses personal information in exchange for personalisation features according to three different levels. This proposal is called the Personal Level Agreement.

## REFERENCES

- Acquisti, A. 2004, *Privacy in electronic commerce and the economics of immediate gratification*, in EC '04: Proceedings of the 5th ACM conference on Electronic commerce, ACM Press, New York, NY, USA, pp. 21-29.
- Brodie, C., Karat, C.-M., Karat, J. & Feng, J. 2005, *Usable security and privacy: a case study of developing privacy management tools*, in SOUPS '05: Proceedings of the 2005 symposium on Usable privacy and security, ACM Press, New York, NY, USA, pp. 35-43
- CO-OPERATION, O. F. E. & DEVELOPMENT 1999, *The Economic and Social Impact of Electronic Commerce Preliminary Findings and Research Agenda*, OECD Press.
- Cranor, L., Dobbs, B., Egelman, S., Hogben, G., Humphrey, J., Langheinrich, M., Marchiori, M., Presler-Marshall, M., Reagle, J., Schunter, M., Stampely, D. A. & Wenning, R. 2006, *The platform for privacy preferences 1.1 (p3p1.1) specification*, <http://www.w3.org/TR/2006/WD-P3P11-20060210/Overview.html> Last Accessed 11 July 2006.
- Economist, T. 2004, *A perfect market*, The Economist.
- Germain, J. M. 2005, *Online consumers window shop more than impulse buy*, <http://www.ecommercetimes.com/story/42761.html> Accessed 29 June 2005.
- Glater, J. D. 2006, *Online, but out of sight*, <http://www.technewsworld.com/48538.html> Accessed 06 March 2006.
- Huang, Y.-J. J. C. Y. C.-T. H. Y.-J. 2005, *On personal data license design and negotiation*, in Computer Software and Applications Conference, 2005. COMPSAC 2005. 29th Annual International, Vol. 1, pp. 281-286 Vol 2.
- Kasanoff, B. 2001, *Make it Personal how to profit from personalization without invading privacy*, 1 edn, Perseus Publishing.
- Kelly, K. 1998, *New rules for the new economy: 10 ways the network economy is changing everything*, London: Fourth Estate, c1998.
- Lederer, S., Hong, I., Dey, K. & Landay, A. 2004, *Personal privacy through understanding and action: five pitfalls for designers*, Personal Ubiquitous Computing. 8(6), 440-454.
- Miller, D. 1998, *A Theory of Shopping*, Cornell University Press.
- C. of Europe, 1981, *Convention for the protection of individuals with regard to automatic processing of personal data*, <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm> Last Accessed 11 July 2006.
- Underhill, P. 2000, *Why We Buy: The Science Of Shopping*, Simon & Schuster.
- Ventegodt, S., J. Merrick, and N. J. Andersen 2003. *Quality of life theory iii. Maslow revisited*. The Scientific World Journal 3, 1050 - 1057.
- Vila, T., Greenstadt, R. & Molnar, D. 2003, *Why we can't be bothered to read privacy policies models of privacy economics as a lemons market*, in ICEC '03: Proceedings of the 5th international conference on Electronic commerce, ACM Press, New York, NY, USA, pp. 403-407.
- Warren & Brandeis 1890, *The right to privacy*, Harvard Law Review. IV(5).