Privacy: Aspects, Definitions and a Multi-Faceted Privacy Preservation Approach

Karen Renaud & Dora Gálvez-Cruz
Department of Computing Science, University of Glasgow
Email: {karen}@dcs.gla.ac.uk

***Abstract*—There are many different definitions and understandings of the concept of privacy. Here we bring all the different aspects of privacy together and propose a comprehensive definition thereof. We also introduce the three different approaches to privacy preservation, and propose a comprehensive and multi-faceted approach in order to gain from the benefits of each and maximise privacy protection. We report on the evaluation of a prototype of such a privacy protective shopping environment.**

I. Introduction

Any unauthorised invasion of a person's moral, intellectual or physical space can constitute a violation of their privacy. Reading somebody else's diaries, opening somebody else's mail or taking unwanted or unauthorised photos all represent privacy clear violations. With the arrival of the Web, the concept of privacy has become a far more nebulous concept. Several definitions have been proposed, each of which focuses on particular aspects of privacy, but there are also claims that defining privacy is, as yet, an unresolved issue [1]. Here we explore various facets of privacy in order to provide a foundation for privacy research.

Early efforts to define privacy can be traced back to 1890, as evidenced by "The right to privacy" [2]. This publication raised the issue of photographers taking 'instantaneous photographs' without previous consent, and considers it a clear invasion of the person's privacy. This concern remains, as evidenced by the residents of Broughton's action against the Google camera car [3]. Judge Cooley [2] referred to privacy as "the right to be let alone", once again something the modern-day person also feels keenly [4], [5]. The Oxford dictionary online (OED), defines privacy as:

> *The state or condition of being withdrawn from the society of others, or from public interest, seclusion.*

Princeton University states that privacy is [6]:

- *The quality of being secluded from the presence or view of others*
- *The condition of being concealed or hidden*

These definitions identify two main aspects of privacy; the first refers to the affected person and the right to establish a separate space; and the second to the society and the limitations of others' access to the person's space. These definitions work together to formulate an idea of a frontier between a person and the surrounding environment, focusing on delimitation of the person's boundaries. Organisations such as *Privacy International* consider privacy to be a fundamental human right, linked with human dignity, defining privacy as:

> *The desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves. (Robert Ellis Smith, editor of the Privacy Journal)*

Ellis' definition goes beyond the OED and Princeton definitions by specifying privacy in terms of a *physical* space, including protected activities within that space and gives control over personal information to the owner thereof.

The Calcutt Committee in the United Kingdom [7], also consider privacy a right with a particular focus on protection against intrusion:

> *The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information.*

While some organisations define privacy by focusing on the concept itself, others delineate privacy based on related terms and contexts where privacy can be found. In this way, privacy is associated with autonomy, dignity, anonymity, freedom, liberty, control and consent [1], as well as the determination of a personal boundary.

Finally, according to *Privacy International*, privacy can be associated with four main concepts [8]: (In each case an example from 2009 is cited to show that these issues are still pertinent 5 years later.)

1) *Information privacy* — also called data protection, refers to the withholding of the information collected about a person and the regulation of that collection. Any records such as bank account, health or government records fit into this category [9].
2) *Bodily privacy* — concerned with physical tests, including any medical sample taken from the person's body, i.e. blood samples, DNA and any genetic or medical tests. Recent concerns about indiscriminate collection and recording of DNA highlights this concern [10].
3) *Privacy of communications* — All communication media regardless of the technology: mail, e-mail, telephone. The UK Government is moving to gain access to social networking sites' communications, which is concerning privacy groups [5].
4) *Territorial privacy* — deals with the limits of intrusion. These limits can be domestic, work, surveillance cam-

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

eras, etc [4], [11].

Privacy's core concepts can be distilled from the different definitions:

- A physical space in which the person can: set boundaries; be concealed from society; and be protected against unauthorised intrusion.
- The subject control disclosure of personal information.
- The person should be left alone, and receive the same protection for their family.
- Privacy can be related to the following terms: Autonomy, Dignity, Anonymity, Freedom, Liberty, Control, Consent.
- Finally, privacy can be related to the following contexts Data protection, Bodily, Communications, Territorial.

The following privacy definition combines all the above-mentioned core privacy concepts into one concise definition [12]:

> *Privacy is the faculty and right that a person has to define, preserve and control the boundaries that limit the extent to which the rest of society can interact with or intrude upon. At the same time, he or she retains full control over information generated by, and related to, him or her.*

This definition considers privacy a human right and gives a person the right to control, and have responsibility for, the delineation of, and right to enforce, personal boundaries. It also proposes that people, by the mere fact of existence, possess information that defines them, and that the disclosure of this information should remain under the owner's control. Finally, it covers the importance of control over one's own bodily information and any information that can be extracted or deduced from it. To summarise, this work proposes that privacy is a person's: right to be aware of privacy precepts, to control disclosure of personal data, to control "person" information and to be left alone (enforce boundaries).

The use or misuse of others' disclosed information involves a different concept: confidentiality which *concerns the communication of private and personal information from one person to another* [13]. Hence confidentiality is concerned with the responsibilities of a custodian of of *other* people's personal data whereas privacy is associated with a person's control over his or her *own* personal data. As soon as private information is disclosed, one needs to trust the custodian to preserve the confidentiality of the data.

Given the fact that many entities are untrustworthy, people should be empowered to protect their own privacy by exercising appropriate controls to match their risk perception within the context of use.

II. Privacy and the E-Shopper

Shoppers in traditional stores can easily maintain their anonymity, and enjoy a relatively private shopping experience while examining goods, loading their trolleys and generally browsing without being concerned about their activities being tracked, recorded or being used to support false inference activities [14].

In order to market products more effectively, stores need to know more about their customers (i.e. using market segmentation) so many stores now provide their customers with loyalty cards. Many shoppers are unaware of the fact that loyalty cards are primarily used to collect information about their purchases, and to match customer demographics to shopping habits, very valuable information, which is hardly repaid by the paltry points awarded.

Loyalty cards have privacy issues since the collected information can be used against the customer. A case in point is that of Mr. Rivera in Los Angeles, USA. When he instituted an action to sue Vons store for a kneecap injury due to slipping on spilt yoghurt, he was told that his high alcohol consumption, stored on his records, was going to be made public in court [15], [16].

Most 21st century stores use the Web to market their goods and e-commerce has consequently exhibited steady growth over the last 10 years [17]. Loyalty cards are superfluous in e-stores because the customer is observed continuously. Different kinds of information is stored about shoppers. *Voluntarily disclosed* information includes the person's address, telephone number, email address etc. Sometimes the customer divulges information *involuntarily*, simply to make use of the site — such as, for example, their mother's maiden name. *Inadvertently disclosed* information is related to web site usage which is continuously collected and stored. Finally, information can be *derived* from a combination of disclosed and observed activities. A person who purchases large amounts of alcohol might, quite unfairly, be classified as an alcoholic. Any automatic classification system is bound to make mistakes [14] and the consequences for the shopper could be unpleasant.

This is the nub of the problem — e-stores ostensibly collect and store information in order to personalise the customer's shopping experience, and, in doing so, to increase their profit margin. Most shoppers have no issue with this. Unfortunately, the information related to a particular shopper can also be misused by the store to gain an unfair advantage (as in the case of Mr Rivera). In other cases the store might have affiliates who have an interest in people's shopping habits. A medical insurer, for example, would be very interested in the "healthiness" of products purchased by people they insure.

Unfortunately, many e-commerce customers often simply do not know that their personal information is being stored or that their activities are being tracked and that this information could harm them [18], [19]. At the very least, the e-store's web software is violating privacy. Any software system can be categorised according to the way it impacts on the user's privacy [20](p133-4):

1) *Privacy invasive* — a system that gratuitously uses personal data without due consideration of privacy principles.
2) *Privacy neutral* — a system within which privacy is not an issue.
3) *Privacy protective* — a system which limits access to personal information and/or provides a way for an individual to protect their own identity.

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

4) *Privacy sympathetic* — a system which limits access and usage of personal data with due consideration of privacy principles.

E-stores are currently *privacy-invasive*, with very little regard for the shopper's privacy rights. What is needed is privacy protective/sympathetic e-stores to redress the inequality between the two parties.

III. Privacy Protection

Since many believe the right to privacy is a human right, and we know that Web users are not being accorded that right, we need a strategy for helping Web users to regain control. One of three approaches is generally used to ensure that privacy is not violated: *raising awareness, regulation* and *the use of technology* — the ART approach.

A. Raising awareness

Awareness of privacy violations is growing as the media reports on cases where the confidentiality of data is not preserved [21], [22], [23], [24]. Organisations such as *Privacy International* also aim to raise the level of privacy-awareness [25]. They also work towards establishing world-wide privacy measures to facilitate the flow of privacy-related information.

Increased awareness of privacy risks has indeed been linked to a reduction in the level of trust and an increased demand for control, especially in relation to consumer privacy [26]. At the same time, increased awareness is bound to lead to a greater demand for control over disclosure, in terms of having the tools with which to protect customers from privacy violations. In terms of our privacy definition, the most important aspect is that of giving the person control over his or her own information. Four distinct privacy control states exist: [27], [26]:

- *Total control* — users have full/total control over disclosed information and environment.
- *Environmental control* — users have little control over disclosed information, but full control over the environment.
- *Disclosure control* — users have full control over disclosed information, but no control over the environment, and
- *No control* — user have no control over information or the environment.

In terms of how much control individuals may wish to exercise, Westin proposed three distinct privacy indices [28], derived from a series of surveys used to explore privacy concerns. Participants fell naturally into one of three main groups:

- *The Fundamentalist group*: people who distrust organisations asking for their personal information, are worried about computer-gathered information and its uses, and favour regulations (revised and new measures) to protect their privacy. Members of this group actively use controls to protect their privacy.
- *The Pragmatic group*: people who weigh the benefits of protection and regulation against the amount of information they are prepared to disclose, believing that trust should not be freely given but earned, and seek to have opt-out options.
- *The Unconcerned group*: people who trust organisations who gather their information to respect it. They are not in favour of new privacy regulations and do not use controls to protect their privacy.

Westin observed a change in privacy perceptions over time [29]. The number of participants falling into the *unconcerned* category decreased, the *fundamentalist* group maintained its numbers, while the number of *pragmatists* increased. Westin attributed this change to the increase of knowledge about technology and the awareness of protection methods [30].

Based on Westin's observations, the creation of awareness is an important factor which has the potential to change the user's privacy perceptions. Hence, an approach is needed in which customers can match their chosen measure of control to the circumstances under which the disclosure should occur. It has also been suggested by Olivero and Lunt [26] that customers, knowing that their information has value to the organisation, should be empowered to exchange a certain amount of information in return for benefits offered by the store.

Awareness, on its own, is sometimes not enough especially when the choice is disclosing information or abandoning the shopping basket. Many e-stores use cookies to track customer behaviour. The privacy risk posed by cookies is well-known and is easily prevented [31]. However, cookies are a very useful and convenient aid to browsing [32]. The fact that they can also unobtrusively and invisibly track the user's behaviour seems to matter less to consumers than the convenience they offer.

Realistically, we can therefore conclude that the raising of awareness is only one part of the solution. Given the tension between privacy protection and convenience, it is important to provide web users with a tool which satisfies both these needs. If we merely raise awareness, we could lead fundamentalists to abandon Web shopping altogether. The pragmatists, however, will probably want to exercise the option of trading certain information for benefits and need a mechanism to support this. However, before addressing this, we consider first the the regulatory aspects of privacy enforcement.

B. Regulation

An early aspiration to regulate privacy is evident in the use of the phrase 'The house is one's castle', during a legal case in the United States of America (USA) in 1604 [33].

The computer era led to a "computer bill of rights" being proposed, in 1966, which provided guidelines to control the storage and access to data stored by computers [34]. Computer privacy was addressed again in 1980, when the Organisation for Economic Co-operation and Development (OECD) published their first guidelines for international privacy [35].

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

During the 1990s several efforts were made to enforce the protection of privacy. The organisation *Privacy International* was created in 1990 to provide a forum for open discussion of privacy issues [8]. The USA's Federal Trade Commission (FTC) has, since 1998, taken action against companies that violate their own privacy policies. In 2002, as a result of privacy workshops, the "Platform for Privacy Preferences (P3P) Project" was created with the purpose of expressing privacy practices in a machine readable way [36], [37].

The use of regulation to preserve privacy has two main disadvantages. The first is that the penalty for noncompliance can be applied only after the privacy violation has occurred. The second disadvantage is that the regulation, and the appropriate penalty, is subject to interpretation. Furthermore Web users need to be aware of the existence of the laws and regulations, and the violation thereof. Moreover, the regulations are not global.

C. Technology

Many customers, once they become aware of the potential risks, make use of privacy-protecting software. Anti-virus, anti-spyware, firewall, spam and parental control products, from companies such as McAfee, Symantec and Trend Micro, which provide some level of protection against spyware and virus threats.

Some tools don't specifically protect either identity or information, but focus on raising the user's awareness of the organisation's policies so that they can make an informed decision about whether to entrust the organisation with their information, or not. For example, the "Privacy Bird" application allows the user to determine the extent to which their privacy is respected by a web site, according to the privacy policies of that web site [38], [39]. Such tools raise awareness but can easily be ignored. The need to protect privacy often conflicts with the need to achieve the goal of purchasing a particular product. When the user weighs up the loss of the purchase against a privacy intrusion that might not be realised, he or she is likely to ignore warnings and go ahead, especially if he or she is a pragmatist or unconcerned about privacy.

Other tools facilitate the protection of privacy. Tavani and Moor [40] explain that there are *privacy enhancing technologies (PETs)*, that can be used either to protect the identity of a person, or the informational content of messages. Examples of the former are Anonymizer[1] and Lucent Personal Web Assistant [41]. The latter are primarily communication tools, and not relevant to our application. The privacy issue, in the context of e-commerce is not that of concealing the person's identity completely. The person has to reveal his or her identity in order for their shopping to be paid for and delivered. What is required in this context is *limited* disclosure, and mediated trust between customers and the e-stores.

D. Summary

Each of the individual ART approaches works only partially. The best approach is therefore to use a three-pronged mechanism which utilises aspects of each of the ART techniques, as shown in Figure 1. Raising awareness (1,2,3) motivates the user to increase his or her knowledge of the regulations (4) and technologies (5) available with which to protect his or her privacy. In an ideal case, an aware customer would value his or her information, would decide when and under what circumstances to disclose it, and would know, if necessary, to place a trade-off value on the information. An aware person would exercise greater control and would be able to use technology to achieve this. Furthermore, by being aware of the existence and subject matter of the regulations in place, the customer would be more likely to understand the extent to which the information can be used or misused.

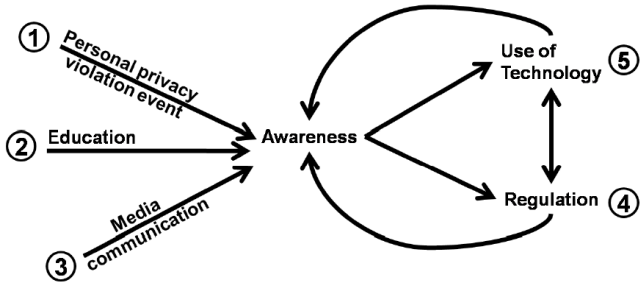

Fig. 1. The ART Approach [12]

However, such a customer would need to make a concerted effort to keep abreast of the latest technologies and regulations: a non-trivial task. The ART multi-faceted approach requires constant vigilance and up-to-date knowledge of regulation(laws) and available software. Therefore, anyone trying to use the ART approach in isolation faces a near-impossible challenge. However, a publicly available software tool, offered as a service, which incorporates elements of all these approaches *does* have the potential to provide an environment that incorporates the benefits of the ART approach with much of the effort being relegated to experts, where it belongs.

IV. A Privacy Preservation Approach

The purpose here is to provide a privacy-protective software tool which will give customers the opportunity to establish a secure identity and exercise as much control as desired over disclosure.

Figure 2 summarises the relationship between the technology system categories (privacy based), the control held by the customers, the privacy indices proposed by Westin in relation to the customer's willingness to embrace regulation, and finally regulation in open privacy regimen (where the firm has the right to collect and sell customer information including identity and purchasing habits) and closed privacy regimen (where customers have the right to remain anonymous) [42].

Customers using privacy invasive systems run bigger privacy risks than customers using privacy protective systems. We're proposing the use of a third party as mediator between the customer and the e-stores. The use of third-party mediators is common in security contexts: for example, websites offering

[1] www.anaonymizer.com

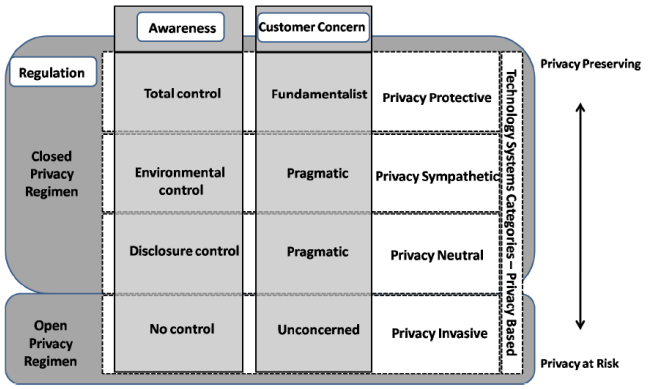

Fig. 2. ART & Privacy Perspectives [12]

services such as certificate authorities (eg. Verisign), third party payments (eg. Paypal) and pseudonymity [43].

We accordingly designed and implemented a *privacy preserving shopping environment* (PPSE) with the following components:

- a *third party website*, named Alter-Ego, whose objectives are to store, facilitate and mediate the customer's identity with the e-store. Alter-Ego stores the customers' preferences and sensitive personal information and facilitates the disclosure of information to participant stores. Using Alter-Ego, the customer is given the flexibility to:
  - decide what information will be sent to a participant store;
  - access an awareness zone where current privacy issues will be highlighted; and
  - have the opportunity to provide feedback about their experiences with signatory e-stores; providing ratings for the participant stores in order to regulate them.

  Alter-Ego makes a distinction between personal data, the information that can identify a living individual, and *sensitive* personal data, the information about the individual in areas such as religious beliefs, physical or mental health or condition, sexual orientation. Alter-Ego avoids the collection, use or storage of personal data (information that could lead to the participant's identification, such as name or address), limiting the collection of information to sensitive and preference data.
- an *agreement* between the e-store and the Alter-Ego, called the personal level agreement (PLA), which formalises the exchange of sensitive personal information and preferences between customer and e-store.
- a number of *signatory e-stores*, who undertake to respect the disclosure levels of the PLA.
- a *PPSE privacy policy*, which all participant stores agree and commit to comply with. This basic privacy policy is augmented by close monitoring of the participant stores' compliance.

We also implemented a signatory e-grocery store called *b-shop* to support evaluation of the PPSE. The PPSE integrates the three components of the ART privacy techniques as follows:

A. Awareness

The PPSE approach aims to raise customers' awareness by continual and updated presentation of information about privacy risks and methods of privacy protection. By making privacy awareness literature available to the customer, the PPSE aims to increase customer knowledge and give the customer the wherewithal to control their personal information. Raising customers' awareness enables them to make a conscious decision to protect their privacy and balance their choice of Web features, i.e. personalisation, against their need for privacy.

B. Regulation

Regulation is reinforced in the PPSE by encouraging customers to participate in the process by giving feedback and ranking their privacy-related experience while shopping with the participant stores. Customer feedback will be used by Alter-Ego to assist the close monitoring of the behaviour of participant stores, and achieve community regulation. Feedback given by the customers will affect e-stores' reputations and warn other customers about risks.

Ranking has been successfully used by companies such as eBay to assist buyers and sellers to build their own reputations. Resnick *et al.* [44], in his analysis of data from eBay, concluded that, under certain circumstances, the feedback net "makes up for the lack of traditional feedback mechanisms" (p23). A positive ranking in a reputation system, such as the one provided by eBay, has a beneficial effect on the sellers. Resnick *et al.* show that buyers were willing to pay, on average, 8% more to sellers with high positive feedback than to new sellers.

C. Technology: The Alter-Ego

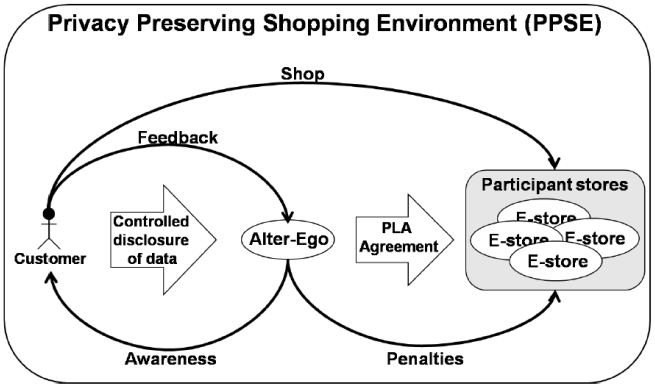

Fig. 3. The PPSE [12]

As Figure 3 shows, customers provide their information to the Alter-Ego website. This information *excludes* data that could be used to identify the client, i.e. name, address. Customers can disclose their sensitive personal information to the participant stores in a regulated way via the Alter-Ego using the PLA agreement. Having disclosed the desired

information, customers can do their shopping directly with the participant store. Figure 3 also shows the Alter-Ego raising awareness, customers giving feedback to assist the regulation process, and finally, penalties being applied to participant stores that do not comply with the privacy agreement.

The PPSE proposes a positive relationship between customer and e-store, by means of a privacy protective system, and an easy-to-use third party website, where the customer is given the flexibility to decide what information to disclose to each participant store. This flexibility, together with the confidence that the participant stores are compliant with the basic privacy policy defined in the PPSE, gives the customer the advantage of shopping while being reassured that the confidentiality of their data is being respected.

There is no need for customers to provide false information in order to protect themselves. Therefore, the information received via the Alter-Ego is expected to be more reliable than the information inferred from simple analysis of raw browsing data. Furthermore, stores that conform with the PPSE precepts would benefit from positive customer feedback, enhancing their reputation.

The Alter-Ego proposes using three levels of information disclosure according to the customer's privacy needs. The levels are low disclosure (bronze), medium disclosure (silver) and high disclosure (gold), and are linked to the amount of data that customers are willing to disclose to the e-commerce store. By providing customers with three different options, the three categories of customers in Westin's index could match their privacy perceptions and expectations and tailor their disclosure. The more data the customer discloses, the more customer data gathered by the store, and the more detailed the personalisation that can be provided by the store in return for the confidence shown by the customer. With detailed user-specified data, the store will have data to formulate a better market segmentation and the customer's privacy will be respected — so everyone wins.

1) Bronze: low disclosure level (for fundamentalists) — corresponds to anonymous access. At this level, anonymity is offered to customers who decide not to disclose any data. Customers can browse the store without revealing who they are. No information is collected that might link the user identity to their browsing activity. However, no customisation, personalisation or recommendations are offered.

2) Silver: medium disclosure level (for new pragmatists) — obtaining and communicating only preference data which can be used by the store to support their marketing strategies.

Preference data includes specific food preferences such as vegetables, fish, pork, which although apparently have no reference to the customer's privacy, have been found to have a link to certain attitudes and beliefs that customers might find embarrassing to share [45].

Customers are presented with five different categories to represent intensity of preference for each of the preferences. These non-ordinal categories provide a finer granularity in the disclosure of the customers' options. The intensity of preference categories are: always, sometimes, maybe, never, don't care.

3) Gold: high disclosure level (for confirmed pragmatists) — corresponds to sensitive information. The options provided to the customer are those that can be considered sensitive such as health issues or religious preferences and give a more detailed profile of the customer.

Customers can indicate the intensity of their preferences (using the granularity provided by the five intensity of preference categories for each of the options presented by the gold level) or introduce new elements to assist their shopping and these customers will receive better personalisation, adding dynamism and flexibility to their shopping experience.

This level supports disclosure of valuable data to support stores marketing purposes such as gender or age. Customers are presented with full personalisation and recommendations. This level allows the store to make use of previous purchases to offer recommendations. Finally, customers are permitted to access and amend the information the store holds about them.

D. Signatories

To qualify as a participant store in the PPSE environment, the store needs to agree to comply with the PLA agreement and the privacy policy defined by the PPSE. The participant stores would have to provide services to match the three Alter-Ego information disclosure levels and respect the associated confidentiality levels. The e-commerce store agrees to the following:

- The confidentiality of the customer's private data will be respected and the data provided will be used exclusively for their own marketing and business purposes.
- The information collected using this agreement will not be disclosed to other signatories or third parties.
- The information disclosed by the customer using the Alter-Ego, will be used to provide extra services, such as personalisation.
- Customers using the gold disclosure level will be allowed to view and amend the information held about them in relation to the preferences and sensitive information associated with them.
- Any contravention of the rules by the participant stores, found by the PPSE or reported by customers, will be investigated and penalised accordingly.

The customer commits to the following:

- To use the Alter-Ego third party mediator Web site for their shopping;
- To provide true preference information so that the store gains from being a signatory; and
- When ranking their privacy experience with the participant store, to provide objective and truthful feedback.

V. Evaluation

In order to evaluate the system a number of e-grocery shopping scenarios were designed to provide the context where the three privacy groupings (fundamentalists, pragmatic and unconcerned) [28] could shop for e-groceries. Participants did their shopping in a privacy protected environment (using the

PPSE) and in a non-privacy protected environment, supporting a comparison.

In order to avoid ethical issues, a persona ("rich description of typical user of the product under development" [46] (p481)) was used as the scenarios' principal actor. No credit card numbers were collected and the scenarios provided a fictitious address. Both scenarios introduced "Peter", a persona with certain privacy requirements due to health problems, and his need to purchase groceries according to a shopping list with elements that, if misused, could impact his personal privacy.

Since satisfaction and resulting customer loyalty were the main objectives of the evaluation, the definition of tasks had to be carefully designed so that effectiveness and efficiency could be kept constant, or at least not influence the comparison. To ensure this, participants were shown how to perform the tasks during a training session. After basic training, participants were given scenarios that contained lists of tasks to perform on behalf of "Peter". The experimental scenarios asked participants to perform tasks which involved the use of the Alter-Ego Web portal and b-shop:

1) *Alter-Ego Web portal:* 1: Registration; 2: Login; 3: Provide Peter's preferences and sensitive information; 4: Select the disclosure level; and 5: Select the participant store.
2) *b-shop:* 1: Select products from the scenario's shopping list; 2: Checkout; and 3: Introduce Peter's checkout details.

Participants were presented with a comparative context where privacy was either preserved or not. Participants were required to use and comment on both environments in a random way. The order of the use of the two environments was randomised. Two approaches were used: one with participants using the PPSE first and then the non-PPSE environment, and *vice versa*.

The evaluation of the PPSE required privacy violations to be explored. To achieve this, the participants were asked to fill in questionnaires before and after the tasks were completed. In addition, a message informing participants that the information was disclosed to selected third parties (including the NHS, Credit Bureau and Insurance Claims Database) was presented after they had shopped in the non-protected environment in order to gauge their reactions to this clear invasion of privacy.

A. Results

We evaluated our PPSE system with 41 users (46% were male). Analysis of the questionnaires presented before the tasks were undertaken in order to assess participants' reactions to various privacy violations in terms of *control over disclosure, control over body* and *boundary enforcement* showed that whereas they were particular about their privacy in terms of the first two, they were far more relaxed in terms of boundary settings — an invasion of privacy here was not perceived as negatively as the first two. Therefore, from this questionnaire it can be concluded that the participants privacy needs are, to certain extent, flexible in the setting of their privacy boundaries. Under certain circumstances, some of them would consider taking a risk, but they do not tolerate the loss of control, or misuse of, their information.

In terms of privacy perceptions there were no significant differences between the participants who used the PPSE first or second. An analysis of responses suggested that the majority of the participants belonged to the pragmatic category followed by fundamentalist and unconcerned in terms of *control over disclosure*. In terms of *control over body / personal information*, the majority of participants belonged to the pragmatic category, followed by fundamentalists and unconcerned. However, in terms of *the right to be left alone (set boundaries)* the majority group, pragmatic, was not followed by fundamentalists, but by the unconcerned. This shift in the distribution suggests that whether participants are conscious of their privacy needs and have a practical open-minded approach to privacy preserving mechanisms, they do not place the same importance when setting boundaries, and do not consider the interaction with others, and the delimitation of boundaries as vital as control over their information. These results prove that they placed differing values on the different aspects of privacy.

The message which reported that the data had been transferred to various third parties elicited extremely negative reactions from participants (even though it was the persona's data that was being reported and not their own). This outraged reaction to privacy violation shows that people do have an innate desire to protect their privacy and to exercise control over their information.

Participants reported (71% and 80%) increased privacy awareness and were satisfied that the PPSE environment would help them to control disclosure of their personal information. The majority of participants from both groups (81% and 95%) said they would recommend the use of the PPSE in case of customers with privacy needs.

The b-shop home page had a link to their privacy policy but none of the participants read it, confirming the findings of Vila *et al.* [47].

VI. Conclusion

Customers using privacy invasive e-commerce stores face a bigger privacy risk than customers using privacy protective systems. Those who are willing to use regulations to ensure their privacy (fundamentalist group) and using closed privacy regimen stores are much less at risk. A privacy-protective system was proposed in this paper which protects customer privacy by placing the customer within an environment with elements to facilitate a more controlled and regulated information disclosure.

With the existing privacy preserving approaches that use one or two of the ART techniques: awareness, regulation and use of technology. Customers are left with inadequate means of protecting their privacy, requiring continuous update in the use of emergent technology (such as cryptographical keys, or non-flexible negotiation such as Privacy Bird), and current legislation, making protecting their privacy a difficult task.

The proposed ART approach and the PPSE relieves the customer of this effort and allows them to exercise the level

of control in accordance with their particular risk perceptions. Evaluations with 41 participants demonstrated broad customer acceptance and increased awareness of privacy issues.

REFERENCES

[1] K. Foord, *Defining Privacy*. Victorian Law Reform Commission, 2000.

[2] S. D. Warren and L. D. Brandeis, "The right to privacy," *Harvard Law Review*, vol. 4, no. 5, 1890.

[3] M. Kennedy, "Coy village tells google street view 'spy' to beat a retreat," 3 April 2009, the Guardian. http://www.guardian.co.uk/technology/2009/apr/03/google-street-view-broughton.

[4] M. Taylor, "Pubs and police fall out over cctv in bars," 16 March 2009, http://www.guardian.co.uk/uk/2009/mar/16/pubs-police-cctv-in-bars.

[5] D. Raywood, "Government may be permitted to record personal activity on facebook and myspace," 26 March 2009.

[6] Princeton University, "Privacy," 2006, wordNet 3.0.

[7] D. Calcutt, "Report of the committee on provacy and related matters. chairman d calcutt," 1990, london: HMSO.(Cm 1102).

[8] Privacy and H. Rights, "Overview," 2007, web Document. http://www.privacyinternational.org/survey/phr2003/overview.htm.

[9] M. Fuchs, "State supreme court upholds privacy of bank records," 2 April 2009, new Jersey News. http://www.nj.com/news/ledger/jersey/index.ssf?/base/news-13/123864580462600.xml&coll=1.

[10] A. Travis, "Right to privacy broken by a quarter of uk's public databases, says report," 23 March 2009, http://www.guardian.co.uk/politics/2009/mar/23/dna-database-idcards-children-index.

[11] D. Derbyshire, "'privacy risk' of new mobiles that give away location and stored details to marketing firms," 3 April 2009, http://www.dailymail.co.uk/news/article-1166844/Privacy-risk-new-mobiles-away-location-stored-details-marketing-firms.html.

[12] D. C. Gálvez-Cruz, "An environment for protecting the privacy of e-shoppers," Ph.D. dissertation, Department of Computing Science, University of Glasgow, 2009.

[13] J. Alexander, "Confidentiality and privacy: what's the difference?" http://www.library.cmu.edu/ethics2.html, 2004, accessed 10 Sept 2006.

[14] L. F. Cranor, "'I didn't buy it for myself' privacy and ecommerce personalization," *Proceedings of the 2003 ACM workshop on Privacy in the electronic society*, 2003.

[15] J. Vogel, "Getting to know all about you," http://archive.salon.com/21st/feature/1998/10/14featureb.html, 1998, accessed 20/02/2007.

[16] What's News at JUNKBUSTERS, "Shoppers cards used against shoppers?" http://www.junkbusters.com/new.html Accessed 26 August 2008.

[17] U.S. Department of Commerce, "Quarterly Retail E-Commerce Sales 46^{th} Quarter 2007," http://www.census.gov/mrts/www/data/pdf/07Q4.pdf, accessed 27 May 2008.

[18] E. Morris, "Online customer experience: Will we get it right one day?" http://www.ecommercetimes.com/story/42274.html, 2005, accessed 29 June 2005.

[19] S. Spiekermann, J. Grossklags, and B. Berendt, "E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior," in *Electronic Commerce*. ACM, 2001. [Online]. Available: http://doi.acm.org/10.1145/501158.501163

[20] R. D. Newbold, *Newbold's Biometric Dictionary* . AuthorHouse, 2007.

[21] T. Espiner, "Government loses 3m learner drivers' details," December 2007, http://news.zdnet.co.uk/security/0,1000000189,39291581,00.htm.

[22] BBC News, "Uk's families put on fraud alert," November 2007, http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm.

[23] T. Lueng, "Hospital loses patient data again in less than a year," 25 March 2009, http://www.networkworld.com/news/2009/032509-hospital-loses-patient-data-again.html.

[24] T. Potter, "Council loses data on 3,000 people," 20 March 2009, http://www.eadt.co.uk/content/eadt/news/story.aspx?brand=EADOnline&category=News&tBrand=EADOnline&tCategory=xDefault&itemid=IPED19%20Mar%202009%2022%3A57%3A19%3A320.

[25] Electronic Privacy Information Center and Privacy International, "Privacy and Human Rights 2003: Overview," Accessed 23 Oct 2007 2003, http://www.privacyinternational.org/survey/phr2003/overview.htm.

[26] N. Olivero and P. Lunt, "Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control," *Journal of Economic Psychology*, vol. 25, no. 2, pp. 243 – 262, April 2004.

[27] C. Goodwin, "Privacy: Recognition of a consumer right," *Journal of Public Policy & Marketing*, vol. 10, no. 1, pp. 149–166, 18p, Spring91.

[28] A. Westin and Harris Louis Associates, "Harris-equifax consumer privacy survey," Tech. Rep., 1991, conducted for Equifax Inc. 1,255 adults of the U.S. public.

[29] H. Interactive, "Privacy on & off the internet: What consumers want," Tech. Rep., November 2001, conducted for Privacy & American Business, 1,529 interviewees. http://www.aicpa.org/download/webtrust/priv_rpt_21mar02.pdf.

[30] P. Kumaraguru and L. Cranor, "Privacy Indexes: A Survey of Westins Studies," *Institute for Software Research International*, 2005.

[31] S. Spanbauer, "Internet tips: Take charge of what web sites know about you," http://www.pcworld.com/article/id,124583/article.html\#, 2006, accessed 02 April 2006.

[32] D. M. Kristol, "HTTP Cookies: Standards, privacy, and politics," *ACM Transactions on Internet Technology (TOIT)*, vol. 1, no. 2, pp. 151–198, 2001.

[33] C. Wolf, *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age*. The Practising Law Institute PLI, 2006.

[34] L. J. Hoffman, "Computers and privacy: A survey," *ACM Computing Surveys (CSUR)*, vol. 1, 1969. [Online]. Available: http://doi.acm.org/10.1145/356546.356548

[35] Organisation For Economic Co-Operation And Development, "The economic and social impact of electronic commerce preliminary findings and research agenda," 1999.

[36] L. F. Cranor, B. Dobbs, S. Egelman, G. Hogben, J. Humphrey, M. Langheinrich, M. Marchiori, M. Presler-Marshall, J. Reagle, M. Schunter, D. A. Stampley, and R. Wenning, "The platform for privacy preferences 1.1 (p3p1.1) specification," http://www.w3.org/TR/2006/WD-P3P11-20060210/Overview.html, February 2006, accessed 11July2006.

[37] L Cranor and R Wenning, "Platform for Privacy Preferences (P3P) Project," http://www.w3.org/P3P/, accessed 28 July 2008.

[38] AT&T Corp, "Privacy bird ®," http://www.privacybird.org/, accessed 28 July 2007.

[39] L. F. Cranor, M. Arjula, and P. Guduru, "Use of a p3p user agent by early adopters," in *WPES '02: Proceedings of the 2002 ACM workshop on Privacy in the Electronic Society*. New York, NY, USA: ACM, 2002, pp. 1–10.

[40] H. T. Tavani and J. H. Moor, "Privacy protection, control of information and privacy-enhancing technologies," *Computers and Security*, vol. 31, no. 1, pp. 6–11, 2001.

[41] E. Gabber, P. B. Gibbons, D. M. Kristol, Y. Matias, and A. Mayer, "Consistent, yet autonomous, web access with LPWA," *Communications of the ACM*, vol. 42, no. 2, pp. 42–47, February 1999.

[42] C. R. Taylor, "Private Demands and Demands For Privacy: Dynamic Pricing and the Market for Customer Information," *SSRN eLibrary*, 2002.

[43] R. Martinez-Pelaez, J. Rico-Novella, V. Morales-Rocha, and M. Huerta, "Digital pseudonym identity card to create digital identities," *IADIS E-commerce*, pp. 313–318, 2006.

[44] P. Resnick, R. Zeckhauser, J. Swanson, and K. Lockwood, "The value of reputation on eBay: A controlled experiment," *Experimental Economics*, vol. 9, no. 2, pp. 79–101, 2006.

[45] M. C. Molina, H. Bettiol, M. A. Barbieri, A. A. M. Silva, S. I. O. C. J. E, and Dos-Santos, "Food consumption by young adults living in Ribeirão Preto, SP, 2002/2004," *Braz J Med Biol Res*, vol. 40, no. 9, pp. 1257–1266, 2007.

[46] H. Sharp, Y. Rogers, and J. Preece, *Interaction Design: Beyond Human Computer Interaction*. John Wiley & Sons, 2007.

[47] T. Vila, R. Greenstadt, and D. Molnar, "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*. New York, NY, USA: ACM Press, 2003, pp. 403–407.

978-1-4244-5494-5/10/$26.00 ©2010 IEEE