Designing Usable Online Privacy Mechanisms: What Can We Learn from Real World Behaviour?

Periambal L. Coopamootoo and Debi Ashenden

Department of Informatics & Systems Engineering,
School of Defence & Security,
Cranfield University,
Shrivenham, Swindon, UK, SN6 8LA
{p.coopamootoo,d.m.ashenden}@cranfield.ac.uk

Abstract. A variety of privacy mechanisms have been designed for the online environment but they have not been effective in ensuring end-users' privacy. In this study, we analyse existing privacy theories devised from offline socio-psychological studies and discuss which of those could be useful in the design of usable online privacy. We found that the Communication Privacy Management framework which provides boundary management processes could be used to design online privacy since it addresses information seeking, boundary rules formation, negotiation and means of addressing turbulence. We argue that since privacy is implicit within interpersonal and communication behaviour, a persuasive approach to designing online privacy could help to make privacy implicit within human-computer interactions, provide end-users with the ability to better engage with, and express their online privacy, and further ensure the usability of online privacy mechanisms.

Keywords: online privacy mechanisms, persuasive technology, privacy behaviours, usable privacy.

1 Introduction

Previous research aimed at understanding online privacy behaviour and its relation to privacy concerns has shown that although end-users claimed to have high privacy concerns, they behaved very differently online [1]. Several studies were performed to understand this discrepancy which was called the "privacy dichotomy". Among the possible explanations attributed to the phenomenon were the imbalance of information between end-users and service providers [2], the need for immediate gratification [3], behavioural biases, peer pressure to share information and the sharing of private information online to try out identities, for instance among young people [4]. Some research, however, has also claimed that online privacy approaches are too complicated for end-users to understand [5] and are not easy to use. In this paper we first explore the historical development of privacy as a concept and explain briefly the differences in privacy behaviour and the characteristics of private information shared online versus offline. We follow this with an exploration of the methodological approaches from sociology and psychology used to understand offline

S. Fischer-Hübner et al. (Eds.): Privacy and Identity 2010, IFIP AICT 352, pp. 311–324, 2011.

privacy behaviour. We compare and contrast this with the research carried out in the information systems field (in particular Human Computer Interaction (HCI)) to develop ways of designing usable privacy mechanisms for online environments. In the discussion section we aim to determine which approaches to understanding real world behaviours around privacy could assist in designing usable online privacy mechanisms. We conclude with recommendations for how a better understanding of interpersonal privacy interactions leads us towards taking a persuasive approach in order to develop effective privacy models before providing an analysis of a disclosure-privacy scenario.

2 Privacy Online versus Offline

In this section we explore the historical development of privacy as a concept and then compare the offline privacy mechanisms employed by individuals with the privacy mechanisms available online and the properties of private information shared offline versus online. Following the comparison, we briefly discuss the consequences those differences have on online privacy.

The first systematic, written discussion of the concept of privacy is said to have begun in 1890 with Warren and Brandeis' famous essay "The right to privacy" which cited political, social and economic changes which led to the recognition for the right to be let alone [6]. They argued that existing law afforded a way to protect the privacy of the individual; the privacy principle they believed was already part of the common law but that new technology, for instance photography and newspapers, made it important to explicitly and separately recognise this protection under the name of privacy. They thus laid the foundation for a concept of privacy that has come to be known as the control over information about oneself. However as explained by DeCew [7], it was only in the second half of the twentieth century that philosophical debates concerning definitions of privacy became prominent due to the development of privacy protection in the law.

In addition to this it has been argued that privacy and intimacy are deeply related. Fried [8] argues that privacy has intrinsic value and is necessarily related to, and fundamental to, one's development as an individual with a moral and social personality to be able to form intimate relationships involving respect, love, friendship and trust. Privacy is valuable because it allows one to maintain varying degrees of intimacy [8]. Gerstein [9] also supports the necessity of privacy for the intimacy which is required in communication and interpersonal relationships for a person to fully experience his or her life. Other researchers such as Rachels [10] expand the value of privacy to intimacy by emphasising the importance of developing diverse interpersonal relationships with others. Rachels' analysis emphasises that privacy is not only about limiting control of information but also access to oneself, both of which allows control over relationships with others, thus connecting privacy to one's behaviour and activities [10].

In more recent literature related to the advances in technology; privacy has been defined as the freedom from judgement [11-13], the ability to exercise privacy tradeoffs [12], the control over who has access to information, for what purpose it is needed and how sensitive the information is in a particular context [14]. Although the explicit impact of technology on privacy has been recognised since the arguments of

Warren et al. [6], there have been compelling arguments for overriding the privacy concerns for accountability and security needs [15].

This overview of the historical development of the concept of privacy demonstrates how legal support for privacy has come to the fore and the role of privacy as a key attribute in the development and maintenance of relationships. From a technological perspective, privacy has been depicted mainly as the control over one's private information and the ability to exercise privacy tradeoffs. It could therefore be useful to understand whether and how technology has catered for the legal and interpersonal aspects of privacy.

Privacy is required for communication and interpersonal relationships [9] and hence by extension required for the maintenance of an identity. It is embedded within the mechanisms of offline communication and participation and differs across societies where individuals socially manage their privacy with respect to others through an ongoing "boundary definition process" [16]. The mechanisms used offline are often implicit within the individual's behaviour in the form of non-verbal cues [17] including body language, oral and visual cues, accessories such as, for example, clothing, curtains and blinds, to avoid the release of information and achieve varying degrees of privacy or openness.

In the online environment, two different approaches are adopted to ensure the privacy of end-users. The regulation approach considers privacy to be a basic human right which requires protection whereas the self-regulation approach views privacy as a commodity which can be traded in the market place. While in the regulated approach, privacy is a must and although privacy mechanisms such as anonymity, pseudonymity and unlinkability technologies are provided, they are usually made explicit, are not often included within the system design and are hard for users to understand [18]. The self-regulation approach on the other hand assumes rational behaviour from online users in consenting to services in exchange for the release of personal information. This idea conflicts with research that looks at the biases and attributions that underpin the behaviour of individuals [1]. It is apparent from the above that both of these approaches cause difficulties for end-users and this may be a result of the difference between the protection offered by these online mechanisms and how individuals make decisions about privacy in the offline world. Thus while those approaches as implemented online aim to provide for the legal needs of privacy and for further protection of the shared information, they require rational and explicit privacy behaviour from the users. This type of behaviour can consequently make online privacy interactions seem impersonal, and make it hard for users to behave according to their concerns; that are often driven by the context of interpersonal relationships.

The different attributes of information in the online environment may further point us towards understanding some of the reasons for the privacy paradox. Certain types of personal information shared in an offline social environment may be considered to have a brief retention time since it often relies on human memory and is bounded within the context and associated human emotions [19]. In the online environment, however, information is persistent and is easily replicated due to the nature of the internet infrastructure. The consequences are that the information online can be easily taken out of context at a later time, flattened of its emotional value and made available for analysis and scrutiny by systems or people of which one might not be aware. The information might be given a different meaning and secondary information might be

inferred. These characteristics might also deny users of their rights to exercise control on their personal information in terms of who has access to it, when and how.

In the offline environment, individuals tend to share private information with a small number of individuals and generally tend to not broadcast it to the wider public audiences, while online broadcasting is much easier to accomplish and personal information is frequently broadcast to a large audience although the user may be sharing with a specific audience in mind [20]. The sharing of one's personal information is also usually done by the individual or others close to the individual which differs from the online scenario where personal information is more easily accessible and can potentially be shared by anyone with access to it. For this reason the properties of online data and its transmission affect the very nature of private information and hence no longer cater for the intimacy required for communication and interpersonal relationships [10].

To summarise, while offline, privacy is implicitly linked to individual behaviour and communication and the building, development and maintenance of relationships; online it is explicitly designed and dependent on human-computer interactions. Privacy is provided by the online system and hence privacy online is constrained by the technology. Moreover, while privacy has a contextual or situational value, the personal information gathered and stored online may be deprived of its context. A lack of awareness of the properties of information online and of the consequences results in users making a poor risk assessment and unknowingly trading off privacy. The asymmetry of information transmission may also cause ambiguity and assumption of privacy where users might believe their interactions happen within a safe system within their computer system in their physical space, thus explaining the privacy paradox.

3 Methodological Approaches to Understanding Privacy Offline versus Online Design

In this section, we briefly explore the social-psychological theories of privacy that laid the foundation for further studies and some extensions that have built on those theories through conceptual studies, systematic analysis and empirical studies. We then review the approaches used to design privacy online and discuss how they cater for the social aspect of privacy and the characteristics of offline privacy behaviour and of private information shared.

3.1 Foundational Social-Psychological Privacy Theories

Westin and Altman's theoretical contributions to the understanding of the social-psychological aspects of privacy have stood the test of time and provide a firm foundation for other researchers to build on [21; 22]. Westin's theory highlights the ways in which individuals protect themselves by temporarily limiting access to themselves by others [21]. Since privacy allows individuals, groups or institutions to determine when, how and to what extent their information is communicated to others, it is viewed in relation to social participation and is the voluntary and temporary withdrawal of an individual or group through physical or psychological means.

Westin describes privacy as being a dynamic and non-monotonic process which is also neither self-sufficient nor an end in itself.

According to Westin's theory, privacy has four states which can be thought of as privacy mechanisms, that is, the means through which privacy is maintained. These states are solitude, intimacy, anonymity and reserve. He also posits four functions or goals of privacy. These are personal autonomy, emotional release, self-evaluation, and limited and protected communication [21]. Empirical research, such as the factor analysis undertaken by Pederson [23], not only found support for Westin's states but also tested the relationship between the states and functions of privacy. While describing his results as coherent and inclusive, he proposes a 6 x 5 'types of privacy x privacy functions' model [23] which provides the link between the types of privacy behaviour individuals exhibit and the functions or goals of these.

Altman [22] on the other hand places social interactions at the heart of his theory, with the environment providing mechanisms for regulating privacy. While for Altman also, privacy is the selective control of access to the self, he also identifies privacy to be a temporal and dynamic process of interpersonal boundary control. This is the process through which individuals regulate interactions with others where privacy has both a desired and actual level and privacy is non-monotonic, bidirectional and applies at the individual and group level. Altman also provides a range of privacy mechanisms for privacy regulation, such as the verbal content of communications, territorial behaviour to enable separation of personal space from others and cultural norms. He goes on to suggest that privacy should be considered as a social process, and that an in-depth psychological study of the aspects of privacy must include the interplay of people, their social world and the physical environment.

Two important extensions of Altman's regulation theory are based on the linkage of privacy and disclosure [24]; these build on Altman's dialectical conception of privacy as a process of opening and closing a boundary to others. Petronio [25] proposes a conceptual and theoretical framework in her articulation of Communication Privacy Management (CPM), arguing that individuals depend on a rule-based boundary system when deciding whether to disclose private information. Central to Petronio's approach is the need to strike a balance between the positive opportunities to interact with others, made possible by technology, and the dangers of losing the means to control and regulate access to one by others. The rules are used to balance revealing and concealing private information - that is disclosure and privacy. These rules are dynamic since they can change, grow or remain stable for periods. Derlega & Chaikin [26] on the other hand extend Altman's boundary concept to a dual boundary model while exploring its applicability to information privacy. They suggest that individuals function within a dyadic boundary that is perceived as a safe zone within which they disclose to invited others or across which disclosure does not pass [26].

Newell [27] performed a systematic classification of past privacy studies across a variety of disciplines and proposed a framework which extends from both Westin's and Altman's theories. She classifies past studies into person-centred, place-centred and interaction perspectives. Within the interaction perspective, privacy is an attitude, a behaviour, a goal or a process. Privacy as behaviour includes choice, control, boundary regulation, interaction management and information management [27] since privacy presupposes the existence of others, the opportunity of interactions with them and the ability to control this interaction.

From the above overview of socio-psychological studies, interpersonal communication through a process of boundary control within behaviour is highlighted as prerequisite to the development and maintenance of relationships. This corresponds with Gerstein [9] and Rachels' [10] ideas outlined earlier around the necessity of privacy for communication and the development of interpersonal relationships.

3.2 Approaches to Designing Online Privacy

We can see that the design of privacy into online systems had its roots in the legal need to protect end-users from the threat of misuse of their personal data and for them to provide an informed consent to its further processing or sharing. Thus privacy policies were implemented as liability shields for businesses and are often long texts that are too legalistic and complicated for end-users to read and understand. In response to this some research has looked at the design of privacy policy plug-ins or user agents [28] that allow end-users to select their preferences and make it easier for them to be alerted when a website does not comply with their preferences. This, however, has to be set a priori to interactions and does not form part of the human-computer interaction during the online experience (for example, in ecommerce transactions or online social networking). Other kinds of plug-ins devised have tried to minimise the collection of profiling information which end-users might not be aware of such as browser filtering or cookie removers. Primelife has also worked towards enhancing the transparency of policies through the 'Creative Commons' type layered approach to privacy [29]. Whilst needing to overcome the challenges listed by Hansen (2010), this is an important work in progress towards enhancing end-users' understanding of their privacy online.

There are also tools and research initiatives that look at embedded access control mechanisms which provide users with the technological functionality of controlling access to themselves and provide them with feedback for the control applied. Examples of this are the fine-grained access controls of Facebook and the user-controlled privacy research carried out by Cornwell et al. [30]. A few steps further and we find user-centric identity management systems that provide users with control of the private details they share and therefore their online identity. The Prime project for instance has analysed and translated legal principles into HCI requirements which were further supplemented by social needs [31]. They extend the privacy policy user-agent by allowing end-users to express their policy preference regarding data disclosure as well as negotiate it with the service provider. The negotiated policy is attached to the data shared and a data track feature can provide the end-users with a comprehensive report of their history of data sharing and of the policies attached to the disclosures [32].

4 Discussion

As reviewed above, studies for the design of online privacy have concentrated on providing technological solutions for the legal needs of privacy while working towards making it usable and providing some control to the end-user. Projects such as Primelife [32] also provide for policy negotiation and reporting facilities which might be more helpful for certain types of end-users to manage their privacy. While this approach

provides the technological solution for further control, and feedback mechanisms about information shared online and hence one's identity, it does not consider privacy as an implicit process within interpersonal communications which is an essential component of privacy and disclosure behaviours and of how one manages one's identity. Moreover, privacy in this approach is made explicit and adds additional steps to be performed during the online experience. Making privacy an additional task during online interactions, although enhancing trust in the service provider could make it cumbersome to use the service and make online communication less natural which undermines the aim of social features embedded within online systems. The aim is to persuade end-users of the interpersonal aspect of human-computer interactions in order to enhance online participation - a large proportion of which includes the disclosure of private information.

Newell [27] suggested more than a decade ago that the vagueness and ambiguity in the definition and representation of privacy could be resolved and wide support obtained if privacy was viewed as an interactive condition of the person and the environment. Pederson's [23] states versus functions matrix (adapted from Westin [21]) might help to design mechanisms if the privacy goals are known. Moreover, while Pederson's matrix is highly valuable for securing the link between the types or means of privacy and the functions or goals of privacy, it is at a high level and cannot be practically applied to interaction design. An application of the matrix will require further research to ensure the concepts can be translated into online interaction design requirements.

Petronio's Communication Privacy Management (CPM) framework [25] on the other hand has been used to understand how people decide to disclose private information in offline settings and also to understand and address the tension between disclosure and privacy by examining how and why people decide to reveal or conceal private information within the ecommerce context [33]. CPM is also a practical framework which can more easily be used to assess online systems although there are fundamental differences between the nature of offline and online environments. CPM is a rule-based theory proposing that individuals develop rules to aid decisions about whether to reveal or conceal information, the rules developed help people maximise the benefits while minimising the risks of disclosure and are a function of the context and disclosure goals.

The theory proposes three iterative processes for boundary management [25]. The first process, boundary rule formation includes the seeking of information and rules development to regulate when and under what circumstances people will reveal rather than withhold personal information whereas the second process, boundary coordination refers to the negotiation of privacy rules between parties through the setting and maintenance of boundary linkages, boundary ownership rights and boundary permeability. The third process, boundary turbulence might result from differences in privacy rules between parties, privacy rule violations or deficient boundary coordination. Boundary turbulence refers to the dynamic process of maintaining and negotiating boundaries to manage personal disclosures.

The different CPM processes could cater for the properties of privacy identified above. For instance, CPM caters for the dynamic and temporal nature of privacy through the coordination and turbulence recovery processes and for bidirectional flow of information through the information seeking and negotiation processes. In addition,

despite the fact that the internet causes persistency of data, a CPM approach to online privacy would allow the user to be to some extent in control of the lifespan of the private information shared according to the coordinated and negotiated boundary. Also, the CPM approach would mean that the user would have control over the audience to which his or her private details are broadcasted.

The processes of the CPM, that is, boundary rule formation, coordination and turbulence are however, dependent on the interaction mechanisms employed within the online environment which can be highly persuasive in favouring rules that minimise the apparent effects of risks and maximise benefits of sharing personal details. Information technology is never neutral but always influences users' attitudes and/or behaviour in one way or another [34]. Moreover, privacy is embedded within human behaviour and communication while expression and persuasion is a big part of communication. Hence persuasion is important for expressive privacy which relates to the social and communication dimension of privacy and encompasses an individual's ability and effort to control social contacts [22]. Thus to enable end-users to express their privacy through human-computer interactions and for service providers to be better able to convey details of information processing, a persuasive approach could be useful. Direct persuasion approaches such as rational arguments or indirect approaches such as simple cues could allow end-users to be in a better position to communicate and participate online while maintaining their privacy. Privacy behaviour for instance, consists of boundary regulation while enjoying social interactions without negatively affecting oneself or the other party. Furthermore, since individuals want to be private and do not explicitly perform privacy decisions at every instant their privacy behaviour is implicit. But in online interfaces privacy mechanisms are made explicit and mostly kept away from the interaction paths. It seems very relevant then to suggest that a persuasive approach could also cater for the implicitness property of privacy behaviour within human-computer interaction and consequently enhance the usability of the online privacy mechanisms.

5 The Persuasive CPM

In this section we first introduce persuasive systems and propose the persuasive CPM approach as a means to enhance usability of privacy online. We then evaluate a disclosure-privacy scenario with respect to the CPM stages in an attempt to identify the boundary rules that can be formed with the current interaction design and to understand whether the design caters for privacy as a communication process.

5.1 Persuasive Systems

Persuasive systems are 'computerised software or information system designed to reinforce, shape or change attitudes or behaviours or both without using coercion or deception' [35]. Such systems employ persuasive techniques that are designed to enable compliance, change behaviour or attitudes and that rely on the voluntary participation of end-users [36]. Studies have shown that human beings have an innate privacy need and hence attitudes to privacy. Since end-users already have a privacy attitude, we suggest employing persuasive techniques to influence behaviour. Hence, the context of the persuasive topic tackled by this paper and research is online privacy behaviour change for adopted, or learnt disclosure behaviour, privacy reinforcement

for those privacy behaviours that are already present but hard to maintain and sustain and the shaping of new privacy behaviours.

A persuasive system design approach [37] though quite a recently developed approach can be used to direct the analysis of systems requiring persuasive strategies and the selection of specific persuasive principles that can be used to achieve specific goals, in different contexts. Persuasive design principles [37] can provide for primary task support, human-computer dialogue support, perceived system credibility and social influence.

5.2 The Proposed Persuasive CPM

In Figure 1 below we propose a persuasive CPM for usable online privacy. The persuasive CPM model is a preliminary adaptation of CPM with persuasive techniques selected for each process of privacy boundary management using the four categories of persuasive systems principles of the persuasive system design approach of Oinas-Kukkonen & Harjumaa [37].

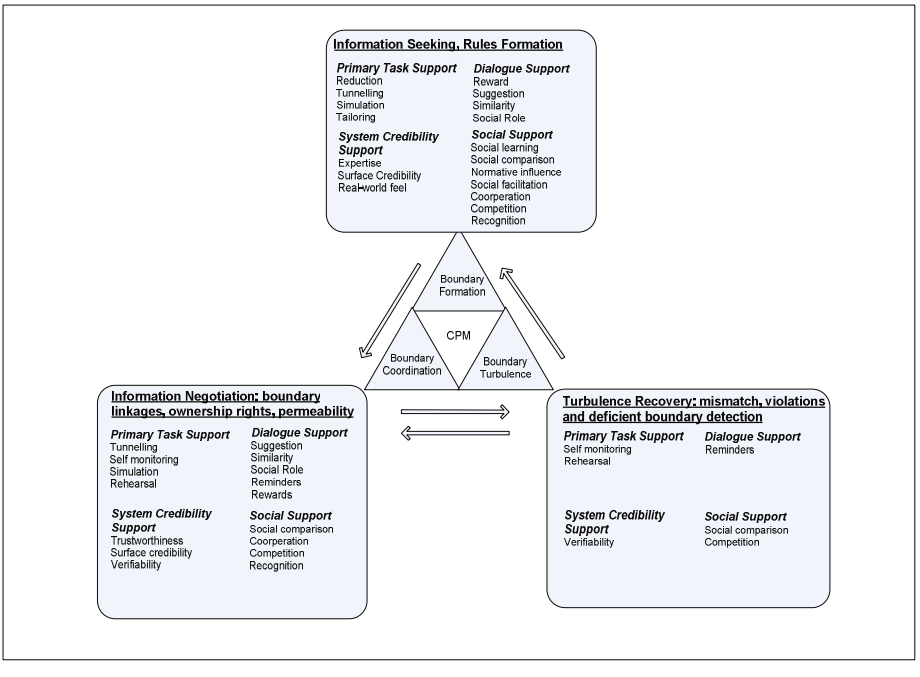

Fig. 1. The persuasive CPM – a preliminary diagram based on Petronio's CPM [25] and Oinas-Kukkonen & Harjumaa's persuasive system design approach [37]

For each stage of the CPM we propose a set of persuasive principles that have the potential of enhancing usability of privacy interactions. For instance, for boundary formation, information is sought and new rules are formed or existing rules are acquired. Hence, the persuasive principles listed in Figure 1 for boundary formation

could facilitate communication to make the end-user aware of the type of boundaries being formed, to help decide on the type of privacy rules and also help facilitate the process of setting these rules.

While this model still needs to be subjected to rigorous analysis and testing, we can already advance that this persuasive CPM approach could cater for the transparency need of privacy and also help towards providing the ability, motivation and trigger to end-users to exercise their right of control over their private information.

5.3 Analysis of a Disclosure-Privacy Scenario with Respect to the CPM and the Persuasive System Design Principles

We analysed the profile creation of Amazon UK in an attempt to understand how interactions within this scenario have been designed with respect to disclosure and privacy using the CPM processes. We explored the scenario to understand how information can be sought, what boundary rules can be formed, how they are coordinated and negotiated and how turbulence can be resolved. We then identified persuasive principles used within this scenario that would favour disclosure and privacy.

While the first two criteria of rule formation, culture and gender are not affected by the interaction design, the design can however contribute to other criteria of rule formation such as motivation, context and risk-benefit ratio awareness. Moreover, the boundaries coordinated during disclosure-privacy can be inclusive, intersected or unified. In order to identify the type of boundary that can be formed within the scenario, we look for the possibility of coordinating boundaries that is by forming linkage, ownership and permeability rules. For each of the different types of boundaries, different linkages and ownership rules can be coordinated. For instance, within inclusive boundaries, role, coercive or susceptibility linkages and manipulative, benevolent or obligatory ownerships occur. Within intersected boundaries, the linkages are goal or identity linkages, and both parties share responsibility of ownership.

Findings. The interface does not provide explicit information to notify or explain that entering personal data will result in a dyadic boundary nor is the risk of disclosure highlighted. On the other hand, it motivates the end-user to disclose using the words ‘share’ and ‘friends’. Thus, the end-user might not realise that he or she is disclosing information to the service provider rather than still being within his or her personal boundary. In fact, the creation of a profile involves a dyadic boundary formation, where the criteria used to trigger boundary rule formation includes context (type of products bought), motivation and benefits - apart from culture and gender. The rules formed within this dyadic boundary are also acquired by the end-user without his or her awareness. Since there are no disclosure warnings and rules cannot be negotiated, the end-user has to accept pre-existing rules set by the service provider.

As the end-user goes through a process of boundary appropriation by appropriating an already defined and set boundary and without having been provided with information about the type of boundary being formed, the coordinated boundary is inclusive. In this type of boundary coordination in the current scenario, the linkages formed can be either coercive or role linkages. In this case it is coercive linkage since the end-user is not made aware that he or she is leaving the personal boundary to form

a dyadic boundary during the interactions of profile creation. If the end-user was aware of this it would be the result of prior experience and the boundary linkage within this inclusive coordination would be role linkages. Role linkages refer to linkages formed with the service provider who takes control of the information disclosed by the end-user due to the former's role of providing services that requires disclosure from the part of the end-user. In both cases, the end-user does not know who else might be linked and have access to this new boundary.

The type of boundary ownership formed is either manipulative or obligatory. That is the service provider manipulates the end-user into disclosing while not making the end-user aware that a dyadic boundary is being formed and that control of ownership of information shared has been lost. The ownership could also be obligatory if the end-user can understand that he or she has left his personal boundary but is obliged to disclose and give up ownership in order to benefit from services. Hence the end-user is not given any control over how the disclosed information can be distributed. Profile creation in this scenario precludes editing and the visibility of the profile is automatically set to 'public'. The profile creation page does not lead immediately to profile editing meaning that one would not know how the profile is visible.

We also identified the persuasive techniques that are present within the interaction design and the table below provides the identified list from each of the four categories of persuasive system design principles that favours disclosure.

Table 1. Persuasive techniques used to favour disclosure

Primary task support	**System Credibility Support**
Reduction: 'It's easy! Just choose a public name for Your Profile.' Self-monitoring: 'Your profile contains information about you and your Amazon activities such as your Wish List and reviews you've written.' Suggestion: of a name in the textbox Personalisation: personalised suggested name. Tunnelling: by providing a text box to write a name and a yellow button to create profile.	Trustworthiness: trustworthy since it is Amazon (widely used) and says 'If you are not X, click here'. Surface credibility: the interface/website looks and feels competent; there are for instance no adverts.
Dialogue Support	**Social Support**
Rewards: 'Your Profile is a one-stop place for your friends and other people to find you and learn more about you.'	Normative influence: 'Connect with friends and other Amazon customers.'

For persuasive techniques that could favour privacy; there is a link at the bottom of the page in very small print. Clicking on the link reveals a page of text that provides for reduction since the text is divided into sections. However the text within the separate sections is condensed and would probably not encourage reading.

This analysis has allowed us to identify the linkages and ownership rules that could be coordinated within the current scenario and the type of boundary that could be

formed. We also found that the interactions designed within this scenario fail to provide for the boundary management processes of the CPM. We identified some persuasive system design principles that could favour disclosure but only one that would favour privacy. It would be valuable to find out whether the addition of persuasive principles for privacy (via the boundary management process of the CPM) would enhance privacy usability online.

6 Conclusion and Future Work

In this paper we have discussed the differences between offline and online privacy. The online and offline environments differ fundamentally in a way that causes a difference in the properties of the private details shared. We explored social-psychological theories of privacy and highlighted that privacy is intertwined with communication and interpersonal relationships. We then suggested an approach through which offline privacy behaviour could to some extent be replicated online, that is by using Petronio's [25] privacy boundary management theory. We proposed a persuasive Communication Privacy Management (CPM) as a means for end-users to be better able to express, and communicate, and hence engage, with their privacy online and analysed a disclosure-privacy scenario with respect to the CPM. The proposed approach has not yet been tested but paves the way for research which considers the changing, reinforcing and shaping of online privacy behaviour through enhancement of human-computer privacy interactions which will lead to usable online privacy. The next step for the research is to analyse other scenarios of online privacy mechanisms added and embedded within systems with respect to the CPM framework and then analyse their persuasiveness according to the persuasive system design approach. We will then perform empirical usability studies with an aim to explore the effect of a persuasive CPM approach on the usability of privacy mechanisms.

References

1. Acquisti, A., Grossklags, J.: Losses, Gains, Hyperbolic discounting: an experimental approach to information security attitudes and behaviour. In: 2nd Annual Workshop on Economics and Information Security - WEIS 2003, May 29-30, University of Maryland (2003)
2. Spiekermann, S., Grossklags, J., Berendt, B.: E-privacy in 2nd Generation E-commerce: Privacy preferences versus actual behaviour. In: 3rd ACM Conference on Electronic Commerce, Tampa, Florida, USA, October 14-17, pp. 38–47. ACM, New York (2001)
3. Acquisti, A.: Privacy in electronic commerce and the economics of immediate gratification. In: 5th ACM Conference on Electronic Commerce, May 17-20, pp. 21–29. ACM, New York (2004)
4. boyd, d.: Why youth love social network sites; The role of networked publics in teenage social life. In: Buckingham, D. (ed.) MacArthur Foundation Series on Digital Learning - Youth, Identity and Digital Media, p. 119. The MIT Press, Cambridge (2007)
5. Cranor, L., McDonald, A., Reeder, R., Gage Kelley, P.: A Comparative Study of Online Privacy Policies and Formats. In: Goldberg, I., Atallah, M.J. (eds.) PETS 2009. LNCS, vol. 5672, pp. 37–55. Springer, Heidelberg (2009)

6. Warren, S.D., Brandeis, L.: The right to privacy. Harvard Law Review 4, 193–220 (1890)
7. DeCew, J.: Privacy. In: Zalta, E.N. (ed.) The Stanford Encyclopedia of Philosophy (Fall 2008), http://plato.stanford.edu/archives/fall2008/entries/privacy
8. Fried, C.: An Anatomy of Values: Problems of personal and social choice. Harvard University Press, Cambridge (1970)
9. Gerstein, R.: Intimacy and Privacy. Ethics 89, 76–81 (1978)
10. Rachels, R.: Why Privacy is important? Philosophy of Public Affairs 4, 323–333 (1975)
11. Itrona, L.D., Pouloudi, A.: Privacy in the Information Age: Stakeholders, Interests and Values. Journal of Business Ethics 22(1), 27–38 (1999)
12. Adams, A., Sasse, M.A.: Privacy issues in ubiquitous multimedia environments: wake sleeping dogs, or let them lie? In: Sasse, M.A., Johnson, C. (eds.) Seventh IFIP Conference on Human-Computer Interaction INTERACT 1999. Edinburgh Conference Centre, August 30-September 3. IOS Press, Riccarton (1999)
13. Strater, K., Richter, H.: Examining privacy and disclosure in a social networking community. In: 3rd Symposium on Usable Privacy and Security, July 18-20, vol. 229, pp. 157–158. ACM, New York (2007)
14. Adams, A., Sasse, M.A.: Taming the wolf in sheeps clothing: Privacy in multimedia communications. In: Seventh ACM International Conference on Multimedia, Orlando, Florida, United States, October 30 - November 05, pp. 101–107. ACM, New York (1999)
15. Swire, P.: Privacy and Information Sharing in the War on Terrorism. Villanova Law Review 51, 101–129 (2006)
16. Palen, L., Dourish, P.: "Unpacking" privacy for a networked world. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Ft. Lauderdale, Florida, USA, p. 126. ACM, NY (2003)
17. Patterson, M.L., Mullens, S., Romano, J.: Compensatory reactions to spatial intention. Sociometry 34, 114–121 (1971)
18. Zwick, Dholakia, N.: Models of privacy in the Digital Age: Implications for Marketing and E-commerce (unpublished Paper), Research Institute for Telecommunications and Information Marketing, RITIM, University of Rhode Island (1999)
19. Blanchette, J., Johnson, D.G.: Data retention and the panoptic Society: The social benefits of forgetfulness. The Information society 18(1), 33–45 (2002)
20. Richter-Lipford, H., Besmer, A., Watson, J.: Understanding Privacy settings in facebook with an audience view. In: Churchill, E., Dhamija, R. (eds.) Proceedings of the 1st Conference on Usability, Psychology, and Security, San Francisco, California, April 14, pp. 1–8. USENIX Association, Berkeley (2008)
21. Westin, A.: Privacy and Freedom. Athenum (1967)
22. Altman, I.: The Environment and Social Behaviour: Privacy, Personal Space, Territory and Crowding. Brooks/Cole Publishing, Monterey, California (1975)
23. Pedersen, P.M.: Models for types of privacy by privacy functions. Journal of Environmental Psychology 19(4), 397–405 (1999)
24. Margulis, S.T.: On the status and collaboration of Westins's and Altman's Theories of Privacy. Journal of Social Issues 59(2), 411–429 (2003)
25. Petronio, S.: Boundaries of privacy: dialectics of disclosure. State University of New York Press, Albany (2002)
26. Derlega, V.J., Chaikin, A.L.: Privacy and self-disclosure in social relationships. Journal of Social Issues 33(3), 102–115 (1977)
27. Newell, P.B.: Perspectives on Privacy. Journal of Environmental Psychology 15(2), 87–104 (1995)

28. Cranor, L., Guguru, P., Arjula, M.: User interfaces for privacy agents. ACM Trans. Computer-Human Interaction 13, 135–176 (2006)
29. Hansen, M.: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Holstenstr. 98, 24103 Kiel, Putting privacy pictograms into practice: a european perspective (2010), http://subs.emis.de/LNI/Proceedings/Proceedings154/gi-proc-154-134.pdf
30. Cornwell, J., Fette, I., Hsieh, G., Prabaker, M., Rao, J., Tang, K., Vaniea, K., Bauer, L., Cranor, L., Hong, J., McLaren, B., Reiter, M., Sadeh, N.: User-controllable security and privacy for pervasive computing. In: Eighth IEEE Workshop on Mobile Computing Systems and Applications, HOTMOBILE, March 08-09, pp. 14–19. IEEE Computer Society, Washington DC (2007)
31. PRIME WP06.1, HCI Guidelines, D06.1.f (2008), https://www.prime-project.eu/prime_products/reports/arch/pub_del_D06.1.f_ec_wp06.1_v1_final.pdf
32. Leenes, R.E.: User-Centric Identity Management as an indispensable tool for privacy protection. International Journal of Intellectual Property Management 2(4), 345–371 (2008)
33. Metzger, M.: Communication Privacy Management in Electronic Commerce. Journal of Computer-Mediated Communication 12(2) (2007), http://jcmc.indiana.edu/vol12/issue2/metzger.html (June 2010)
34. Oinas-Kukkonen, H., Harjumaa, M.: Persuasive system design: key issues, process model and system features. Communications of the Association of Information Systems 24, 485–500 (2009)
35. Oinas-Kukkonen, H., Harjumaa, M.: Towards deeper understanding of persuasion in software and information systems. In: First International Conference on Advances in Computer-Human Interaction, Sainte Luce, Martinique, ACHI, February 10-15, pp. 200–205. IEEE Computer Society, Washington, DC (2008)
36. Oinas-Kukkonen, H.: Behaviour change support systems: a research model and agenda. In: Ploug, T., Hassle, P., Oinas-Kukkonen, H. (eds.) 5th International Conference, Persuasive 2010, pp. 4–14. Springer, Heidelberg (2010)
37. Oinas-Kukkonen, H., Harjumaa, M.: A Systematic Framework for Designing and Evaluating Persuasive Systems. In: Oinas-Kukkonen, H., Hasle, P., Harjumaa, M., Segerståhl, K., Øhrstrøm, P. (eds.) PERSUASIVE 2008. LNCS, vol. 5033, pp. 164–176. Springer, Heidelberg (2008)