CRANFIELD UNIVERSITY

COOPAMOOTOO Periambal Lutcheemee

EFFECTIVE ONLINE PRIVACY MECHANISMS WITH PERSUASIVE COMMUNICATION

CRANFIELD DEFENCE AND SECURITY

PHD THESIS

Academic Year 2012-2013

Supervisor: ASHENDEN Debi

January 2013

This thesis is submitted in partial fulfilment of the requirements for the degree of

Doctor of Philosophy

Abstract

This thesis contributes to research by taking a social psychological perspective to managing privacy online. The thesis proposes to support the effort to form a mental model that is required to evaluate a context with regards to privacy attitudes or to ease the effort by biasing activation of privacy attitudes. Privacy being a behavioural concept, the human-computer interaction design plays a major role in supporting and contributing to end users' ability to manage their privacy online. However, unless privacy attitudes are activated or made accessible, end users' behaviour would not necessarily match their attitudes. This perspective contributes to explaining why online privacy mechanisms have long been found to be in-effective.

Privacy academics and practitioners are queried for their opinions on aspects of usable privacy designs. Evaluation of existing privacy mechanisms (social network service, internet browsers privacy tabs and E-Commerce websites) for privacy experts' requirements reveals that the privacy mechanisms do not provide for the social psychological processes of privacy management. This is determined through communication breakdowns within the interaction design and the lack of privacy-disclosure dialectical tension, lack of disclosure context and visibility of privacy means.

The thesis taps into established research in social psychology related to the attitude-behaviour relationship. It proposes persuasive communication to support the privacy management process that is to enable end user control of their privacy while ensuring typical usability criteria such as minimum effort and ease of use. An experimental user study within an E-Commerce context provides evidence that in the presence of persuasive triggers that support the disclosure and privacy dialectic within a context of disclosure; end users can engage in privacy behaviour that match their privacy concerns. Reminders for privacy actions with a message that is personally relevant or has a privacy argument result in significantly more privacy behaviour than a simple reminder. However, reminders with an attractive source that is not linked with privacy can distract end users from privacy behaviour such that the observed response

is similar to the simple reminder. This finding is significant for the research space since it supports the use of persuasive communication within human-computer interaction of privacy designs as a powerful tool in enabling attitude activation and accessibility such that cognitive evaluation of an attitude object can be unleashed and end users can have a higher likelihood of responding with privacy behaviour. It also supports the view that privacy designs that do not consider their interaction with privacy attitudes or their influence on behaviour can turn out to be in-effective although found to support the typical usability criteria.

More research into the social-psychological aspects of online privacy management would be beneficial to the research space. Further research could determine the strength of activated or accessed privacy attitude caused by particular persuasive triggers and the extent of privacy behaviour. Longitudinal studies could also be useful to better understand online privacy behaviour and help designs of more effective and usable online privacy.

Acknowledgements

I would first and foremost like to thank my supervisor, Debi Ashenden, for recruiting me for this journey. Her guidance, support and motivation were invaluable for this work and kept me going. My thanks also to Annie Maddison for her help at the crucial end. Thanks to my thesis committee members, Prof. Peter Hill and Philip Nobles. To all the VOME project members with whom I shared discussions about the area and Conn Crawford for his help during the user studies, thank you. Thanks to Trevor Ringrose and Marie Cahillane for their advice.

Special thanks to all my friends and family across the miles who shared many highs and lows and continue to make me a better person. Thanks to my parents, Batma and Soondren Coopamootoo, and my elder brother, Teerooven, who are my foundation, for their wisdom, generosity and strength.

Finally, I would like dedicate this work to my sister, Teeroona, and my younger brother, Kumaran, who are my inspiration. Thanks for their unwavering belief, support and love.

Table of Contents

Figures

Tables

Chapter 1:

Introduction

1.1 Introduction

The research within this thesis formed part of a UK-based multidisciplinary research project called Visualisation and Other Methods of Expression (VOME) whose overall aim has been to devise better means to engage end users in managing their privacy online and to help them towards making informed consent decisions (VOMEa, 2012). This thesis addresses the problem of ensuring usable online privacy mechanisms. It starts by exploring the theoretical criteria of usable online privacy, designs a methodological approach that balances the weaknesses of individual research methods and determines the actual usability criteria. This is followed by identification of usability weaknesses in existing privacy designs. The thesis then proceeds to present an approach aimed at clearing the identified weaknesses.

This chapter provides an overall depiction of the thesis. It first defines key concepts used throughout the context of the thesis. The research problem is then presented followed by a discussion of the scope of the thesis. The chapter proceeds with the research approach and a roadmap of the thesis and ends with a summary of the research contributions.

1.2 Definitions

Several key concepts are used throughout the thesis. Some are defined in literature in a variety of ways and others were derived from these definitions for the purpose of the current research. This section presents the definitions and points to the section of the thesis that provides further reviews and explains the selection and formulation of the definitions for each of these concepts.

Attitude (reviewed in section 3.3.2): An attitude is a learned, global evaluation of an object (person, place or issue) that influences thought and action (Perloff 2010a, pp 43). Attitudes can be viewed as an association between the object and the evaluation (Fazio, 1989).

Privacy (reviewed in section 2.3): Privacy is a human right (Council of Europe, 1950). It also relates to the control of access to the self (Altman, 1975) including information about the self (Belloti and Sellen, 1993; Dourish, 1993).

Privacy attitude: Privacy attitude is consequently a learned or global evaluation of a person, context or situation that influences thought and privacy behaviour.

Availability of attitudes (discussed in section 3.3.2): An attitude is said to be available if it exists within a person's cognitive structure that is the person possesses the attitude due to prior association and evaluation with an object (Fazio, 1989).

Attitude activation (discussed in section 3.3.2): Attitudes are activated (associated with an object) when individuals categorise some experience in terms of the attitudes (Fazio, 1989). Multiple attitudes become connected through experiences of co-activation. Privacy attitudes are therefore activated during interaction with a person or situation or environment and the experience is categorised as an instance requiring control of access to the self.

Attitude accessibility (discussed in section 3.3.2): Attitude accessibility is related to the ease with which a particular attitude (an available attitude) may be retrieved from memory (Fazio, 1989). The accessibility of the attitude is affected by the strength of

the attitude and aspects of the context that serve to highlight particular attitudes as being relevant to that context. Strong attitudes are more accessible.

Strong attitude (discussed in section 3.3.2): An attitude is strong if there is a consistent, well-rehearsed link between an attitude object and its evaluation (Augoustinos et al., 2006); therefore individuals have a strong privacy attitude if they consistently evaluate a context of disclosure as requiring privacy protection. Such individuals correspond to Westin's description of privacy fundamentalists (Kumaraguru and Cranor, 2005).

Behaviour (defined in section 3.3.2): Behaviour is what people do and involves their actions (Miltenberger, 2011).

Online privacy mechanisms (discussed in section 2.2.3): Online privacy mechanisms refer to both standalone privacy tools added to systems or embedded privacy designed within systems.

Effectiveness of online privacy mechanism (defined in section 2.4.1 and discussed in 2.3 and 2.4): ISO 9241-11 defines usability in terms of enabling end users to achieve a set of goals with effectiveness, efficiency and satisfaction (ISO, 1998). An online privacy mechanism is effective if it enables end users to take privacy actions that match their attitudes.

1.3 The research problem and thesis scope

Privacy is a human right (Council of Europe, 1950). It is also a behavioural concept that relates to interactions within an environment (Rachels, 1975; Gerstein, 1978) and as such the environment both determines privacy behaviour and is influenced by behaviour. Privacy can therefore be described as a socio-psychological process that is embedded within and supports interpersonal interactions and communication (Margulis, 2003). However privacy is tacit in nature and cannot be easily described by end users (VOME, 2012b). It also depends on the context of disclosure (Joinson and Paine, 2007). Privacy is consequently a dynamic process (Altman, 1975; Palen

and Dourish, 2003) such that the extent of privacy protection relies on the value attributed to the disclosed information at a point in time.

Technology has taken privacy to previously uncharted territory. Technology has become so omnipresent that sharing and disclosing personal information online is common. Privacy issues that emanate from online disclosure extend into real world consequences (Solove, 2006; Detica and Cabinet Office, 2011). Therefore end users' privacy needs are at a tension with organisations' requirements to collect personal information. Organisations however have a legal requirement of ensuring end users' privacy protection (European Parliament, 1995; UK Government, 1998). Online privacy mechanisms have been designed to support these requirements. It was however found that although end users have privacy concerns, their online behaviour do not match these concerns (Spiekermann et al., 2001; Acquisti and Grossklags, 2005a). This discrepancy has been attributed to end users' psychological dispositions (Acquisti, 2004; Strandburg, 2005) and limitations within online designs (Milne and Culnan, 2004; Jensen and Potts, 2004). Previous research has proposed better visualisation methods, approaches of presenting information to enhance readability and performance and ways of aiding privacy task completion (Cranor et al., 2006; Richter-Lipford et al., 2008; McDonald et al., 2009; Kelley et al., 2009; Richter-Lipford et al., 2010). However, these approaches might not be sufficient in ensuring end users can use privacy mechanisms according to their concerns (privacy goals) that is in ensuring effectiveness of online privacy mechanisms.

In addition, although enhancements were proposed and usability was evaluated through different criteria depending on the aspect of human-computer interaction under investigation, the requirements for usable online privacy were not determined first to guide evaluation. Such an approach would direct evaluation of privacy as an interactional process embedded within a context of disclosure. This would better help to identify weaknesses within systems that contribute to in-effective privacy mechanisms.

Furthermore, although seamless privacy management is considered as a socio-psychological process offline, it is not known whether online designs support such a

process. The nature of the online environment and the privacy consequences that can emanate spread beyond end users' mental pictures during disclosure (Strater and Richter, 2007). Given that privacy is an interactional process, the human-computer interaction design is at centre stage in supporting end users' mental model of privacy during online interactions. Also, attitude-behaviour discrepancies have been the subject of much debate and research since many decades (LaPierre, 1934; Campbell, 1963; Schuman and Johnson, 1976; Ajzen and Fishbein, 1977; Regan and Fazio, 1977; Sivacek and Crano, 1982; Stiff and Mongeau, 2003; Ajzen and Fishbein, 2005). It is believed that attitudes can predict behaviour and that the observed relationship is dependent on strength and accessibility of attitudes (Fazio and Williams, 1986) and consistency of the measures of attitude and behaviour (Campbell, 1963; Ajzen and Fishbein, 1977; Ajzen and Fishbein, 2005).

Therefore the research within the thesis revisits concepts and findings from previous research in social psychology in an attempt to influence the online privacy attitude-behaviour relationship through persuasive communication. In doing so, it proposes an innovative approach of ensuring effectiveness of online privacy mechanisms through a better human-computer communication approach that guides and enables the reflection of the privacy attitude construct in memory into behaviour. It also demonstrates whether existing privacy designs provide the processes of privacy management. The thesis is designed to answer the following three research questions:

- RQ1: What are the requirements for usable online privacy mechanisms?
- RQ2: How usable are existing online privacy mechanisms?
- RQ3: How does persuasive communication impact the effectiveness of online privacy mechanisms?

This research is innovative in proposing to guide behaviour from attitudes as a means of enhancing effectiveness of online designs since such an approach has not been used within the online privacy domain before. The thesis will specifically help designers assess and enhance the privacy management processes of their designs. It will also help businesses in ensuring their privacy protection practice supports end users. Such

support would consequently help end users to discern between those service providers who genuinely protect their privacy and those who don't.

The research focuses on the behavioural and interactional aspects of privacy online and hence does not go in depth into the legal and technological side. The research does not propose new technological solutions or tools for managing privacy but proposes a method for enhancing the interaction designs of existing privacy mechanisms. This method can be applied to any form of privacy designs and even to designs for other purposes such as security, health and energy conservation.

The research also only evaluates the effectiveness aspect of usability. This is because research on effectiveness of privacy is important since, as shown by the definition of effective online privacy mechanisms in section 1.2, it determines whether privacy designs enable end users to manage their privacy according to their attitudes and goals. However, other aspects of usability can also contribute to effectiveness and could be addressed in future research.

1.4 The research approach

The research was undertaken within a mixed method approach that was guided by a social science perspective. It employed human-computer interactions (HCI) research methods since a key pillar of the research is usability. It first explored the requirements for usable online privacy design by querying privacy experts. It then evaluated privacy designs of three types of online systems. This was followed by an experimental user study that determined the influence of persuasive communication in activating end users' attitudes.

A Delphi approach was used that enabled a multidisciplinary group of privacy experts to iteratively review their opinion of the requirements of design that would ensure usability. The Delphi approach in this research space is innovative in providing the structure to enable legal, technological, psychological and HCI privacy experts to propose opinions and to reach consensus on the complex issue of usability of privacy.

Analytical HCI techniques were used to determine whether online privacy designs provided for the social-psychological processes of privacy management. A real world theoretical framework guided the evaluation.

After reflecting on the social-psychological implications of the relationship between attitudes and behaviour, the influence of persuasive communication in influencing that relationship was addressed. This was enabled through a user study that simulated an E-Commerce shopping task.

1.5 The thesis overview

Figure 1 below (in the next page) portrays the overall framework that guided the different sections of the research and the thesis breakdown within this framework. It essentially consists of two sections: an inductive part and a deductive part. The inductive part is an exploration that contributes to establishing the theoretical criteria of the real world problem of ensuring end users' privacy online, defining the research gap and research problem, designing methodology to address the research gap, identifying the real criteria and evaluating existing online privacy designs for weaknesses in supporting the criteria. This is followed by a deductive experimental part that assesses the influence of the proposed approach that provides the criteria and addresses the weaknesses.

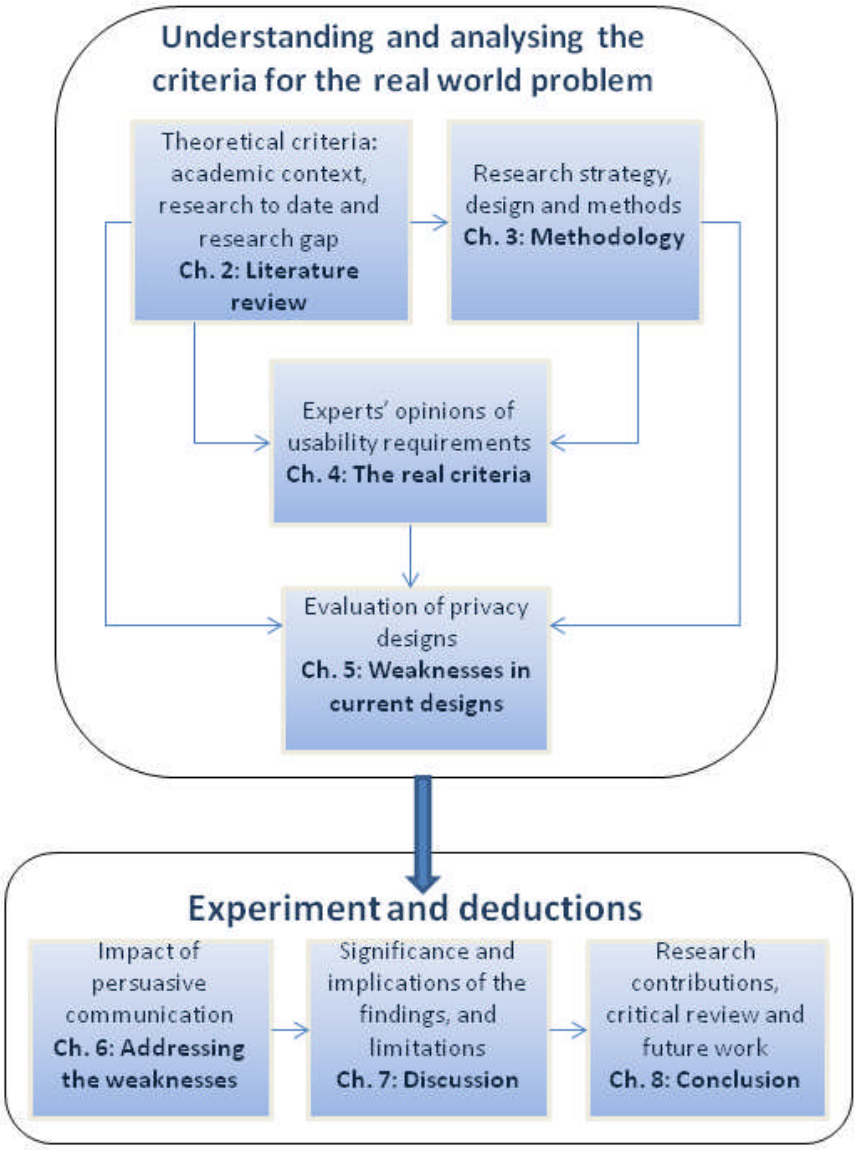


Figure 1: Map of the thesis

The literature review in Chapter 2 theoretically explores the real world problem of ensuring end user privacy online. It presents the social, organisational and technological components of the real world problem. It then reviews the academic context and research conducted to date in the research space. It focuses on the three pillars of this research which are: privacy, usability and persuasive communication. Chapter 2 concludes by discussing the research gap and articulating the research problem.

In Chapter 3, the methodology is elaborated by first restating the research questions followed by an articulation of the research strategy and the philosophical foundations. The chapter then describes the research design with a reflection on the validity of the design. It follows with a list of the data collection and analysis techniques that were used to answer the research questions.

The real criteria for usable online privacy were determined in Chapter 4 by querying privacy experts in a Delphi study. The Delphi approach was chosen to allow experts from various privacy research and practice areas to contribute their differing point of views and to enable a discussion among them through iterative feedback. The Delphi stages are detailed starting with the preparation phase followed by three rounds of design and analysis.

The thesis then proceeded to evaluate existing online privacy mechanisms for the requirements suggested by privacy experts and to identify HCI weaknesses in the design of privacy that would affect the effectiveness of online privacy. Chapter 5 starts with a pilot study and is followed by an evaluation of the ease of use of Facebook. Since weaknesses were identified in the approach, a more rigorous approach of evaluating online designs for usability was conducted on internet browsers' privacy tabs and E-Commerce websites' notice and choice function.

Following the exploratory part of understanding the criteria for usability of online privacy and analysing existing systems for vulnerabilities in supporting privacy interaction, a user experiment was conducted as described in Chapter 6. The aim of the user study was to find out whether persuasive communication affects the effectiveness and usability of online privacy mechanisms. Chapter 7 provides a general discussion for the research including the significance and limitations of the findings and Chapter 8 concludes the thesis.

1.6 The research contributions

An important contribution to the research space is the finding that contrary to conclusions of previous research (such as Spiekermann et al., 2001; Acquisti and Grossklags, 2005a), privacy fundamentalists do take more privacy behaviour than

privacy unconcerned as expected from their privacy attitudes. Privacy behaviour is affected by persuasive communication such that the framing of the messages within the design can either distract end users and result in poor privacy behaviour or have not much to do with privacy but still bias towards privacy behaviour or serve as the argument that strengthens privacy behaviour. This contribution portrays a gap in research – better understanding of the socio-psychological process of online privacy management and the interaction of design components with this process and the outcome of the interaction in future research would be beneficial for the research space. It also means that existing design that has not taken the psychological impact of their design components on privacy attitude and behaviour into account cannot ensure that their privacy designs will be effective.

The thesis also reviews the theoretical criteria of the real world problem of ensuring end user privacy online and comes up with a description of research gap and design of methods that would contribute to research on more usable online privacy. Another contribution of the thesis is a list of the requirements for usable online privacy designs from a multidisciplinary standpoint produced by querying privacy experts. This helped to pin down the main components of design that would contribute to usable privacy mechanisms and to guide the rest of the research. The key requirements included end user control, privacy to run in parallel to system services, privacy to require minimum user effort and easy to use systems. Experts stressed on the complexity and challenge of designing usable online privacy which supports and explains the findings of the literature review that is online privacy designs suffer from a large amount of usability issues. To address the challenge, the experts suggested a list of ways that can help to provide for the conflicting requirements of end user control and minimum effort in balance with system services and advised on carefully considering the context of use during design.

The research also found that privacy mechanisms are not consistent in their communication of privacy information that could help end users to manage their privacy as effectively as they are used to offline. Privacy mechanisms are either not accessible within the context of use or the disclosure link is missing. Privacy mechanisms hence do not provide the processes to support end users' privacy

management. This contribution is important because it sheds some light on why existing privacy designs are not effective for managing privacy. The lack of support to the disclosure context or the availability of privacy mechanisms would make it tricky for end users to cognitively evaluate their private-public boundary hence rendering the availability of the privacy mechanisms not useful in enabling end users to manage their boundaries. It would also be difficult for end users to associate their available privacy attitudes with an imaginary disclosure context.

Chapter 2:

Literature Review

2.1 Introduction

The literature review begins by introducing a real world problem that arises from conflicting requirements: the need for end users to disclose personal information so as to benefit from online services and end users' requirement for privacy protection. The variety of privacy mechanisms that is available online and that caters for the tension is then introduced. The second part of the literature review looks at the academic foundation of this real world problem and reviews the research to date that addresses the problem while focusing on privacy behaviour and privacy designs. The first pillar is an exploration of privacy scholarship. The substantive contributions and methodological contributions are also provided. Since a prerequisite of successful information systems is effective human computer interactions, the second pillar is usability. However, because of the need to ensure business models that depend on disclosure are not disrupted and the need to accommodate different types of end users, the third pillar of the academic and research to date review is persuasive technology. The last section of the literature review elaborates on the research gap that can be discerned, that is on the need to look at the human computer interactions design of privacy from a social-psychological communications perspective and the benefit of influence strategies such as persuasive technology.

2.2 Real World Problem

The internet has revolutionised the way business is conducted. It has provided powerful new ways to locate, learn about, and buy all types of products and services (Norris et al., 2000). It has also dramatically changed the way people communicate and has consequently enabled the creation of new virtual structures such as virtual social communities (Bargh & McKenna, 2004).

During the process of using communication technology to interact and acquire services online, content is often created and personal information is disclosed. This makes end users vulnerable to risks such as the loss of personal information, privacy intrusion, identity theft and fraud and becoming the target of behavioural marketing. As a result there is a need to protect end users' personal information when they engage online.

The requirement of protecting end users' privacy is however at a tension with the business requirements of collecting and processing personal information that support the provision of competitive services to end users. Online privacy protection therefore has a social, organisational and technological dimension. In the next sub-sections, these dimensions are reviewed and discussed.

2.2.1 Social

This section discusses the social implications of the lack of privacy protections. These include exposure to identity theft and fraud, misrepresentation of information and loss of control over personal information.

Individuals disclose a large amount of personal information online to enable the creation and management of online identities that support online transactions and online social life. While the maintenance of an online identity provides a lot of benefits to end users such as complementing and facilitating traditional social communication (Birnie and Horvath, 2002), a major problem for end users is not being able to judge the extent of activity and accessibility of their online identities (Strater and Richter, 2007). This might be mainly because online disclosure differs from offline disclosure. 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 as found by Richter-Lipford et al. (2008). The sharing of one's personal information is also usually done by the individual or others close to the individual and 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 (Rachels, 1975). The situation also makes it easy for third parties to create digital dossiers of their end users' behaviour exposing them to physical and cyber risks. The consequence of cyber crimes to end users can be very costly. This is shown by the cost of cyber crime to UK citizens, as stated by the Detica's E-Crime report (2011), which is thought to be £3.1 billion per annum. These cyber crimes include identity theft, online scams, scareware and fake antivirus (Detica and Cabinet Office, 2011).

Another social implication that develops due to the characteristics of the online environment is the retention time of personal information. In the offline social environment, personal information 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. 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 to the unawareness of end users be made available to systems or people for analysis and scrutiny. 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.

The use of online social interactions can also lead to an acceptance to be socially pressured to conform into relinquishing control of access over information about oneself and the control of access to oneself as discussed in Gross and Acquisti (2005).

This can result into a redefinition of personal space which might create conflict in offline life relationships. The later have to continuously adapt with the online persona or identity.

To summarise, providing for end users' privacy protection would have social benefits. It has the potential to relieve the risks of cyber crime, to ensure end users' online content are protected from distortion and to maintain end user control and avoid conflicts with offline identity.

2.2.2 Organisational

This section discusses the organisational implications of collecting and processing personal information. These include the threat of cyber attacks, loss of customer trust in the organisations' services and breach of legal requirements.

Some organisations need to collect, process, store and manage customer information much of which involves personal information in order to provide quality services to customers. These include customised and personalised services. The potential privacy problems that can arise from the different stages of personal information manipulation activities have been outlined by Solove's (2006) taxonomy. For instance, information collection can result in surveillance. Information processing can cause aggregation of data by linking different personal information. This would make it easy to identify individuals from their online interactions, with the potential to cause insecurity and exclusion. Information dissemination harms could include breach of confidentiality, disclosure, exposure and increased accessibility. Organisations that manipulate customer information are consequently an attractive target for cyber attacks. It has in fact been shown in Detica's Cyber E-Crime report that the loss or theft of customer data costs UK businesses up to £1 billion per year (Detica and Cabinet Office, 2011).

In addition to the financial implications, data breaches including the loss or mismanagement of customer data also contributes to end users' uneasiness when engaging in transactions that involve the release of personal information and reduces their trust in the service provider (Velmurugan, 2009). With regards to trust, the lack of understanding and control of the technology provided by service providers and

used to share personal information also contributes to a loss of trust and a negative emotional reaction to the use of the technology (Adams and Sasse, 1999). There is consequently a need for organisations to counteract privacy issues before they arise, to solve them before people lose their trust and reject technology and services from the service provider. Furthermore, end users might not be able to differentiate between organisations that ensure the protection of their privacy versus those that do not. They instead base their selection on the presence of security or privacy cues (Jensen et al., 2005) that do not actually have much bearing on the service providers' management of end users' personal information (Miyazaki and Krishnamurthy, 2002).

Moreover, privacy is a human right in Europe and it is a legal requirement to ensure end users' privacy (Council of Europe, 1950). The UK Government's Data Protection Act (1998) which was intended to bring the UK in line with the European Parliament's Electronic Commerce Directive (1995) aims to define UK law for all parties involved in the processing of data on identifiable living people and provides a way for individuals to control information about themselves. The Act defines eight principles to which service providers involved in collection, processing and usage of personal information must comply. The Privacy Impact Assessment (PIA) has also been proposed by the Information Commissioner's Office of the UK to assess compliance to the Data Protection Act that is organisations' privacy risks in the collection, use and disclosure of personal information (Information Commissioner's Office, 2009). As a result, privacy protection of end users is tightly linked with the needs of the organisation to comply with privacy regulations. To ensure compliance, organisations strive towards obtaining end users' consent. However, for consent to be fair, it has to be informed consent that is achieved when fully informed end users participate in decisions about their personal data. Informed consent

> 'originates from the legal and ethical right the user has to direct what happens to his information, and from the ethical duty of the organisation using personal data to involve the user in the control, use and maintenance of these data' (Van der Geest et al., 2005).

To summarise, organisations that collect and process personal information are at risk of cyber attacks. Cyber attacks and other data breaches can result in damaged reputation and loss of customer trust. In addition, since organisations deal with

personal information, they have to comply with privacy regulations. To do so, they have to provide for informed consent. This leads to the next section that is the means employed by organisations to inform end users of personal information processing and of tools that are useful for ensuring their privacy.

2.2.3 Technological

While each of the activities that information systems perform with personal information such as data transfer, data storage and data processing can raise privacy concerns, their impact on privacy varies on how they are performed, what type of data is involved and who uses the data. As discussed in the previous section, the businesses that operate these information systems have to abide by legal requirements to ensure protection of end users' personal information. To do so they design privacy mechanisms into the systems. This section discusses the ways of ensuring end users' privacy protection through technological designs. It highlights how the designs are used and their effectiveness.

Privacy mechanisms can be added to or embedded to online systems making those systems privacy-friendly systems and the mechanisms privacy-enhancing technologies (PETs) (Van Blarkom et al., 2003). PET is the umbrella term for hardware and software mechanisms that not only ensure compliance with privacy regulations but is also believed to provide more flexible ways for people to protect their privacy (Enterprise Privacy Group, 2008). Privacy mechanisms can support end users as part of their overall strategy to manage the risks involved in disclosing personal information.

Privacy-friendly systems can be divided into two types of systems that depend on the type of privacy engineering approach used. They are either privacy-by-policy systems or privacy-by-architecture systems (Spiekermann and Cranor, 2009). Privacy-by-policy systems focus on the implementation of notice and choice principles of the European Directive on Electronic Commerce, the UK Data Protection Act or the Fair Information Principles standard of the US. This means that notice should be provided in the form of at least some information about the service collecting personal information, how these will be used, potential recipients, ways by

which the information is collected, whether disclosure by end users is voluntary or required and the measures taken by the service provider to ensure protection of end users' personal information (Federal Trade Commission, 2000). In addition, they have to provide end users with the choice of what and how to disclose (Federal Trade Commission, 2000). On the other hand, privacy-by-architecture systems minimise collection of identifiable personal information and emphasise on anonymity and client-side data storage and processing. Therefore, by definition, systems that rely on privacy-by-policy ought to integrate notice, choice and access mechanisms in order to ensure end users are aware of privacy risks and offer choices that enable control over their personal information whereas privacy-by architecture systems ought to ensure profiles cannot be linked with a reasonable or automated effort.

The privacy-by-policy approach has been adopted by many businesses since it does not interfere with their current business models that rely extensively on personal information. They do so by providing terms of agreement and privacy policies to which end users ought to agree in order to benefit from a provided service. Privacy notices are used for compliance purposes and as a result are designed as exhaustive legal texts and are not accessible or informative to consumers (Milne and Culnan, 2004). They have been said to be "inadequate tools" (Cate, 2010, pp 59) for managing privacy online. As quoted in Cate (2010), the Federal Trade Commission, explains that

> "Notice and choice don't provide intrinsic privacy protection, although they might serve other purposes. Consequently, they've become at worst a substitute for more meaningful privacy protections." (Cate, 2010, pp.60-61)

Since it has been recognised that it is hard to ensure end users can exercise control over their information solely through privacy policies of service providers, development of software or hardware that enable this control has been encouraged. Platform for Privacy Preferences (P3P) is a standard developed by World Wide Web Consortium designed to provide internet users with a clear understanding of how personal information will be used by a particular website (W3C, 2007). It is based on privacy preferences set on the website and how they compare with the end user's own privacy preferences. While P3P version 1.0 provided insufficient support to end

users' evaluation of a site's policy, AT&T Corp. designed a tool, Privacy Bird (AT & T Corp., 2006) that reads P3P policies and displays them in an understandable language. The tool partly addressed the issue by allowing end users to specify their own privacy preferences, compares them with a website's P3P-encoded privacy policy when end users visit the website and alerts them when the policy does not meet their standards. A few browsers also allow end users to specify certain limited privacy preferences and compare them with the P3P policies of visited websites. For instance, Internet Explorer allows end users to initially state few privacy preferences and blocks cookies from sites that do not adhere to these preferences. However, these software systems require end users to make privacy decisions a-priori, without regard to specific circumstances in a particular context.

Privacy-by-architecture mechanisms on the other hand do not involve policies but instead take a technological approach to ensure privacy through anonymity and pseudonymity tools (Spiekermann and Cranor, 2009). Anonymity of end users means that they cannot be identified or tracked online. This approach has been used in anonymous email remailers such as in Babel (Gulcu and Tsudik, 1996) and anonymous web browsing tools such as Anonymizer (Anonymizer, 2012). Anonymizer is a web proxy that strips off identifying headers and source addresses from the web browser. Another approach is "onion routing" which is built upon the notion of "mix network" (Chaum, 1982). A mix network is essentially a chain of proxy servers (called mixes). In onion routing, a message or packet is encrypted to each mix node using public key cryptography. The resulting encryption is similar to a layered "onion" with the original message in the innermost layer. As the message traverses over the network, each mix node strips off its own layer of encryption to reveal where to send the message next. For example, Tor (Tor Inc., 2012), a concrete onion routing system can provide anonymous communication such as web browsing, remote login sessions, instant messaging and other applications that rely on the TCP protocol. Another approach is centred on the concept of "k-anonymity" (Sweeney, 2002). It is concerned with a practical problem of releasing data about individuals without revealing identifying information about them. In a k-anonymized release,

each individual's record is indistinguishable from at least k-1 other individuals' records.

Since end users need to be authenticated to gain access to certain systems, identity management solutions can help to ensure their privacy. Authentication seeks to ensure that end users are actually the person they claim to be and this is usually achieved by employing a username in combination with a password, where the username is considered as the digital identity of end users and the password as their authentication. A more sophisticated, and thus more secure, scheme is two-factor authentication, which involves two independent ways for verifying identity. It may include a user having something (e.g., a bank ATM card or a time dependent token card) and the user knowing something (e.g., a PIN). One of the goals of emerging identity management systems is to allow end users to have more than one digital identity and be able to freely choose which identity to use. An industry example is Microsoft's CardSpace (Chappell, 2006), an "identity metasystem" that allows end users to create multiple virtual identity cards. Each virtual card created by end users contains the minimum amount of information (retrieved from an identity provider) that they need to divulge to carry out the transaction to which the card applies. CardSpace thereby uses the metaphor of the various cards that are used to identify individuals in the physical world, such as business cards, driver's licenses and credit cards. With these virtual cards, end users no longer have to worry about daunting passwords. The problem with these mechanisms is that end users need to manage a number of identities and their authentication factors.

OpenID is an open specification of a truly distributed identity system (Cross, 2008). OpenID providers are essentially authentication brokers between end users and OpenID enabled websites. They allow end users to log into an OpenID supported website without registration. End users' passwords and other credentials are safely stored by OpenID. Because of its open and distributed nature, ease of use, and easy adoption for websites, OpenID is gaining more and more momentum. However because of the use of a single login, it suffers from single point of failure.

Anonymizers and identity management attend to concerns such as improper monitoring and improper use by observing identity principles (e.g., pseudonymity) but not data principles such as notice/access and choice/consent. They also take control away from end users. However, although some privacy designs, such as those designed in social network services, enable end user control, they remain remotely used.

This section showed that although privacy mechanisms are designed online, they might not be accessible to end users and consequently not usable in ensuring end users can manage their privacy. In the following sections, the literature review first explores the two main themes of the real world problem: privacy and usability and then reviews the research's proposed enhancement approach: persuasive technology.

2.3 Privacy

As elaborated in the real world section above, it can be seen that the main focus of this literature review is about privacy. In this section of the literature review, the academic context of privacy is presented followed by an exploration of research to date that aimed to ensure end users' privacy.

2.3.1 Privacy in an academic context

This section explores the historic, philosophical, political, social and legal roots of privacy. It shows that the use of the term privacy is not uniform and there remains to date confusion over the meaning, value and scope of the concept of privacy.

Although there are several sceptical and critical accounts of privacy (Thomson, 1975; Posner, 1981; MacKinnon, 1989; Bork, 1990) mostly taking a reductionist approach to the concept of privacy claiming that privacy is not a concept on its own but rather part of other conceptual systems, most theorists such as Schoeman (1984) take the 'coherentist' view that privacy is a meaningful and valuable concept whose characteristics have emanated through a variety of cases. The systematic written discussion of the concept of privacy is said to have begun in 1890 with Warren and Brandeis' (1890) famous essay "The right to privacy" which cited political, social and

economic changes that led to a recognition for the right to be let alone. They argued that existing law afforded a way to protect the privacy of the individual. They believed the privacy principle 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 (Warren and Brandeis, 1890; Schoeman, 1984). They thus laid the foundation for a concept of privacy that has come to be known as the control over information about oneself. However 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 Privacy Act of 1974 (Buckley, 1974).

Westin endorsed the value of privacy as the control over information by describing privacy as the ability to determine for oneself when, how and to what extent information about one is communicated to others (Westin, 1967). Bloustein (1964) also supported Warren et al.'s position on the need for a general theory of individual privacy that reconciles its divergent strands. It defines one's essence as a human being and it includes individual dignity and integrity, personal autonomy and independence. A more common view however has been to argue that privacy and intimacy are related. Fried (1970) argued 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 he argued because it allows one to maintain varying degrees of intimacy (Fried, 1970). Gerstein (1978) also supported the necessity of privacy for intimacy which is required in communication and interpersonal relationships for one to fully experience his life. Schoeman (1984) endorsed these views and stressed that privacy provides a way to control intimate information about oneself that has many other benefits, not only for relationships with others, but also for the development of one's personality and inner self. Other researchers such as Rachels (1975) expanded the value of privacy to intimacy by emphasising the importance of developing diverse interpersonal relationships with others.

Rachels (1975) further criticised the reductionists' view of privacy by urging that privacy is a distinctive right. He defended the view that privacy is essential to maintain a variety of social relationships, not just intimate ones, privacy accord the ability to control who knows what about oneself and who has access to one, and thereby allows one to vary behaviour with different people in order to maintain and control a variety of social relationships, many of which might not be intimate. Rachels' (1975) analysis emphasised that privacy is not only limited to control over information but also access to oneself, both of which allows control over relationships with others, thus connecting privacy to one's behaviour and activities.

In more recent literature highly related to the advances in technology, privacy has been defined as the freedom from judgement (Itrona and Pouloudi, 1999), the ability to exercise privacy tradeoffs (Adams and Sasse, 1999), the control over who has access to information (Belloti and Sellen, 1993; Dourish, 1993), the purpose and sensitivity of the information in a particular context (Westin, 1967; Adams and Sasse, 1999). Although the explicit impact of technology on privacy came to the fore since the arguments of Warren et al., there have been reasons for overriding the privacy intrusions. Since the terrorist attacks of September 11, 2001, there has been increasing views of the need to trade privacy for security and surveillance for public safety (Chandler, 2009). However, it might be argued that such approach of trading privacy for security strikes the wrong balance. Indeed, rather than security and privacy being zero-sum approaches to society's safety, a win-win approach is more complementary to good system designs. In the past few years research has examined ways in which respect for privacy might be balanced with justifiable uses of emerging technology (Agre and Rotenberg, 1997; Brin, 1998; Austin, 2003).

Westin et al. (1991) described individuals according to their privacy concerns. He defined 'privacy fundamentalists' as individuals who are extremely concerned with how their personal information is used and therefore are generally unwilling to share it with anyone; the 'privacy pragmatists', who share some of these concerns but prefer to make decisions on a case by case basis; and the 'privacy unconcerned' who are willing to give away information without much thought whenever it is requested of them (Westin et al., 1991). However, end users often appear unconcerned about

privacy until it is actually breached (Regan, 1995). This is because privacy is deterministic and tacit in nature that is, although users value their privacy, they cannot easily explain what it means to them and how they engage in private interactions until there is an effect to which they might relate. Privacy is also a volatile concept in the sense that end users' privacy perceptions may alter according to contexts and value tradeoffs that change over time and space for the same information.

The lack of clear and consistent definitions, different theoretical viewpoints and the fact that end users have varying views of the importance of privacy might infer the idea of a communication problem between the technology developers and end users. The next section reviews online privacy research to date.

2.3.2 Privacy research to date

Previous research in the area of online privacy has aimed at achieving a better understanding of privacy behaviour online and has studied end users' privacy decision making processes. They have done so using different perspectives and under different conditions. This section discusses their substantive and methodological contributions.

Substantive results

As reviewed in the previous section, privacy concerns are situated and dependent on the individual. End users can be categorised according to their online privacy concerns as privacy unconcerned, pragmatists and fundamentalists as shown through Westin's Privacy Segmentation Index (Kumaraguru and Cranor, 2005). However, privacy concern does not seem to corroborate with privacy behaviour. This was found by Spiekermann et al. (2001) and later confirmed by Acquisti and Grossklags (2005a). They found a privacy dichotomy in that although customers claim to be concerned about their online privacy; they do not behave according to these concerns both in terms of observed behaviour (Spiekermann et al., 2001) and reported behaviour (Acquisti and Grossklags, 2005a). Spiekermann et al. (2001) observed voluntary disclosure of address to a 'bot' and the types and number of questions answered. They found that rich and soft online communication with the automated software induced even privacy fundamentalists and profile averse participants to disclose (Spiekermann et al., 2001) personal information. These findings triggered

further research into understanding privacy decision making and factors that influence privacy behaviour.

The occurrence of the privacy dichotomy might be due to the fact that individuals are not rational decision makers. In a study to understand end users' decision making process with respect to privacy, Acquisti (2004) found that individuals do not act as rational economic agents as expected by privacy designs. Instead they exhibit bounded rationality and behavioural bias. While models of rational behaviour were seen to be unrealistic in E-Commerce, models of psychological distortions that reflect end users' self-control problems and the need for immediate gratification can be deduced (Acquisti, 2004). End users give higher value to the immediate benefits they can obtain from revealing personal information rather than the long-term desire to maintain privacy and under-estimate the cumulative risks associated with the cost of privacy loss (Acquisti, 2004). This happens even if end users perceive the risks of not protecting their privacy as significant. In another study Acquisti and Grossklags (2005b) found that limited information, ambiguity and uncertainty affect privacy decision making by reducing the valuation of personal information when compared with a certain benefit such as a discount (Acquisti and Grossklags, 2005b). Strandburg (2005) adds to the psychological perspective by further explaining the need to disclose immediately by arguing that people have a willpower problem and cannot resist the temptation to reveal (Strandburg, 2005).

Moreover, trust has also been found to impact end users' privacy behaviour. Jensen et al. (2005) show the effect of eleven variables on participants' choice of E-Commerce website. They investigated whether there was a relationship between the variables and purchase decisions and found that participants did not consult the policy as much as they reported they would and the likelihood that they would consult the privacy policy was unrelated to Westin's privacy concern categories (described in the previous section) and to gender. However the presence of the privacy policy did affect website choices. It was found that participants selected sites that had a privacy policy although they did not open and read the policy (Jensen et al., 2005). Trust is also induced through the reputation of the business and the presence of privacy cues, such as privacy seals including TRUSTe and Policy-User-Good (Jensen et al., 2005).

In their research on perceived privacy and trust, Joinson et al. (2010) found that trust moderates the impact of privacy concerns on behaviour by interacting with perceived privacy, such that high trust compensates for low privacy and vice versa. This finding has implications for research that looks into privacy designs such that studies that manipulate privacy and keep trust at a relatively high level might not find a significant association between privacy and behaviour (Joinson et al., 2010). In another study involving the P3P privacy enhanced search engine, Privacy Finder, it was found that participants trusted the privacy policy information, annotated to search results by the Privacy Finder. The Privacy Finder displayed a green, yellow or red bird icon revealing the status of the privacy policy. It was found that the information provided by the Privacy Finder had significant influence on the choice of websites for privacy sensitive purchases. Participants also assumed that a red bird icon was worse than no icon which was actually an indication that the privacy policy was unknown and could not be read by the privacy tool (Gideon et al., 2006). These studies show how users can be misled by the presence of privacy information that induces trust in the business and can explain behaviour that contradicts privacy concern.

Privacy policies can be successful in promoting end user choice only if the policy is read and the information contained in the notices are used. In a study to understand the motivations of end users to read privacy policies across a variety of situations, Milne and Culnan (2004) found that individuals tend not to read privacy polices when they have prior experience with the company. However for respondents who read the policy, they did so due to concerns when financial details were involved, to see how their personal details will be used and shared with others, to avoid receiving junk mail. Although concern motivated end users to read the policy, their perceived comprehensibility of the policy affected whether they actually read the policy.

The review of research to date of this section showed that end users do not behave according to their privacy concerns for several reasons. These include the following:

- End users are not rational economic agents and cannot be expected to interact online as rational beings. Instead people exhibit psychological distortions and behavioural bias.

- HCI provides limited and ambiguous information that causes uncertainty during privacy decision making and reduced valuation of personal information and privacy.
- Privacy HCI designs might not be usable due to end users' own assumptions (Privacy Finder's green, yellow and red icon) causing them to be misled.
- Privacy cues do not connect with end users' privacy attitudes to the extent of resulting in interactions with privacy mechanisms but instead link with trust attitudes to influence choice of service provider.
- Rather than the HCI interactively motivating end users and contributing to their engagement with privacy mechanisms, end users' own individual concerns (such as for financial details) was found to be the reason for privacy actions.

Therefore there is a need to better understand online privacy management as an interactive process and the role of HCI in contributing to this process and supporting end users' management of their privacy. There is also a need to better comprehend end users' response to different types of design elements.

Methodological approach

The methodological approach taken by previous research to understand privacy user behaviour and privacy decision making consists of a variety of methods. These include model mapping and the use of questionnaires, surveys and user experiments.

In his study of online privacy decision making, Acquisti (2004) used behavioural economics to map a model of rational privacy decision making and showed why end users could not be expected to behave according to the rational model (Acquisti, 2004). An online survey of adult internet users was conducted by Milne and Culnan (2004). They collected reported accounts of the frequency with which respondents read the privacy policy. They also asked the respondents to elaborate on the reasons for the number of times they read the policy. This approach helps to understand the motivations for reading the privacy policy. However, respondents' own reports of their behaviour or expected behaviour might not be an ideal reflection of their privacy behaviour. This is because the respondents might be answering the survey with how

they should behave rather than how they usually behave. Such surveys also require respondents to imagine themselves in the situation. This process might not be accurate given that, as discussed in the previous section, privacy is a tacit concept which is grounded in a particular situation.

Acquisti and Grossklags (2005b) also used a survey method but opted for an experimental survey design methodology to enable evaluation of the effect of uncertainty and ambiguity on privacy behaviour. The experimental manipulation of conditions was also used to explore the interaction effect of trust with privacy behaviour. Joinson et al. (2010) first used questionnaires to measure privacy concern, self-disclosure, situational perceived privacy and trust and devised a model of their interactions. This was followed by an experimental manipulation of privacy and trust using a web-based survey. The experimental manipulations for privacy were strong versus weak privacy policy whereas trust was manipulated by hosting the survey on an educational domain versus on a domain designed to reduce trust that included advertisements and spelling and coding mistakes. Although this approach included pre-questionnaires that supported the experimental survey and controlled and manipulated the experimental conditions, it however took respondents from their natural setting. This might cause the participants to respond with what is expected of them rather than provide an indication of their usual behaviour.

User studies and laboratory experiments were also used. Jensen et al. (2005) used an experimental approach to complement their demographic survey in order to better understand user behaviour. They presented participants with eight pairs of simulated E-Commerce web pages with controlled variation of twelve factors and asked participants which sites they would prefer to buy from. The variables were price of item, indication of SSL encryption, use of third party cookies and P3P, TRUSTe privacy seal, credit-card symbols, the company e-mail address, telephone number, postal address and four distinct privacy policies. On the other hand, Gideon et al.'s study involved a laboratory user experiment where participants were presented with a privacy enhanced search engine to select websites from which to make a privacy sensitive and a non privacy sensitive purchase. However participants may not be as likely to act naturally in laboratory setting than in their natural setting. In addition

this might generate a strong feeling of being under observation that consequently inhibits natural behaviour.

This section described the different methods used within privacy research to date. To summarise:

- the methodological approach might suffer from ecological validity since they either relied on self reporting of behaviour or was conducted within a laboratory which differs from end users' real life setting.
- The section also showed the difficulty of designing the most suitable study involving measurement of privacy behaviour that avoids all possible weaknesses. The very nature of privacy management can weaken the research methods used.
- Therefore the research methods within this thesis and measurement methods for privacy behaviour have to be carefully designed such that the characteristics of privacy are taken into account.

2.4 Usability

Privacy as the focus of the literature review was explored in the previous section. However as discussed in section 2.2.3 above, privacy mechanisms are available for online use but end users might not be able to use them for the purpose for which they were designed. Hence the second sphere of the literature review is the usability of privacy online. In this section, the academic context of usability is presented followed by an exploration of research to date that addresses the usability aspect of online privacy mechanisms.

2.4.1 Usability in an academic context

This section explores the foundations of usability. It starts with the origin of usability followed by measurement approaches.

Human-computer interaction (HCI) is the study of the interaction between people and computers and is concerned with the physical, psychological and theoretical aspects of this process (Dix et al., 2004). In the 60's and 70's the goal of developers was to

provide increasingly sophisticated software with more and more functionality that catered for a small number of trained end users only (Preece, 2001). However, over the following decade, there was a raised interest in the HCI research area by psychologists and human factors researchers (Dumas, 2007). The term usability was then adopted to replace the vague and subjective connotations acquired by the term 'user-friendly' (Bevan et al., 1991) and researchers were exploring both the use of scientific research experimental methods and checklist reviews as usability evaluation methods (Preece, 2001).

However, usability was still a poorly defined concept (Preece, 2001) with no accepted definition mainly due to the different requirements believed to make a product usable (Bevan et al., 1992). The definitions developed from different views of what usability is, three of which relate to usability measurement as analysed by Bevan et al. (1992). They were the product-oriented view, user-oriented view and the user-performance view. In the product-oriented view, usability can be measured in terms of the ergonomic attributes of the product whereas for the user-oriented view, usability can be measured in terms of the mental effort and attitude of the user. In the user-performance view, usability can be measured by how the user interacts with the product in terms of ease-of-use and acceptability (Bevan et al., 1992).

Furthermore, a survey of the literature performed by Rengger (1991) has identified four classes of performance measure. These are goal achievement which means accuracy and effectiveness; work rate which refers to productivity and efficiency, knowledge acquisition which relates to learnability and learning rate, and operability which involves error rate and function usage. Macleod et al. (1998) on the other hand defined usability to be ease of use and acceptability and claimed that the latter affects whether the product will be used. However, while measurement of the internal state, that is the user's physical state such as muscular or ocular fatigue, affective state such as preference and confidence, and mental state such as mental effort and fatigue, measured through psycho-metric (Kirakowski and Corbett, 1988) or psycho-physiological measures (Wiethoff et al., 1991) have been claimed to provide evidence of ease of use and acceptability, these are also factors that a-priori affect the effectiveness, efficiency of the product and the satisfaction experienced in usage

(Jordan, 1998). Thus we can argue that their measurement does not completely reflect the usability of the product but rather the state of the user which might be independent of the product usability.

ISO's definition of usability is however a more widely accepted definition of usability, that is, that the usability of a product is a function of the particular user or class of users being studied and the environment in which they work (Brooke et al., 1990; ISO, 1998). This view was also accepted by Shackel (1991) who devised a usability framework based upon earlier similar approaches. Shackel (1991) states that usability "depends upon the dynamic interplay" of the "four principal components of any user-system situation: user, task, tool and environment". ISO 9241-11 provides a framework whose purpose is to describe the components of usability and the relationship between them. ISO 9241-11 not only defines usability but also explains how to identify the information which is necessary to take into account when specifying or evaluating usability of a visual display terminal in terms of measures of user performance and satisfaction similar to Shackel's framework (Shackel, 1991).

This section provided a review of the different viewpoints of usability. It suggests that selection of a measurement factor of usability, such as effectiveness, efficiency, learnability, error rate, ease of use and acceptability, depends on the aspect of HCI under investigation. The next section elaborates on usability research conducted within the privacy domain to date.

2.4.2 Usability in research to date

This section reviews previous privacy research that has addressed the usability aspect of online privacy mechanisms. Un-usability of privacy mechanisms, in particular lack of readability and accessibility, is often provided as explanation to end users not using online privacy mechanisms.

Substantive results

In section 2.2.3, in this chapter, it was highlighted that the privacy policy might not be effective in ensuring end users' privacy online. The studies described in this section

support the in-effectiveness stance since they found privacy policies to be too legalistic, un-readable and un-usable.

In a review of the observations from three US Federal Trade Commission workshops, Cate (2010) stressed that policies have been considered as contracts which supports Milne and Culnan's (2004) survey findings that policies were too legalistic and hence not readable. Anton at al. (2004) found that 40 online privacy statements from 9 financial institutions lacked clarity and demonstrated in their study that most policies require a reading skill higher than the adult US internet population's average literacy level. They further proposed a standardised method of expressing privacy policies and for policies to be clearly articulated in a meaningful way. From their accessibility and readability analysis of 64 privacy policies, Jensen and Potts (2004) found problems with the structure and content of privacy policies. They concluded that the form, location and legal context of privacy policies make them un-usable as decision making aids for privacy concerned end users. Although the websites analysed had accessible privacy policies, they failed to provide adequate notification of changes or to present policies in a language end users can understand.

Proponents of improved privacy protection through the policies called for a simplified and unified format that presents information in a condensed and accessible form (Bettman et al., 1986; Derby and Levy, 2001). It has been argued that systems need to provide feedback and allow end users to perform an assessment of tradeoffs (Belloti and Sellen, 1993). Other studies have recommended more reader friendly alternatives to conventional privacy policies (Pollach, 2007), ways of presenting privacy information more clearly (Gideon et al., 2006) the need for privacy software to be designed in such a way that they allow even moderately computer-literate online users to protect themselves from the degree of self-disclosure they are afraid of (Spiekermann et al., 2001), and the requirement that an individual has a means to exercise control of access to the self and is aware of the potential consequences of exercising that control (Dourish, 1993).

Privacy researchers and industry groups have designed enhancements to the privacy policy formats with the aim of helping end users read and compare policies. One

enhancement is layered policies which present a short form of the policy in addition to a full policy (McDonald et al., 2009). Another enhancement is the Privacy Finder which is in a brief bulleted format (McDonald et al., 2009). In a comparative study McDonald et al. (2009) evaluated layered policies, the Privacy Finder report and conventional human-readable policies and found that participants of the study were not able to reliably understand the privacy policies in any of the formats. Compared to conventional policies, participants read the layered and bulleted formats faster but at the expense of accuracy for the layered format. Although the bulleted format resulted in higher accuracy than the conventional format, all the formats and policies were similarly disliked. Policies were also found to be not user-friendly for the moderately computer-literate users (McDonald et al., 2009).

There has also been research into specific privacy enhancing technologies, for instance P3P. Recommendations have been followed by attempts to devise better user interfaces for P3P. For instance, Cranor et al. (2006) described their design approach for user interfaces for P3P user agents. They also discussed design challenges for user interfaces for specifying privacy preferences and concluded that user interface designers need to find ways to manage the complexity, educate users about privacy, or express privacy concepts using language they already understand, guide users through the process of expressing their privacy preferences, and offer various options that meet the needs of a diverse set of users (Cranor et al., 2006).

Cranor et al. (2006) evaluated user interfaces for privacy agents that can fetch P3P privacy policies automatically, compare them with end users' privacy preferences and alert and advise end users. They developed one such user agent called Privacy Bird and found that although participants in their survey thought the bird sound was annoying, participants reported a change in their behaviour caused by the Privacy Bird (Cranor et al., 2006). Behaviour was reported to change with regards to filling forms online, taking advantage of opt out opportunities, ceasing to visit some websites, comparing policies at similar sites and trying to frequent sites with better privacy policies. Moreover, although not statistically significant, participants of the laboratory study had a quicker rate of finding privacy information with Privacy Bird than with Internet Explorer 6.0 or reading policies. They found the Privacy Bird to be

both useful and usable and appreciated short summaries of information as long as they did not hide important information.

Reasons given in the literature for under-utilisation of privacy in social network include poor interface design, permissive default settings, social conformance, and inherent trust in the online community (boyd, 2004; Acquisti and Gross, 2006; Govani and Pashley, 2007; Gross and Acquisti, 2005). Richter-Lipford et al. (2008) designed a prototype to improve privacy management in Facebook. Whilst they demonstrated that Facebook users had difficulty understanding the existing settings, they found that their audience view prototype enabled end users to have a better mental model and improved visual feedback (Richter-Lipford et al., 2008). In a subsequent study, Richter-Lipford et al. (2010) compared two different privacy policy representations: AudienceView that represents a policy as the different views of information as seen by various audiences or groups of user and ExpandableGrids which is a general, matrix-based visualisation of a policy showing effective combination of policy rules. They found that both interfaces were highly usable but there was no performance difference between the two interfaces (Richter-Lipford et al., 2010). However, users had clear and different preferences. Some preferred AudienceView for the visual feedback but disliked the number of page visits while others liked the compact overview available for ExpandableGrids with all settings in one location. They concluded from their results that either interface would be usable for similar privacy policies and that different representations of the policies may appeal to different users (Richter-Lipford et al., 2010).

This section explored the design of privacy mechanisms from a usability perspective. However, as discussed by Ackerman and Cranor (1999) privacy poses a difficult HCI problem since the privacy mechanisms must not only provide information and enable decision making (such as through enhancements to readability, performance or enabling better understanding of privacy policies as described above) but also has to enable this to happen seamlessly and without interference to social engagements. This view was also re-iterated by Cranor et al. (2006) in their discussion of the design challenges that need to be addressed to enable end users to specify privacy preferences. This is because

- the proposed separate enhancements to readability and performance or enabling better understanding of privacy policies might not ensure that end users are able to manage their privacy effectively as per their privacy goals.
- Moreover, as concluded in the review of usability within an academic context above (section 2.4.1), there are different usability viewpoints and selection of a measurement factor of usability depends on the aspect of HCI under investigation.
- Therefore before evaluating usability of online privacy, there is first a need to better understand the requirements of usable online privacy mechanisms through a multidisciplinary perspective (not only legal or technological).
- Such an approach might enable the design of a better means of evaluating usability of online privacy and help to suggest proposals for usability enhancements.

Methodological approach

The methodological approach adopted by the research that investigated usability aspects of privacy included both evaluations of specific designs and comparisons of different designs based on end user choice. The methods comprised analytical evaluations of design, user surveys and comparisons to better understand how end users interacted with the designs and laboratory user studies to measure effectiveness aspects such as performance.

Anton et al. (2004) performed goal-driven requirements engineering and readability analysis of 40 privacy policy statements from 9 financial institutions. The analysis enabled the identification of vulnerabilities, ambiguities and conflicts. They were concerned that they, experienced analysts, encountered difficulties in understanding policy statements. Jensen and Potts (2004) analysed 64 privacy policies belonging to a set of high-traffic websites and a set of health care websites. Their analysis differs from Anton et al. (2004) in that they assessed policy accessibility first in terms of ease for users to find the policy and second in terms of the ease for users to get a complete picture of the policy. Ease of finding the policy was measured through placement of policy link and visibility whereas ease of getting a complete picture was measured

through the length and number of pages the policy is spread across. They also determined policy readability using the Flesch Reading Ease Score (Flesch, 1848). These two analyses provided valuable insight into whether end users can be expected to access and read privacy policies but did not suggest how the design could be improved to enhance accessibility and readability. Although the evaluations were structured, analytical evaluations have the disadvantage of not involving end users and of being an interpretation from a given perspective.

Experimental survey designs and laboratory experiments were also conducted. McDonald et al. (2009) conducted an online between subject survey where 749 participants were presented to one of 15 privacy policy representations. They contrasted 6 companies' conventional natural language policies and their corresponding Privacy Finder report privacy policy format plus three layered policies. The study questions assessed comprehensibility, psychological acceptability and demographics and assessed whether participants had higher accuracy scores, shorter times to answer and greater psychological ability with both of the standardised formats than with their natural language counterparts. Cranor et al. (2006) also conducted a user survey to find out how the P3P user agent, Privacy Bird was used in practice and collected self-reported data from individuals who have been using Privacy Bird for several months in their own homes and offices. The participants reported a change in behaviour following use of Privacy Bird. In a subsequent laboratory study, they compared effectiveness of Privacy Bird with Internet Explorer and reading privacy policies. 12 experienced Internet Explorer users were given a brief tutorial of the browser agent and Privacy Bird and were then asked to answer questions with regards to a web site's privacy policy. The control was to read the policy at a different web site without the help of privacy bird. The time taken to find information was collected. The researchers also evaluated the capabilities of Privacy Bird with respect to Bellotti and Sellen's (1993) framework for design for privacy related computer supported co-operative work, computer mediated communication and ubiquitous computing environment and discussed how Privacy Bird provided these. Self-reported accounts might be to some degree biased with participants reporting what they thought researchers wanted to hear whereas laboratory

experiments take participants away from their natural setting such that they cannot be completely expected to behave as they naturally would.

Richter-Lipford et al. (2008, 2010) used iterative prototyping and testing. In 2008, Richter-Lipford at al. conducted a within subject comparison user study where participants were asked to perform a set of five tasks on two interface asking them to determine the effects of the privacy settings in terms of determining who had access to what information. Their comfort or confidence about who would get access to their information was also queried for the two versions. In a follow up study, Richter-Lipford et al. (2010) conducted another within subject study to compare the tradeoffs between the AudienceView and ExpandableGrids. Users were asked to complete 17 individual tasks for each interface, after each they were asked to rate their confidence in their actions or responses. In the first four tasks they read and understood a policy and to gauge their understanding of the settings, they were asked which friend groups could access some information from their profile. The other tasks involved simple and complex configurations followed by an exploration and self configuration of privacy settings while thinking aloud. The within subject study might suffer from carry-over effects such that when participants reach the second interface, they might detect and process information quicker and be more confident. 17 individual tasks for each interface could also cause fatigue to affect the findings.

This section described the variety of approaches used to assess the usability of online privacy. Although each of the different approaches contributes valuable insight into the research area, it is practically unfeasible to design a usability study that perfectly matches a real world situation and at the same time generates rich data. A fitting approach could however be to conduct at least two studies with different approaches that support and complement each other. This is because as shown by the above review:

- analytical evaluations suffer from the disadvantage of not involving end users and largely depend on evaluators' interpretations.
- Participants' self-reports might not be reliable due to a possible tendency to please researchers or due to participants' reports of assumed ideal behaviour.

- Participants in within subject user studies involving comparisons might be affected by carry-over effects and fatigue.

2.5 Persuasive technology

Although privacy mechanisms are available online, due to the nature of privacy and the diversity of end users, usability alone might not ensure that privacy designs can connect with end users' attitudes. Influence methods might provide this support to privacy designs. The third sphere of the literature review is persuasive technology. In this section, the academic context of persuasive technology is presented followed by an exploration of research to date that addresses the influence of website components or designs on end user privacy behaviour.

2.5.1 Persuasive technology in an academic context

This section of the review highlights the origin of persuasion in communication. It then portrays the use of persuasive communication within technology.

Persuasion, as defined by the philosopher Aristotle over 2300 years ago, is "the art of getting people to do something they wouldn't ordinarily do if you didn't ask" (Borg, 2007). Borg argues that basic human values have not changed much over the centuries and the groundwork laid by Aristotle for successful communication provided the most influential theory regarding persuasion. Aristotle observed that as social animals, all humans were called upon to persuade fellow human beings almost on a daily basis since all persuasive situations comprise of taking the audience from a certain starting point A and moving them to point B which is the objective. That shifting of attitude is what is called persuasion. Since at the initial point A, the person is uninterested or resistant to one's ideas or proposals, the person needs to have or be provided with an understanding of the views one is putting forward and more importantly believe the message. For instance a persuasive speech might employ entertaining, thought-provoking, and eloquent methods but those techniques might not be the purpose of the speech but rather to move the audience to the point B.

At the core of Aristotle's Rhetoric theory, where rhetoric is defined as "the ability to see what is possibly persuasive in every given case", are non-argumentative tools of persuasion (Rapp, 2010). These are the three systematic 'technical' means of persuasion where technical refers to the fact that it rests on a method and one must understand the method used and know why some things are persuasive while others are not. Those three technical means according to Borg (2007) are the ethics, the emotional appeal and the logic of the persuasive means. Ethics refers to the ethical character and reputation of the persuader that is credibility whereas the emotional appeal is the emotional disposition of the one being persuaded. Thus the persuader must have an ability to identify and to understand the other person's feelings, ideas and situations. The third technical means is the logic of the persuasive means which can be either inductive or deductive.

Persuasion has been studied in recent decades by psychologists, such as Cialdini (1998), as a means of social influence. They have hoped to define methods of guiding people towards the adoption of an idea, attitude or action. Perloff (2010b, pp12) defines persuasion as a communication process:

> "a symbolic process in which communicators try to convince other people to change their attitudes or behaviours regarding an issue through the transmission of a message in an atmosphere of free choice".

Perloff's (2010b) definition shows that persuasion involves the use of symbols and language rich with meaning that is aimed towards an attempt to influence others. The message transmitted can be verbal or non verbal, reasonable or unreasonable, factual or emotional and can consist of arguments or simple cues. The other important component of the persuasion definition is free choice that is individuals must be free to take the actions desired such as altering their behaviour or not in a communication setting. On the other hand, Cialdini (1998) defined six 'weapons of influence' which are reciprocity, commitment and consistency, social proof, authority, liking and scarcity. These 'weapons' have been widely used in marketing, advertising and politics (Cialdini, 2000).

In addition, probably due to the pervasiveness of technology, persuasion as a technique to enhance end user experience and boost consumption, has emerged within the computing area (Fogg, 2003). The psychologist, B.J. Fogg, who has studied the use of technology as an aid to persuasion, has coined the word 'captology' to capture the area of research, applications and design of the use of computers as persuasive technologies (Fogg, 2003). Captology is an acronym for "computers as persuasive technologies' (Fogg, 2003, pp5) and persuasion in this context has been defined as an attempt to change attitudes or behaviours or both. In their discussions of persuasion in software and information systems, Oinas-Kukkonen and Harjumaa (2008b) however defined a persuasive system as one "designed to reinforce, change or shape attitudes and behaviours or both without using coercion or deception". This definition is based on Miller (1980) who asserted that persuasive communication can be in the form of any message that is intended to shape, reinforce or change the responses of another or others. This definition restricts persuasive communication to the intention of persuading others but corresponds with the intentional use of computers to persuade end users. Oinas-Kukkonen and Harjumaa (2008a) moreover add in their systematic framework for designing and evaluating persuasive systems that of these three outcomes, a persuasive interaction aimed at a shaping outcome may have a higher likelihood of success than one aimed at changing behaviour. Moreover, while Fogg (2003) considered persuasive systems as those that used human-computer persuasion, Oinas-Kukkonen and Harjumaa (2008a) considered persuasive systems as those using both human-computer and computer mediated persuasion. The reasons being that computers and systems do not have intentions on their own but rather those who create, develop and distribute the technology do and although computers cannot communicate the same way humans do, human-computer interactions have been shown to exhibit patterns similar to social interactions (Nass et al., 1994; Fogg, 1998).

Persuasive technologies can be categorised according to their functional roles (Fogg, 2003). When used as a tool, persuasive technologies make target behaviour easier to do, lead people through a process and perform calculations or measurements that motivate whereas when used as a social actor, they are persuasive by rewarding people with positive feedback, model a target behaviour or attitude or provide social

support. On the other hand when used as a medium they provide an experience by allowing people to explore cause-and-effect relationships, providing people with vicarious experiences that can motivate or help people to rehearse behaviour.

This section showed that although persuasion has been practised since Aristotle's era, it is only in the early twenty-first century, due to Fogg's (2003) work, that technology has formally been recognised as a support to persuasion. Since persuasive technology can make target behaviour easier to achieve, motivate and provide positive reinforcement and allow simulation and rehearsal of experiences, it can be a valuable asset in enhancing the effectiveness of complex systems such as privacy management mechanisms.

2.5.2 Persuasive technology in research to date

In this section, research that looked at the influence of website components or of designs on end user privacy and disclosure behaviour are reviewed. The section shows how these components can be considered as persuasive before reviewing other research that have suggested or implemented design approaches that can be considered under persuasive technology.

Substantive results

In a study to explore the effect of internet seals of approval, such as TRUSTe and BBBonline, Miyazaki and Krishnamurthy (2002) found that the presence of the internet seals of approval logo raises favourable perceptions of the business' privacy-related practices. This finding is particularly interesting since it follows another study by the same researchers (Miyazaki and Krishnamurthy, 2002) where they found that the presence of the seals of approval did not reflect the businesses' online privacy practices (as seen from their privacy policy). This study is supported by Jensen et al.'s (2005) discussed in section 2.3.2 of this chapter where it was found that the presence of privacy policy or other trust marks caused end users to trust the websites that consequently influenced their choice to do business with them. In terms of persuasive technology, the internet seals of approval, noticeable presence of policy or other trust marks act as cues that reassure end users of the credibility of the businesses and influence end users' disclosure and privacy decisions. A similar conclusion was

reached in Gideon et al.'s (2006) study as elaborated in section 2.3.2 above. The privacy icon and the privacy report that are annotated to search results help to provide accessible privacy information that reduces the information asymmetry between end users and service providers. They also make it easy for end users to distinguish between service providers by enabling end users to select service providers who seem better able to protect their privacy. It was also shown that when privacy information was made accessible, some end users were more willing to pay a premium for services from more privacy protective service providers (Gideon et al., 2006).

Researchers have proposed and designed privacy mechanism prototypes that contain persuasive technology elements that take a functional role of suggesting or warning end users. Ackerman and Cranor (1999) reported on two sample privacy critics that are semi-autonomous systems that help people protect their online privacy by offering suggestions and warnings. The first one checks a consumer complaints database before warning end users whilst the second one watches the type of information entered by end users and warns them when the P3P proposal requests data that can be used in combination to identify end users.

Privacy designs also provided visual feedback that can be considered as a persuasive element. Watson et al. (2009) assessed the performance of their prototype, designed to provide improved visual feedback in the form of information sharing to different audiences, against that of Facebook. The prototype can be categorised as an example of Fogg's (2003) cause and effect simulation persuasive design and can provide a better mental model than Facebook. Although the participants to their study were able to modify the privacy policy of the prototype version quicker and with more confidence than that of Facebook, they did not exhibit higher configuration accuracy. Watson et al. (2009) suggested that their prototype would be more effective than Facebook by requiring less cognitive effort to complete tasks. Kelley et al. (2009) designed a 'Nutrition Label' type privacy policy and found that participants were better able to understand the differences between privacy policies, the control over their information and the time-based cost of reading privacy policies. Participants were better or similarly able to accurately find information and compare policy in the label to that of the usual privacy policy. The visual feedback of the label allowed

participants to easily find privacy information at the same place every time. They also found that participants more consistently selected the company with the stronger policy.

Another study involving persuasive element proposed contextual integrity (Richter-Lipford et al., 2009), that is a framework that can be used to enhance the visibility and ease of understanding of flows of information across a social network site. Contextual integrity would be persuasive by providing visible information flows that could appeal to end users to manage their privacy, by making context more concrete and enhancing control over information flows.

This section reviewed research on online privacy that has some persuasive elements. The review showed that

- design elements can engender trust, suggest actions, warn end users or provide visual feedback that can connect with end users' privacy attitudes.
- It is clear however that there is a lack of research about how and why persuasive technology would affect privacy behaviour and support privacy management as an interactive process.
- These studies stressed on end user understanding of the policy or privacy settings, made the policy more likeable and stressed on choice of company website.
- They however did not explore the effect of persuasive communication on the effectiveness of privacy mechanisms in terms of the privacy attitude-behaviour relation.

Methodological approach

The approach used by previous research to determine the influence of design elements on privacy perceptions and behaviour were not targeted at finding the influence of persuasive methods. Instead they formed part of user studies designed for other purposes. For examples, Miyazaki and Krishnamurthy (2002) used a between subject user experiment design that presented participants with printed information for the different websites containing three different seal of approval logos. Participants'

perceived favourableness of the business' privacy practices was then assessed together with the reported likelihood that the participants would disclose personal information. Approaches that can be considered under persuasive technology were also proposed and implemented as enhancements to designs without being referred to as persuasive methods such as in Ackerman and Cranor's (1999) study in the previous section.

This section reiterated the findings of the previous section, in that there is a lack of research designed to specifically explore how persuasive elements of system design affect end user privacy decision and behaviour. It would be valuable to find out how and why different persuasive elements affect end user behaviour and the implications in different disclosure-privacy contexts.

2.6 Research gap and research problem

The real world problem as stated in the first section of this literature review arises due to the conflict between end users' requirements and business requirements. The characteristics of the online environment and un-usability of the available privacy mechanisms contribute to the problem of ensuring privacy of end users online. The difficulty in ensuring usability of privacy mechanisms is also related to the tacit and contextual nature of privacy such that although end users claim to be concerned about their privacy, they find it hard to take privacy actions when interacting online.

Following the review in the previous sections of this chapter, this section brings together review findings and discusses the research gap. It then formulates the research problem and articulates the research question.

2.6.1 Substantive

Individuals instinctively manage their privacy offline but as seen in the previous sections of the literature review, this is hardly achievable online. Previous research found a dichotomy between privacy concerns and behaviour that is although end users have privacy attitudes, their behaviour failed to reflect their attitudes (Spiekermann et al., 2001; Acquisti and Grossklags, 2005a). Research that looked into privacy decision making found that end users are not rational economic agents and cannot be

expected to interact online as rational beings (Acquisti and Grossklags, 2005a). Instead people exhibit psychological distortions and behavioural bias. As reviewed in section 2.3.2, privacy HCI designs do not help since they

- provide limited and ambiguous information that causes uncertainty during privacy decision making and reduced valuation of personal information and privacy,
- cause a link with other attitudes such as trust that influences disclosure instead of connecting with end users' privacy attitudes,
- do not take end users' assumptions into account such that designs can be misleading,
- do not interactively motivate end users and contribute to their engagement with privacy mechanisms.

Following section 2.4.2, an HCI approach that solely focuses on improving understanding of disclosure information (such as through better readability) or at easing task completion (such as through enhanced performance) might not be sufficient in ensuring privacy attitudes are activated or accessed and that privacy mechanisms are effective. Similar to usable security (Whitten and Tygar, 1999), usability of online privacy has to be better understood to enable better means of evaluating online privacy and of proposing enhancements. Previous research has not explored how effective and usable privacy should be designed from a multidisciplinary (non-predefined) perspective and a general focus that is not specific to a context of use (the Privacy Incorporated Software Agents consortium has defined HCI requirements - HCI-P from legal requirements (Patrick and Kenny, 2003) and Privacy and Identity Management in Europe for Life has added a socio-cultural aspect to it (PRIME WP06.1, 2008); others have derived usability from end users' behaviour in surveys and the question of usability of online privacy from an experts' view has not been addressed). Therefore to determine the characteristics of privacy designs that would contribute to their effectiveness and usability that is would allow end users to use the privacy mechanisms according to their needs or privacy attitudes, the research within this thesis first explored and defined the requirements of usable online privacy mechanisms irrespective of contexts.

As highlighted above, previous research has noted a variety of usability issues and in-effectiveness of privacy mechanisms. Privacy being a behavioural concept, this research evaluated the usability through a social-psychological assessment of existing privacy designs by demonstrating whether they actually provided for the requirements. These usability requirements are expected to enable end users to seamlessly achieve their privacy goals. Seamless and intuitive privacy management also means that the social psychological processes that would ensure the privacy designs are effective in supporting end users' privacy attitude-behaviour relation is provided. Therefore the second research question aimed to find out whether and how existing designs actually provided these processes.

From section 2.5.2, although enhancements to online privacy has been proposed, previous research

- has not considered the impact of these proposed improvements on the effectiveness of online privacy mechanisms in terms of aligning end users' privacy behaviour with their attitude.
- They have not categorised these enhancements as influence methods or as persuasive technology and consequently not explored how the different types of enhancements connect with privacy attitudes to affect the attitude-behaviour relation.
- They have also neither compared the effects of different influence methods nor explored how and why these could affect end users' privacy management behaviour.

An investigation of how persuasive technology influences privacy behaviour would allow research to offer improvements to the human-computer interactions design of privacy by focusing on how the system communicates with end users and the impact of this communication in activating privacy attitudes. This approach will also contribute to ensuring effectiveness and hence usability of privacy mechanisms. This is because although end users possess privacy attitudes, these exist within end users' cognitive structure and are not necessarily invoked during online interactions. For end users' privacy attitudes to be associated with online interactions, the attitudes

might need to be activated that is end users have to categorise the online interaction experience as an instance requiring control of access to their personal information. The privacy attitudes might also have been associated with a similar interaction before but needs to be made accessible that is retrieved from memory. Persuasive communication can present privacy information and help paint a mental model that would activate privacy attitudes or make privacy attitudes accessible such that end users can undertake privacy behaviour that matches their privacy attitudes and in doing so ensure effectiveness of online privacy mechanisms.

Therefore the research investigated whether persuasive communication can provide the social-psychological link within privacy designs that ensures end users' privacy attitude and behaviour consistency. End users with stronger attitudes such as highly privacy concerned individuals (where strength refers to a consistent and well-rehearsed link between an attitude object and its evaluation) can be expected to have high attitude accessibility to engage into privacy behaviour more easily than those with lesser activated attitudes. The thesis' research selects a context and evaluates the impact of different persuasive communication approaches on privacy behaviour.

- The first research question was: what are the requirements of usable online privacy mechanisms?
- The second research question was: how usable are online privacy mechanisms? This research question also helped to explicate how and why, as claimed by previous research, privacy designs are in-effective in ensuring end users' privacy.
- The third research question was consequently: how does persuasive communication affect the effectiveness of online privacy mechanisms?

2.6.2 Methodological

The previous sections highlighted the issues in designing evaluation of privacy design and privacy behaviour and showed that designing the most suitable approach is difficult due to the nature of privacy. The weaknesses of the different methods included:

- ecological validity,
- researcher bias or focus on a specific perspective,
- carry over effects and participant fatigue.

Moreover, although previous research has tried to map economic models of behaviour (Acquisti 2004), has conducted user surveys and experiments to understand behaviour and has evaluated the usability of some privacy mechanisms (Milne and Culnan, 2004; Acquisti and Grossklags, 2005a; Jensen et al., 2005), it has not mapped or investigated a communication approach to evaluating or enhancing online privacy designs. Previous research has not looked at affecting the attitude-behaviour relation as a means of improving effectiveness of online privacy mechanisms. It has not considered privacy designs through a socio-psychological lens although it has previously been said that end users respond to technology by exhibiting social behaviours and by making social attributions within human-computer interactions that are similar to human-human interactions (Nass and Moon, 2000). A socio-psychological lens would not only enable understanding of offline individuals' privacy management methods that could inform online designs, but also help evaluate and propose designs that communicate privacy online to end users more effectively. A socio-psychological approach would also help to better understand privacy attitudes and help cater for critical differences in perceptions of disclosure and technological possibilities for different levels of privacy concern individuals. It would consequently also help to formulate persuasive methods that would help privacy attitudes to be reflected within behaviour.

To answer the above research questions and contribute to filling the methodological gap, the research within this thesis queried privacy experts on improving usability of online privacy mechanisms through iterative questionnaires. This was followed by analytical evaluation of existing privacy designs for socio-psychological processes of privacy management through a systematic evaluation method. Persuasive communication was then designed within a disclosure-privacy context and its impact on privacy behaviour was assessed within an experimental user study that did not take place within a laboratory setting. The methodology design consequently consists of a selection of methods that support and complement each other so as to minimise their

individual weaknesses. The next chapter elaborates on the research strategy and method design and lists the studies designed to answer the research questions.

Chapter 3: Methodology

3.1 Introduction

In the previous chapter the research gap was identified within the research space. This includes:

- a lack of exploration of the criteria for effective and usable privacy from a multidisciplinary (non-predefined) perspective and a general focus that is not specific to a context of use. Such an exploration would help to design privacy evaluation methods and support proposals for usability enhancements.
- No investigation for the socio-psychological processes of privacy management within privacy HCI designs that would be an indication of what is missing in current designs to support privacy interactions as a behavioural concept.
- Previous research has not viewed its proposed enhancements to privacy designs as influence methods that affect activation and accessibility of privacy attitudes such that the later is reflected in privacy behaviour. It has also not explored how and why these could affect end users' privacy management behaviour.

The purpose of this chapter is to describe the methodological approach that underpinned the research and contributed to closing the above gaps. The research questions are first stated followed by an articulation of the research strategy and the philosophical foundations. The chapter then elaborates on the research design

framework and includes a reflection on the validity of the design. It follows with a list of the data collection and analysis techniques that were used to answer the research questions.

3.2 Research Questions

The research first aimed to define the requirements of usable privacy mechanisms that is mechanisms that provide for the processes of privacy management. The research then assessed existing privacy mechanisms for social-psychological processes of privacy management that would enable effective privacy mechanisms, and explored the influence of persuasive communication in influencing privacy behaviour and in aiding the privacy attitude construct to be reflected in behaviour. The research questions that were derived following the literature review of the last chapter are:

- RQ1: What are the requirements for usable online privacy mechanisms?
- RQ2: How usable are existing online privacy mechanisms?
- RQ3: How does persuasive communication impact the effectiveness of online privacy mechanisms?

3.3 Research Strategy

In this section of the methodology chapter, the research strategy is depicted. The perspective taken to answer the research questions is first detailed. Second, the section follows with a social-psychological exposé of the relationship between attitude and behaviour that discusses the strategy to address the privacy dichotomy introduced in the literature review.

3.3.1 Social science approach

As detailed in the Literature Review Chapter in section 2.3.1, privacy is a multidimensional concept. It has a physical, social, psychological and legal dimension. The socio-psychological dimension of privacy is particularly essential to the maintenance of relationships because privacy is implicit within the communication that forms part of interpersonal interactions (Fried, 1970; Gerstein,

1978). In the online environment, end users interact with service providers or other end users. The online human-computer interactions (HCI) could hence be thought to be as important to online privacy management as the interpersonal interactions are to real world privacy management. In the same way as exploration of the interpersonal interactions would benefit from a social science approach, it follows that deliberation of the usability of HCI design of online privacy would also benefit from such an exploration that exposes rich interpretations about the expected effectiveness of current designs. This philosophical approach could then also facilitate the formulation of alternate designs. However, since controlled user studies are core to assessing HCI, a positivist approach is essential to evaluating the effect of a particular condition – in this case the effect of persuasive communication on usability. Thus the research applies a pragmatic viewpoint that combines qualitative and quantitative research techniques and seeks to offer a logical and practical alternative to using a viewpoint at the extreme end of the positivist-interpretivist spectrum. The pragmatic viewpoint makes use of pluralistic approaches to understand and derive knowledge about a problem which requires both the need to explore and explain (Creswell, 2009a). This research hence moves past the paradigm wars that advocate an either-or approach by tapping into the advantages of both philosophies.

Figure 2 below depicts the research strategy which is bounded within a socio-psychological theoretical lens. It is a mixed method design that employs a sequential exploratory strategy. The sequential exploratory strategy starts with qualitative data collection and analysis followed by quantitative data collection and analysis. Weight is placed on the first phase that is the qualitative phase. The findings of this phase then guide the evaluation of the quantitative phase.

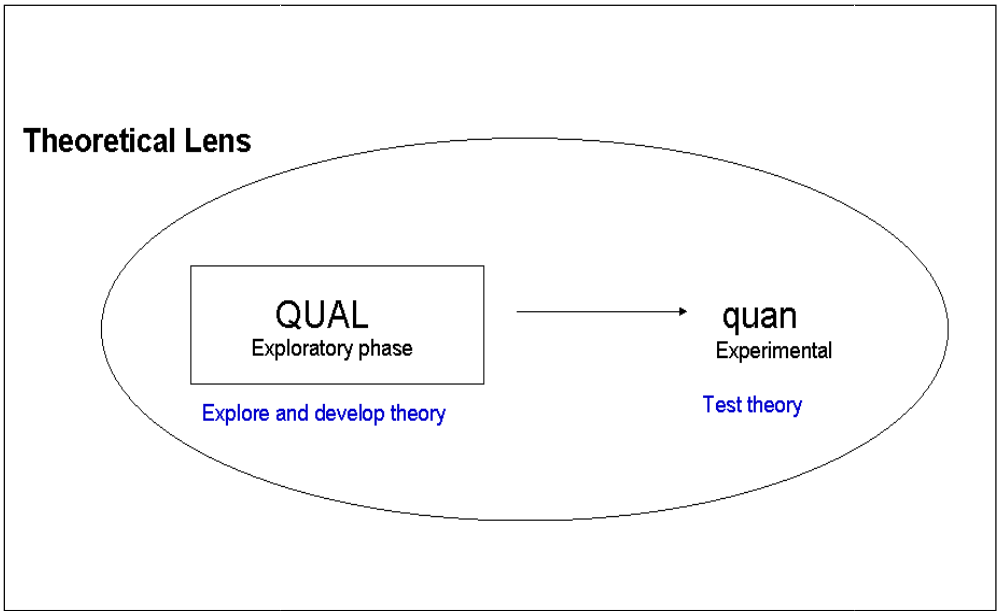


Figure 2: Sequential exploratory research flow using the notations in Creswell (2009a)

3.3.2 Social-psychological exposé of attitudes and behaviour

This section looks at the socio-psychological foundations of attitude and behaviour and discusses the reasons previous research have found discrepancies between privacy attitude and behaviour. It then shows how persuasive communication can be used to fill the gap between privacy attitude and behaviour.

Attitudes and behaviour

Attitudes have been given numerous definitions over the past century. According to scholars, an attitude is

- "an association between a given object and a given evaluation" (Fazio, 1989),
- "a psychological tendency that is expressed by evaluating a particular entity with some degree of favour or disfavour" (Eagly and Chaiken, 1993),
- "a learned predisposition to respond in a consistently favourable or unfavourable manner with respect to a given object" (Fishbein and Ajzen, 1976),

- "a more or less permanently enduring state of readiness of mental organisation which predisposes an individual to react in a characteristic way to an object or situation with which it is related" (Cantril, quoted in Allport, 1935, p.804)

While the first two definitions stress the association with an object/entity and evaluation of the latter, the last two definitions highlight the behavioural view of attitude. Perloff (2010a) discusses these and puts together a more stable definition that encompasses the key aspects of the above definitions. He follows McGuire (1985) in defining attitude as an object of thought and a dimension of judgement:

> "An attitude is defined as a learned, global evaluation of an object (person, place or issue) that influences thought and action." (Perloff 2010a, pp 43)

Perloff's definition helps towards better understanding the concept of attitude: first people are not born with attitudes; rather attitudes are learnt over the course of life through socialisation (Perloff, 2010a). Attitudes are developed through encounters with social objects leading to the second part of the definition - evaluation which includes both cognition and affect. Evaluation of encounters can then be expressed through thoughts, feelings, intentions to behave and behaviour. Third, attitudes help people to organise their social world and hence influence behaviour (Perloff, 2010a).

Together with cognitive and affective responses to evaluations, behavioural responses form the three main classes of responses (Rosenberg and Hovland, 1960). Behaviour is what people do and involves people's actions. It has more than one dimension that can be measured such as frequency, intensity and duration. Since it is an action, the occurrence of behaviour can be observed, described and recorded both by the person doing the behaviour and by others (Miltenberger, 2011). Behaviours impact the physical or social environment. People interact with their environment by either responding to stimuli or intentionally performing an act with consequences. Behaviour can thus be of two types: respondent behaviour or operant behaviour (Miltenberger, 2011). Respondent behaviours are brought about by stimuli and occur automatically in the presence of the stimuli. They are elicited by antecedent stimuli and are relatively insensitive to their consequences. They help the organism adapt by

regulating organisms' physiology and contribute to their safety. Operant behaviour on the other hand is "behaviour that acts on the environment to produce an immediate consequence and in turn is strengthened by that consequence" (Miltenberger, 2011, pp 63). Operant behaviour 'operates' on the environment and has been described as behaviour that is voluntary and purposeful (Leslie, 1996) as opposed to behaviour that is reflexive or outside of the subject's control. Operant responses are not elicited by antecedent stimuli but rather rely on the reinforcing or punishing effects of a consequence to strengthen or weaken operant behaviour (Sturmey et al., 2007).

Reasons for why privacy behaviour may not match privacy attitudes

The privacy dichotomy depicts the discrepancy observed by previous research between attitude and behaviour (Spiekermann et al., 2001; Acquisti and Grossklags, 2005a). Such a discrepancy is however not a new occurrence since sociologists have studied the problem of attitude-behaviour inconsistency from more than three decades ago following LaPierre (1934)'s questioning of the assumption that attitudes cause, reflect or correlate substantially with behaviour. He found that the anti-oriental attitudes of tourist accommodation owners' did not reflect in their behaviour towards allowing the stay of a Chinese couple in their establishment. This section discusses why privacy attitudes does not necessarily lead to privacy behaviour by first looking at the structure of attitudes and then discussing the measurement of privacy attitudes and behaviour in previous research.

Structure of attitudes

The structure of attitudes can be described in two ways: either through the relationship between the cognitive, affective and behavioural components of the particular attitude or through the associations across attitudes and the links between attitudes and different attitude objects (Eagly and Chaiken, 1993). However, three characteristics of attitudes have been deemed to be important. These are the accessibility of attitudes, the activation of attitudes and the possibility of ambivalent attitudes (Augoustinos et al., 2006). These aspects of attitudes could explain the privacy

dichotomy observed by previous research, that is, that privacy behaviour does not always match attitudes. They are discussed in the paragraphs below.

Social psychology distinguishes between the availability of an attitude and its accessibility (Higgins, 1996). While availability of an attitude refers to whether it is present within a person's cognition, accessibility of attitude refers to the ease with which the attitude may be retrieved from memory (Fazio, 1989). Augoutinos at al. (2006) explained that the accessibility of an attitude is dependent on the properties of the attitude such as strength of the attitude and aspects of the context that highlight particular attitudes as being relevant. This is important because accessible attitudes lead to corresponding behaviour more closely than less accessible attitudes (Fazio and Williams, 1986). Therefore, whilst individuals have privacy attitudes, these may not be accessible when they interact online. The low accessibility of privacy attitudes during interactions may be first due to the lack of relevance of the online disclosure context to privacy attitudes and second due to the weak strength of the privacy attitude. It is important to note here that rather than extremity in terms of positive or negative value of the attitude, the strength of a particular attitude refers to a consistent, well-rehearsed link between an attitude object and its evaluation (Augoustinos et al., 2006).

Although attitudes may be available, they may not be active; that is they may not be associated with an object or issue to cause its evaluation (Fazio, 1989). This characteristic of attitudes can also explain the privacy dichotomy, that is although individuals hold privacy attitudes, they may not be able to associate these attitudes with their online activities. Another explanation can be that the privacy attitudes are not strongly associated with the disclosure context. It was shown by Fazio et al. (1986) that when the association between an object and its evaluation is strong enough, simply noticing the object would cause the evaluation to become activated.

Attitudes can have multiple cognitive and affective components thus leading to different evaluations of an object. These ambivalent attitudes are unstable since the evaluation expressed at a particular moment depends on the elements of the attitude that is most accessible at that time (Eagly and Chaiken, 1993). Privacy attitudes for

the online environment can be said to be ambivalent since a variety of different personal information disclosure contexts exists online that makes it hard for individuals to maintain stable and strong evaluations. This property of online privacy attitudes may also explain why individuals' do not behave according to their privacy attitudes.

Measurement of attitude and behaviour

Measurements of privacy attitudes in previous research have used general measures of privacy attitudes and compared these to disclosure actions (Spiekerman et al., 2001; Acquisti and Grossklags, 2005a). The discrepancy in their observed privacy behaviour and attitude may be either due to inconsistency in terms of the specificity of attitude and behaviour or due to taking disclosure actions to be a direct measure of privacy behaviour.

Since LaPierre questioned the relationship between attitude and behaviour in 1934, there have been a lot of discussions, among which calls for better measurement of attitude and behaviour. Schuman and Johnson (1976) for instance discussed the need to consider conceptual congruence, that is, the expectation that a particular attitude and behaviour should go together versus the empirical finding that they do or do not go together. Ajzen and Fishbein (1977) reviewed the findings from the past decades about the influence of attitudes on behaviour and concluded that previous studies that have observed the attitude-behaviour inconsistency suffered from measurement issues (Ajzen and Fishbein, 1977). They found that these studies did not distinguish between two types of attitudes: general attitudes towards an object versus attitudes towards performing behaviours with respect to an object or targets, that is behavioural intentions and they suffered from two types of inconsistencies: evaluative inconsistencies and literal inconsistencies. These are explained in the following paragraphs and were taken into account when designing the user study for the research.

Evaluative inconsistency occurs when broad attitudes are compared with single behaviours. This is a problem because it is only under certain conditions and/or for certain individuals that general attitudes have strong impact on behaviour. The

principle of aggregation has been said to improve attitude-behaviour consistency and can be applied to the case of evaluative inconsistency (Ajzen and Fishbein, 2005). According to the principle of aggregation, general attitudes fail to predict specific behaviour because of a lack of compatibility in the action, context and time elements. This is because general attitudes identify only the target element whereas specific behaviours involve a particular action directed at the target in a given context and point in time. Therefore, Westin's Privacy Segmentation Index (Kumaraguru and Cranor, 2005) would not be compatible with specific online privacy behaviour. It was seen that while general attitudes are typically poor predictors of individual behaviour, they showed strong correlations with an aggregate measure of behaviour (Fishbein and Ajzen, 1974). Thus identifying a set of behaviours that have evaluative implications in the research and are broadly representative of the domain under investigation would not only increase positive correlations with attitudes and increase measures of reliability but would also ensure that the behavioural criterion has construct validity.

Literal inconsistency is the inconsistency between behavioural intentions and actions. Such inconsistency can be caused if behaviour is not easy to perform as argued by Campbell (1963) or if there is a time interval between measurement of intention and assessment of behaviour, and if intentions change during that time, the intentions will tend to be poor predictors of behaviour. The principle of compatibility that requires that the measures of attitude and behaviour involve exactly the same action, target, context and time elements whether defined at a very specific or at a more general level, can help to improve literal inconsistency (Ajzen and Fishbein, 1977). Just as behavioural aggregation makes it possible to demonstrate strong attitude-behaviour correlations, at the global level, the shift from general attitudes towards behaviour intentions enables the use of the attitude construct to predict single behaviours. Therefore, although end users have privacy attitudes, a lack of behaviour intention would result in low expected behaviour. However relatively low intention-behaviour correlations can also be obtained if intentions are not stable, for instance. In this case, prompting people to form an implementation intention can help to close the attitude-behaviour gap.

Moderators of the attitude-behaviour relationship

From the above it can be said that together with consistent measurements, the structure of attitudes plays an important role in the link between attitude and behaviour. Elements of designs that affect the accessibility, activation and ambivalence of attitudes would consequently affect the attitude-behaviour relationship. Moreover, Stiff and Mongeau (2003) and Ajzen and Fishbein (2005) agree that the attitude-behaviour relationship depends on whether the general attitudes were formed as a result of central or peripheral processing, whether the attitudes were formed as a result of direct experience or second-hand information, whether there is vested interest or involvement with the attitude object and whether the attitude is stable. Designs especially aimed at doing so employ persuasive communication. The paragraphs below discuss how persuasive communication can moderate the attitude-behaviour relationship by interacting with the structure of attitudes.

When attitudes are formed, accessed or activated, cognitive evaluation of an object or situation can occur via central processing or peripheral processing (Augoustinos et al., 2006). Central processing can be triggered by arguments with ample information whereas peripheral processing relies on simplistic associations or cognitive shortcuts of negative and positive attributes to some object, action or situation (Petty and Wegener, 1998). Therefore, by including elements that favour one of these two types of processing, privacy designs might cause individuals with the same attitude to behave differently and vice versa. Another key variable is involvement, that is the extent to which an individual is willing and able to think or elaborate about the position advocated and its supporting materials. When individuals are motivated by the design and able to think about the content of the message, elaboration is high. Elaboration involves cognitive processes such as evaluation, recall, critical judgement and inferential judgement. The degree of elaboration can be taken to be a function of factors such as personal relevance of the topic to the receiver and the presence of distraction.

Direct experience with the object of the attitude influences the attitude-behaviour relationship (Fazio and Zanna, 1981). Therefore privacy attitudes formed through

personal experience with an object or situation will be stronger and more related to subsequent behaviours than privacy attitudes formed through indirect experiences of others. This is because privacy attitudes formed through direct experience are more accessible and hence more able to predict and guide behaviour than those formed through indirect experience. Regan and Fazio's (1977) study of college students' attitudes about a campus housing shortage provided support for this proposition by showing that direct experience moderates the size of the attitude-behaviour correlation (Regan and Fazio, 1977). In Regan and Fazio's experiment, vested interest and ego involvement may also have confounded the effect of direct experience. Sivacek and Crano (1982) found that students in the vested-interest group (those who would not be able to drink for two years or more till they are 21 years old) exhibited a stronger attitude-behaviour correlation than students in the moderate and low vested interest group (Sivacek and Crano, 1982).

Construct differentiation that is the number of different dimensions along which people judge objects and situations, also moderates attitude-behaviour relationship (O'Keefe and Delia, 1981). Limiting construct differentiation of privacy attitude in a given context would limit privacy attitude ambivalence and ensure privacy attitudes are stable. Stable privacy attitudes would be expected to be more frequently reflected in behaviour than unstable ones. Although privacy pragmatist that is individuals who make privacy decisions on a case by case basis can be expected to have more ambivalent attitudes, they might exhibit less ambivalence if similar online contexts have the same privacy designs.

This section provided a discussion on the relationship between attitudes and behaviour. It stressed the importance of measurement and the structure of attitude on the relationship. It follows that elements of online design that impact the structure of attitudes such as persuasive communication and consistent attitude and behaviour measurements could enable positive association between attitudes and behaviour.

3.4 Research Design

In this section a human-computer interaction (HCI) research approach is presented since the human-computer interaction design is a major precursor of usability. Also, having formulated the research strategy in the previous section, a framework is required to not only ensure that the studies conducted to help answer the research questions are valid and reliable, but also to ensure that the studies link and support each other. The section portrays the framework for data collection and analysis. The exploratory part of the research employed a Delphi study and two case studies, whereas the quantitative part involved a user experiment. The section also elaborates on the validity of the research designs.

3.4.1 HCI

HCI is a multidisciplinary subject that has historically branched out of computer science and psychology but the need to cater for the full complexity of people's use of computers means that it also encompasses social science, organisational theories, cognitive ergonomics and philosophy (Caroll, 1997). The following paragraphs discuss the role HCI played at the different stages of the research.

Design of usable online privacy is a difficult task since end users should be able to manage their privacy while using the system for other purposes such as online shopping and social networking (Ackerman and Cranor, 1999). Interactions with online privacy are complex and apart from typical usability requirements such as ease of use, the criteria that would allow end users to manage their privacy seamlessly and make online privacy usable are not known. Privacy needs are subjective and privacy behaviour can be driven by social values, trust, identity and motivation among others. Grounded theory has been found to provide insights that address such complex issues (such as in Pace, 2004; Adams et al., 2005; Razavim and Iverson, 2006). Grounded theory is a method of qualitative research, originally identified within social science as the product of close inspection and analysis of qualitative data (Glaser and Strauss, 1967). It aims to produce new theories that are grounded in the qualitative data gathered during the research. Grounded theory methodology combines systematic levels of abstraction into a framework of interpretation of a phenomenon which can be

iteratively verified and expanded throughout the study (Corbin and Strauss, 2008). It was hence suitable to identify the requirements of usable online privacy mechanisms for the first research question, RQ1.

The research then further tapped into HCI to understand whether existing online privacy mechanisms can be considered to be usable and how the privacy interactions would be perceived by end users. The emphasis was on understanding the communicative attributes of the privacy mechanisms that would enable end users to manage their privacy effectively. Since the aim was to understand and explore rather than measure and manipulate, a qualitative approach to HCI was designed. While the interpretations of the researcher are vital, it was necessary to reduce the influence of the researcher to avoid bias. This was achieved by making use of the rigorous procedures of an inspection method and theoretical principles of privacy management.

Having identified requirements for usable online privacy through grounded theory and explored existing designs, a controlled experiment approach was adopted to examine the privacy behaviour in the context of interactions with persuasive messages. Controlled experiment is an HCI approach that has been adopted from research methods in psychology (Caroll, 1997). It is widely used to evaluate interfaces, styles of interactions and to understand cognition in the context of interactions with systems (Blanford et al., 2008). The question most commonly answered is whether a change in conditions or value of a given variable is linked to a change in another variable. Controlled experiments are hence fitting as the HCI research approach to determine the influence of persuasive communication conditions on privacy behaviour.

3.4.2 Delphi

The Delphi method has been developed as a technique to obtain reliable consensus among a group of experts when judgemental information is required (Okoli and Pawlowski, 2004). It is applied within research as a method of data gathering that collects data from respondents within their domain of expertise. The objectives of the Delphi study employed within this research were to seek out information which may generate consensus and to correlate informed judgements spanning across a wide

range of privacy disciplines in the quest to explore requirements for usable online privacy.

Delphi design

The privacy experts queried came from a variety of privacy disciplines. The Delphi approach hence helped to provide for a multidisciplinary rather than solely a technological or legal perspective. It helped to identify usability enhancement factors emerging from particular privacy focus followed by revision and assessment by a multidisciplinary group. This happened through the iterations of the Delphi with later iterations validating and refining the opinions of the first iterations. The iterative nature of the Delphi is hence an approach to grounded theory through which, as explained in section 3.4.1 above, qualitative findings in the first iteration of investigation are used to design subsequent iterations of a study and in doing so help to thoroughly assess an issue (Adams et al., 2008). Hence experts' opinions identified in the first round of the Delphi were used to design the second questionnaire whose aim was to detect consistency and identify conflicts. As a consequence, the Delphi approach not only produces richer data than surveys and questionnaires but it is also a more rigorous and reliable approach than studies designed with single iteration that do not follow up on initial findings.

The analysis of the Delphi data from the first and second round was performed through grounded theory coding techniques. Coding is an analysis method through which data is broken down, conceptualised and put back together in new ways (Corbin and Strauss, 2008). It involved the initial identification of codes (usability factors) that were then compared to find consistencies and differences. Consistencies between factors revealed a theme and eventually each theme saturated when no new factors related to it could be formed. The coding process contains two analytic procedures: the making of comparisons and the asking of questions which are also a major part of grounded theory. These two procedures help to give concepts precision and specificity (Corbin and Strauss, 2008). The two types of coding schemes that were used within this research were open and axial coding. Although open and axial coding are distinct analytic procedures, during analysis, one usually alternates

between the two modes (Corbin and Strauss, 2008). Open coding allows initial categorisation of information about a phenomenon by segmenting the information. The first step of the analysis was to conceptualise the data; that is break down an observation, a sentence, a paragraph, and give each discrete incident, idea or event a name that stood for or represented a usability factor. Each factor was then compared so that similar factors were given the same name. Once those factors were identified, themes developed by grouping the factors into concepts. The themes could be said to have conceptual power since they pulled together around them other groups of concepts or sub-categories around them. In axial coding, the data from open coding was assembled in new ways. Axial coding puts data back together by making connections between a theme and sub-categories (Corbin and Strauss, 2008). The focus was on specifying a theme in terms of the conditions that gave rise to it, the context in which it was embedded, the action/interactional strategies by which it was handled, managed, carried out and the consequences of those strategies.

Depending on the aims of the research, Delphi studies can be designed as a factor identification Delphi or a ranking Delphi (Skulmoski et al., 2007). In the factor identification Delphi, themes are identified and reviewed without being ranked in terms of importance whereas in the ranking Delphi, participants rank the factors identified. Since the aim was only to identify requirements and not to find out which is more important, a factor identification Delphi was used.

The Delphi approach was however time consuming including waiting times for several rounds of data gathering followed by in-depth analysis. This disadvantage was nonetheless outweighed by the rich qualitative data obtained. The other issue was identifying a group of experts who were willing to participate and motivated to continue participation through all the rounds of the study. Identification of experts was however made easier since the study was launched following a gathering of privacy experts at the IFIP Summer School in 2010.

Validity of Delphi

As discussed in the previous section, the findings of the Delphi study are reliable and valid due to the different rounds that fed into each other to validate the previous

findings. It helped to determine the accuracy of the qualitative findings by taking the specific description and themes back to participants to determine the accuracy of the translated data.

Any bias that the researcher brought to the study was catered by the Delphi study structure which queried participants' opinion and performed systematic coding (several times and inter coder validity) on the initial data collected and took the consolidated opinions collected back to the participants for discussion. The analysis was also explained in a very clear and detailed manner. Moreover, internal validity was achieved within the Delphi by confirming the themes through a second researcher who was provided with the list of codes and participants' responses to perform a run through. The results were cross checked among the two researchers through comparison of the independently derived codes.

Throughout the Delphi study, a diary was maintained with the aim to leave an audit and decision trail. This helped to ensure the rigorousness of the study. To ensure that there was no drift in the definition of codes in the Delphi study, constant comparison was employed. These processes provided an audit trail (consisting of raw data, data reduction, analysis outcomes, data reconstruction and synthesis results such as categories, findings, process notes) and provided for neutrality of findings which helped to ensure the data was free from the biases of the inquirer (Lincoln and Guba, 1985).

3.4.3 Case study

Having gathered experts' opinions about the requirements of designs that would cater for usable online privacy, the research proceeded to find out whether existing designs provided for the main themes of those requirements by answering the second research question (RQ2), that is, 'How usable are online privacy mechanisms?' (How are privacy options communicated to end users? Would end users be able to use the privacy mechanisms to achieve their privacy goals?). A case study approach was designed using the principles of a real world privacy management framework. The following sections reflect on these choices and explain how they were used.

Case study design

Case study research method is an empirical inquiry research method that investigates an existing phenomenon within its current settings and context using multiple sources of evidence (Yin, 2009). Hence the case study method enabled the investigation of the usability of different online privacy mechanisms as close as possible to their context of use. A case can be an event, an entity, an individual or a unit of analysis (Yin, 2009); in this research, a case is an example of privacy mechanism provided online.

Since case studies are concerned with the how and why phenomena happen they supported the investigation of how usable the privacy mechanisms designed online are. Moreover, case-study research is not concerned with the entire aspects of a phenomenon and thus does not aim to generalise a sample to the entire population. Instead, case-studies are intended to focus on a particular issue, feature or unit of analysis (Noor, 2008). This feature of case studies was useful since there was a need to understand different design approaches of designing privacy in depth. Case studies can also cater for embedded-design, that is, multiple units of analysis within a study (Yin, 2009). Within this research two case studies were conducted to investigate two different approaches of designing privacy within online services and each case study had three units of analysis. The case study design can be described as a multiple-case design with multiple units of analysis. This provides for an embedded design approach that includes multiple units of analysis where the aim is to look for consistent patterns of evidence across the units within a case. Embedded designs, by requiring extensive analysis provide more robust results and compelling arguments (Yin, 2009). The downside is however the raised focus on sub-units and loss of higher level (holistic) aspects. This was however resolved through cross-case analysis that was performed in order to identify a trend if any among the different cases. The process generally followed by case studies is shown in Figure 3 below.

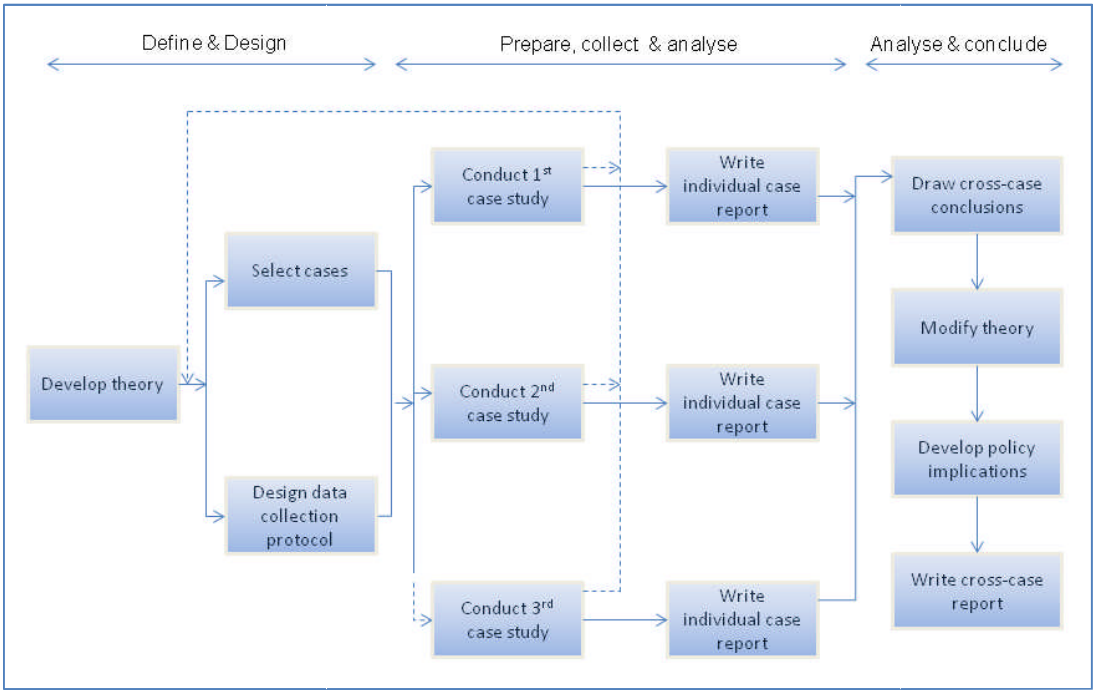


Figure 3: The case study method in general (Yin, 2009)

Since the case-study data collection involved multiple cases, a protocol that helps towards the asking of good questions was required. The protocol helped to avoid interpretation bias by providing the procedures and general rules to be followed. The case study protocol design that is the way the questions were asked followed the procedures of semiotic inspection. Semiotic inspection is an analytical evaluation technique that provides a rigorous approach to inspecting communication within designs. It is further explained in the next section of this chapter. At the heart of the protocol was a set of questions; which were considered as the instrument. The questions acted as reminders of the data to be collected. The questions consisted of those to ask of individual cases, of the pattern of findings across multiple cases, and of the entire study. The questions asked during the inspection relate to the requirements of usable online privacy mechanisms. These requirements are catered by the environment and the individual offline and are depicted by the socio-psychological principles of the Communication Privacy Management theory. The principles describe the seamless ability of individuals to manage their privacy offline that is lacking online. The principles are presented as a theoretical framework that can be used to assess whether online privacy designs are as effective as within offline

interpersonal interactions as discussed in Coopamootoo and Ashenden (2011). It helped to identify communication issues and where changes to communicability of the design of privacy mechanism might enhance usability.

CPM was devised to understand the way people manage private information from a communication perspective, targeting the privacy regulation that takes place through inter personal communication interactions (Petronio, 2002). It is useful in untangling the dialectical tension of being both connected and autonomous. The interplay of needing both privacy and openness allows individuals to make decisions about the way they manage their privacy. To allow for this tension between disclosing and concealing also leads to the need to consider the role of others, for instance the recipient of the information, in privacy management. The theory was applied to two privacy designs to help understand and evaluate the usability of existing designs and to enable the design of privacy solutions that are beyond solely securing protection for the self and restricting access to others. CPM theory is based on five principles of private information management that represent the organising principles interlinking both individuals and collectives (Petronio, 2010).

CPM Principles and evaluation questions

The CPM principles were translated into a list of questions that were used in the qualitative analysis stage. The CPM principles are explained below and the privacy evaluation questions using the CPM lens are provided.

Principle 1 of CPM stipulates that disclosure and privacy form a dialectical tension (Petronio, 2010); that is, if there is no disclosure, privacy management would not be required. When individuals disclose and they know they are disclosing, they usually communicate via some privacy rules. Since disclosure and privacy form a dialectical tension, if end users know or can understand that they are disclosing, they might require and look for privacy mechanisms. This principle corresponds to the notice principle of the EU Electronic Commerce Directive (European Union, 2003) and of the FIPs (Federal Trade Commission, 2000) which say that end users should be given notice of the service provider's information practices before any information is collected from the end users. Notice should be provided in the form of at least some

information about the service collecting personal information, how these will be used, potential recipients, ways by which the information is collected, whether disclosure by end users is voluntary or required and the measures taken by the service provider to ensure protection of end users' personal information. As explained in the paragraphs explaining case study protocol design, a set of questions are useful to guide the case study. From Principle 1 of CPM, the questions that the researcher asked when evaluating the design were: (1) would end users know what they are disclosing, (2) would end users know to whom they are disclosing, and (3) would end users know how they are disclosing (that is what actions cause disclosure)?

Within Principle 2 of CPM, individuals believe they own their personal information and hence have a perception of rightful ownership and a right to control it (Petronio, 2010). They further believe that they are entitled to disclose information or keep it private depending on what seems the best choice for them. Hence for end users to require or use privacy mechanisms they must realise that the design is causing a release of control and ownership. From the design, it would be difficult for the researcher to assess whether end users would realise a release of control and ownership. This principle was hence not used within the analysis.

Principle 3 of CPM stipulates that since individuals own their information and have a right to control it, they should have the means to regulate the flow of information that they define as private through the formation of privacy rules. The need for end users to have the means to exercise control of access to the self and the awareness of the potential consequences of exercising that control had also been highlighted by Dourish (1993). Thus, the questions asked by the researcher as part of the case study protocol when evaluating the design were: (1) would end users have the means to regulate the flow of their disclosures online (that is are privacy mechanisms, tools or features provided to form privacy rules?) and (2) would end users know that these means are available?

Principle 3 however suggests that five criteria: gender, age, motivation, context and risk-benefit are important during privacy rule formation (Petronio, 2010). Since age and gender are characteristics of end users and cannot be controlled by the system

design where as motivation, context of use and awareness of risks and benefits can be influenced by the system design, the next three questions referred to within the case studies were: (3) would end users be motivated to form privacy rules by the interaction design, (4) is there a context for disclosure and (5) are the risks and benefits presented to end users?

According to Principle 4 of CPM, once private information has been disclosed, parties become responsible for co-owning and co-managing the information. This means that for a viable relationship to exist, and to allow smooth interaction between the parties involved in the disclosure, privacy rules must be coordinated through linkages between those disclosing information and the recipients of the information. Linkages can be of different types depending on the balance of information shared between the parties and the balance of power that results. For instance, if end users were to knowingly disclose some personal information to the service provider for the purpose of benefitting from services, the type of linkages formed would be of role type. However if end users did not know that linkages would be formed (personal information disclosed to service provider), the linkages would be of coercive type. Also, during rules coordination, the parties involved negotiate ownership of the information shared and permeability, that is whether others can be linked within the boundary of personal information shared between the two parties and the extent to which they can be linked. For Principle Four, the questions asked by the researcher when evaluating the design were: (1) who is linked within the boundary, (2) what type of links joins them, are they coercive or role linkages, (3) is there ownership negotiation and (4) is there any permeability negotiation?

Principle 5 of CPM stipulates that dissimilar expectations and misunderstandings of privacy parameters can cause conflict in the handling of private information (Petronio, 2010). This turbulence has to be dealt with by re-coordinating personal information boundary rules. Therefore, if end users receive feedback after disclosure they could be aware of turbulence to their desired privacy and proceed to re-coordinate their privacy boundary rules. The translation of this principle into questions used within the case studies is supported by Belloti and Sellen's (1993) recommendations that online privacy mechanisms need to provide feedback and enable end users to perform

assessment of trade-off. The questions asked by the researcher when evaluating the design were: (1) how would the end users know when there is turbulence, how can turbulence be noticed, (2) is there any feedback after disclosure, such as a report of access, and (3) are there methods to deal with turbulence such as re-coordination and re-negotiation of rules?

Validity of case studies

An important aspect of ensuring the robustness of the case study is to use different sources of evidence. Each case study had three units of analysis that is three examples of the technology. Semiotic inspection also consists of the evaluation of help sections, static interfaces and dynamic interactions. In the case-studies, semiotic inspection steps were rigorously followed by looking for the principles of the CPM. This justifies the inferences made since the development of these is at the centre of potential problems in mixed research (Teddlie and Tashakkori, 2003). Heuristic evaluation using the list of requirements derived from the Delphi study was not conducted since heuristic evaluation is highly dependent on the researcher and it would have been hard to evaluate the design for some elements of the list.

Reliability on the other hand refers to the consistency across different researchers and different projects (Creswell, 2009b). For instance, for consistency, it was suggested by Yin (2009) that procedures of case studies should be fully documented. This was ensured in the research by maintaining a detailed case-study protocol and database and checking transcripts to identify obvious transcription mistakes in the case-studies. The protocol was important to increase the reliability across the multiple cases of case study research and to provide guidance in carrying out the data collection.

3.4.4 User experiment

User experiments involve participants performing a task and are usually conducted to verify a theory and provide evidence to support or reject hypotheses derived from the theory. The theoretical foundations of section 3.3.2 helped to advance that persuasive communication employed within online systems can affect privacy behaviour by causing end users to elaborate about privacy, by acting as a cue that affects privacy

behaviour or by motivating end users towards privacy behaviour. The question most commonly answered by controlled experiments is whether there is a significant impact of a change to the value of a certain variable on the value of another variable (Blandford et al., 2008). A user experiment was hence conducted to help answer the third research question that is 'How does persuasive communication impact the effectiveness of online privacy mechanisms?'. By nudging towards privacy behaviour, usability of privacy mechanisms, in terms of effectiveness and user satisfaction, can also be improved.

User experiment design

Apart from observing user actions, user experiments can also involve a qualitative part that queries user information and opinion before and/or after the experimental task. The qualitative part substantiates and supports the quantitative findings. During the research a demographic questionnaire was first set followed by the experimental task. The task was followed by qualitative questions that gathered participants' opinion. A between subject experiment was designed such that each participant took part in only one condition. This was done to avoid practice effects and fatigue from affecting participants' actions.

Validity of user experiment

Validity in quantitative methods represents how well a variable measures what it is supposed to, whether the independent variable is really independent, whether there is a relationship between the independent and dependent variables and whether the findings can be generalized across population, settings and time. These quantitative validity concerns were catered for by the experiment design for instance it was ensured that an aggregate measure of privacy behaviour was compared with general privacy attitude and not disclosure behaviour with attitude. The aggregate measure of behaviour ensured evaluative consistency and construct validity. The effect of the experimental condition and independent variables on user behaviour was statistically analysed to identify significance and the requirements of those statistical tests such as sample size were assured. A discussion of the validity of the user experiment is further undertaken in Chapter 6.

3.5 Research Methods

In this section, the studies undertaken to answer the research questions are introduced. Although further details about the design of each study are included in the chapters that follow, the rationale for the choice of research method involved in data collection and analysis of each study is provided. The table below summarises the research questions, the research approach taken and the studies conducted to answer each research question.

Table 1: Research questions and the studies undertaken to answer them

Research Question	***Method***	***Approach***	***Study #***
What are the requirements for usable online privacy mechanisms?	Delphi	Qualitative exploration	Study 1
How usable are online privacy designs in terms of communication?	Survey of social network users	Qualitative exploration	Study 2
	Cognitive Walkthrough of social network	Qualitative exploration	Study 3
	Semiotic inspection of Internet Browsers	Qualitative exploration	Study 4
	Semiotic inspection of E-Commerce websites	Qualitative exploration	Study 5
How does persuasive communication impact the effectiveness of online privacy mechanisms?	User Study	Quantitative experiment	Studies 6 & 7

3.5.1 Usability requirements: Study 1

As detailed in the research design section, a Delphi study was conducted to answer research question RQ1; that is 'What are the requirements of usable online privacy mechanisms?'. The aim of this study was to explore the key requirements of privacy designs that would ensure that they are effective and usable. The Delphi study is a structure consisting of several iterations that used questionnaires as data collection method and coding and constant comparison as data analysis methods. Questionnaires were used as they enable both the query of opinions through open ended questionnaires and multiple choice questions. Compared to other methods of querying participants for opinions such as focus groups, the questionnaire provided a structured way of asking the same questions to different experts and enabled the researcher to collate and analyse the data fairly easily. Since the questionnaires were sent via email, they supported the property of the Delphi in ensuring participants are anonymous to each other such that the discussion that occurred in the second and third iterations of the Delphi was free from peer influence.

3.5.2 Social network service survey: Study 2

Surveys are widely used data gathering methods that allow investigation of problems in a realistic setting and can be done at a relatively low cost. Surveys also provide easy means of collecting data from a variety of people. During the initial stage of the research a descriptive survey was performed since the aim was to attempt to picture whether and how privacy mechanisms were currently used and how satisfied end users were rather than explaining why they are used in a particular way. A pilot study contributed to answering research question RQ2, that is 'How usable are existing online privacy mechanisms?'. The perspective taken was whether end users were aware of the availability of privacy mechanisms in the most used social network service, Facebook. It was consequently possible to determine whether participants understood the privacy implications within Facebook. This preliminary study helped to guide the direction of research, in particular whether end users could interact with online privacy. This hinted towards whether the social-psychological processes of privacy management were present.

Data was collected through an online questionnaire and analysed through simple addition and percentages. This was appropriate since it was only a pilot study with a small number of participants to gauge whether end users were aware of and used privacy mechanisms that were included in designs.

Previous research has suggested that students' poor awareness of privacy implications while using Facebook would explain the low use of its privacy mechanisms (Govani and Pashley, 2007). This pilot survey however differed from Govani and Pashley (2007) in that it did not aim to find out about awareness of means due to possible privacy consequences but rather awareness of privacy controls due to the design of the privacy interactions. The survey study however was not sufficient on its own to enable evaluation of the usability of online privacy mechanisms.

3.5.3 Social network service cognitive walkthrough: Study 3

Following the survey, a cognitive walkthrough was performed in order to determine whether the design would actually enable end users to understand their privacy implications during disclosure. Cognitive walkthrough takes a relatively structured approach and is designed to uncover usability issues by following a sequence of actions a user would take to perform a set of tasks (Polson, 1992). It is a task-oriented approach in that it considers the goal structure and the ways goals are addressed in completing a task. Cognitive walkthrough is based on the theory of exploratory learning, that is, end users are believed to learn to use a system through exploration, or first time use without formal training (Wharton et al. 1994; Rieman et al. 1995). A cognitive walkthrough evaluates the ease with which a typical user can successfully perform a task using a given design interface (Polson, 1992).

Using the cognitive walkthrough each step necessary to perform a task was evaluated in an attempt to uncover design errors that might interfere with learning by exploration. The cognitive walkthrough had two phases which were the preparatory phase and the analysis phase. In the preparatory phase, the tasks, action sequences for each task, user population and the interface were defined whereas in the second phase, the researcher worked through each action of every task being analysed.

The cognitive walkthrough was used as a follow up to the first pilot study in order to find out whether there was a link between the survey responses and the design of privacy. However, although it has the advantage of being an analytical usability evaluation method that does not require user involvement, it can suffer from evaluator bias (Hertzum and Jacobsen, 2001). It also focused on whether end users would learn to use the system and complete a set of privacy-related tasks. It did not show whether the design would support the social-psychological processes specific to privacy management.

3.5.4 Case study of internet browsers and E-Commerce websites: Studies 4 & 5

Following Study 3, a more rigorous approach to evaluating usability of online privacy mechanisms was designed through the case study framework. The case studies aimed to find out whether the interaction design provided for the requirements of online privacy through the socio-psychological processes of privacy interaction and whether end users could be expected to manage their privacy using the existing interaction designs. In the real world, the environment and individuals cater for the requirements that enable individuals to seamlessly manage their privacy. The requirements that enable seamless privacy management are described by the principles of CPM. The principles of CPM were used to help the research in determining whether online designs would be effective in enabling privacy management and why this is the case. The protocol followed by the case studies were defined by the principles of Communication Privacy Management (explained in research design section above).

Data was collected by evaluating interaction designs through the Semiotic Inspection Method (SIM). SIM is an analytical usability evaluation method involving expert analysis of the quality of the human-computer interactions provided by an interface (de Souza et al., 2006). SIM was chosen over cognitive walkthrough because the latter is not rigorous enough to obtain valid results on why current privacy designs are not usable and are too general for application to privacy human-computer interactions. SIM on the other hand is a semiotic engineering evaluation method that is theory-based and that also does not involve actual users during evaluation (de Souza et al.,

2006). The purpose of theory-based evaluation methods in human-computer interactions is to assess the quality of interfaces and interaction in the light of a given perspective of human-computer interactions. SIM also enables a comparison between different ways of communicating privacy mechanisms that is through the static interface, the dynamic interactions and the supporting help sections which is not provided by cognitive walkthrough. The primary purpose of SIM is to evaluate the communicability of interactive computer artefacts by focusing on user interface meanings expressed by design (de Souza et al., 2010). SIM helps to examine the diversity of signs that users are exposed to while interacting with computing artefacts. The signs present in computer interfaces are words, colours, dialog structures and graphic layouts.

SIM is hence suitable for the research on human-computer interaction evaluation of privacy that allows a communication perspective to be taken. Semiotic engineering views HCI as a "set of unique and contingent instances of meta-communication from designer-to-user" (de Souza et al., 2006, pp.148). While being qualitative and interpretive, semiotic engineering evaluation methods provide the means to facilitate the evaluator's interpretation and assessment of the quality of the meta-communication across the wide scope of human-computer interaction instances. It has been argued that the interpretive results of SIM are objective, can be validated, and are comparable to other accepted methods because of the preparation and validation steps of the inspection method (de Souza et al., 2010).

3.5.5 User Study: Study 6 & 7

After evaluating the communicability of privacy mechanisms and theorising on how persuasive communication would improve usability by aligning privacy behaviour with attitudes, a user experiment was conducted to investigate the influence of different persuasive communication messages. The usability experiment enabled the comparison of user behaviour under different conditions and the framework enabled pre-task and post-task questionnaires to support the quantitative measurements. Moreover, the quantitative findings benefit from reliability offered by statistical analysis. The user experiment is further described in Chapter 6.

3.6 Summary

This chapter illustrated the research strategy consisting of a social science research approach. It was followed by the framework supporting the use of different HCI based design methods at different stages of the research. It described a pragmatic viewpoint as suitable and necessary to both exploring existing privacy designs and assessing the influence of persuasive communication. The chapter is followed by a description of each study conducted to answer the research questions.

Chapter 4:

The real criteria

4.1 Introduction

In Chapter 2, the research gap was identified and research questions shaped. The criteria (requirements) for usable online privacy (from a non-legal and non-technological perspective) are not known and it follows that not knowing the criteria for usable online privacy would mean that evaluation of online privacy mechanisms would not be guided by these criteria. Subsequently proposals for enhancements that follow the evaluations would not ensure that online privacy is usable and effective as a behavioural and interactional process.

Previous research has not determined the requirements of usable privacy from a multidisciplinary perspective and a general context. Therefore the purpose of Study 1 as stated in the Methodology Chapter is to identify and explore the key requirements of usable online privacy from a multidisciplinary perspective. Such a perspective would include requirements that support the socio-psychological nature of privacy management and would provide a template against which online privacy can be evaluated as an interactional process. Study 1 is hence designed to answer the first research question (RQ1): 'What are the requirements for usable online privacy mechanisms?'.

This chapter describes a Delphi study conducted in 2010. The Delphi approach was chosen to allow experts from various privacy research and practice areas to contribute

their differing point of views and to enable a discussion among them through iterative feedback. In the sections below, the Delphi stages are detailed starting with the preparation phase followed by three rounds of design and analysis. The chapter then provides the recommendations before concluding.

4.2 Method

Sections 3.4.2 and 3.5.1 in Chapter 3 provided the rationale for the choice of the Delphi method to answer research question RQ1. In this section, the Delphi participants, procedure design and apparatus used are detailed.

4.2.1 Participants

Delphi studies can consist of either a homogeneous or heterogeneous group of participants depending on the outcome targeted by the research study (Skulmoski et al., 2007). The group chosen is homogeneous since the participants belong to the area of privacy but with specialisations in a variety of privacy disciplines. In 2010, the participants, including academics and practitioners from the UK, Germany, Netherlands, Norway, Switzerland and Italy, were working on European privacy projects and their work was either of a technological, legal, social, design or ethical nature or a combination of these. Having participated in the '2010 Privacy and Identity Management in Europe for Life' Summer School, where the usability issue posed by current online privacy approaches was prominently highlighted, they were at least generally aware of the problem. Moreover, they were chosen since it was believed that usable privacy mechanisms design would benefit more from a holistic approach, that included views from various privacy research and practice disciplines, than a solely technological or legal viewpoint that has been shown to be ineffective (in Chapter 2 Literature Review).

50 participants were targeted and 22 responses were received in the first round. This amount dropped to 17 in the later rounds. The number of received responses was sufficient for a study with homogeneous sample as shown by Skulmoski et al. (2007) in their review of research using the Delphi Method.

4.2.2 Procedure

In this section, the design approach of the three iterations of the Delphi is elaborated. It explains how the three rounds supported and linked to each other.

Round I

The aim of the first round was to identify themes from the responses to an open ended question. The themes were thought to provide common and/or diverging recommendations or requirements for what could make online privacy more usable. The participants were contacted by email (and provided with two weeks to respond with a reminder sent after the first week). The first task for participants consisted of answering an open-ended question followed by their privacy area of focus as shown in figure 4 below:

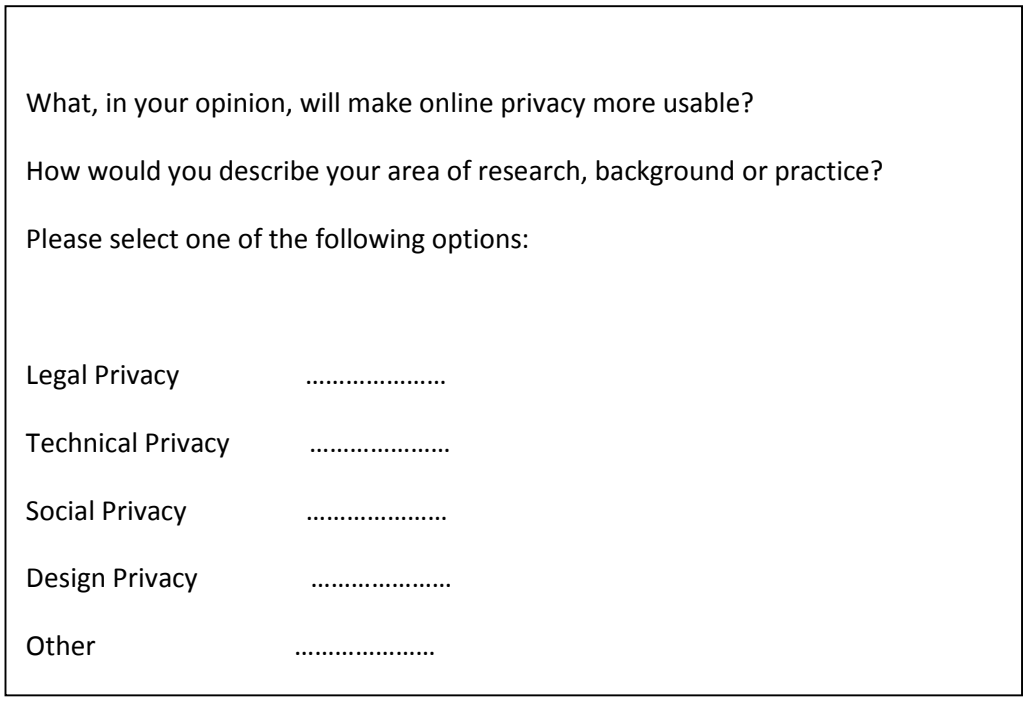


Figure 4: Delphi Round I questions

Round II

The outcome of Round I was analysed and the list of factors identified that had the potential to enhance the usability of privacy online was sent back to participants. A questionnaire was sent to participants and they were asked to denote the importance of each factor on a scale of 1 to 7; 1 being least important and 7 being most important. They were also asked to comment on the categories and factors identified so as to verify whether the identified factors were what they meant in their responses to the previous round of the study and to identify different viewpoints. This process was aimed at identifying agreement, conflicts and overlaps and at reducing the list of factors to a more concise one. The questionnaire of Round II is available in Appendix A.

Round III

A questionnaire was designed for the third round with the aim to explore the conflicting factors and identify solutions or possible agreements on how to resolve the conflicts identified in Round II. The questionnaire was designed with questions requiring Yes/No answers and comments. The third questionnaire is provided in Appendix B.

4.3 Analysis

This section explains how the data collected from the three rounds of the Delphi was analysed. The analysis included coding and comparison of participants' comments.

4.3.1 Round I

From the 22 responses received, one was discarded since the open-ended question section was empty. The 21 responses were then read to identify themes and sub-categories of those themes. The sequence of tasks for the analysis followed the flow in the figure below. Figure 5 below is an adaptation from Creswell's data analysis sequence for qualitative research (Creswell, 2009b).

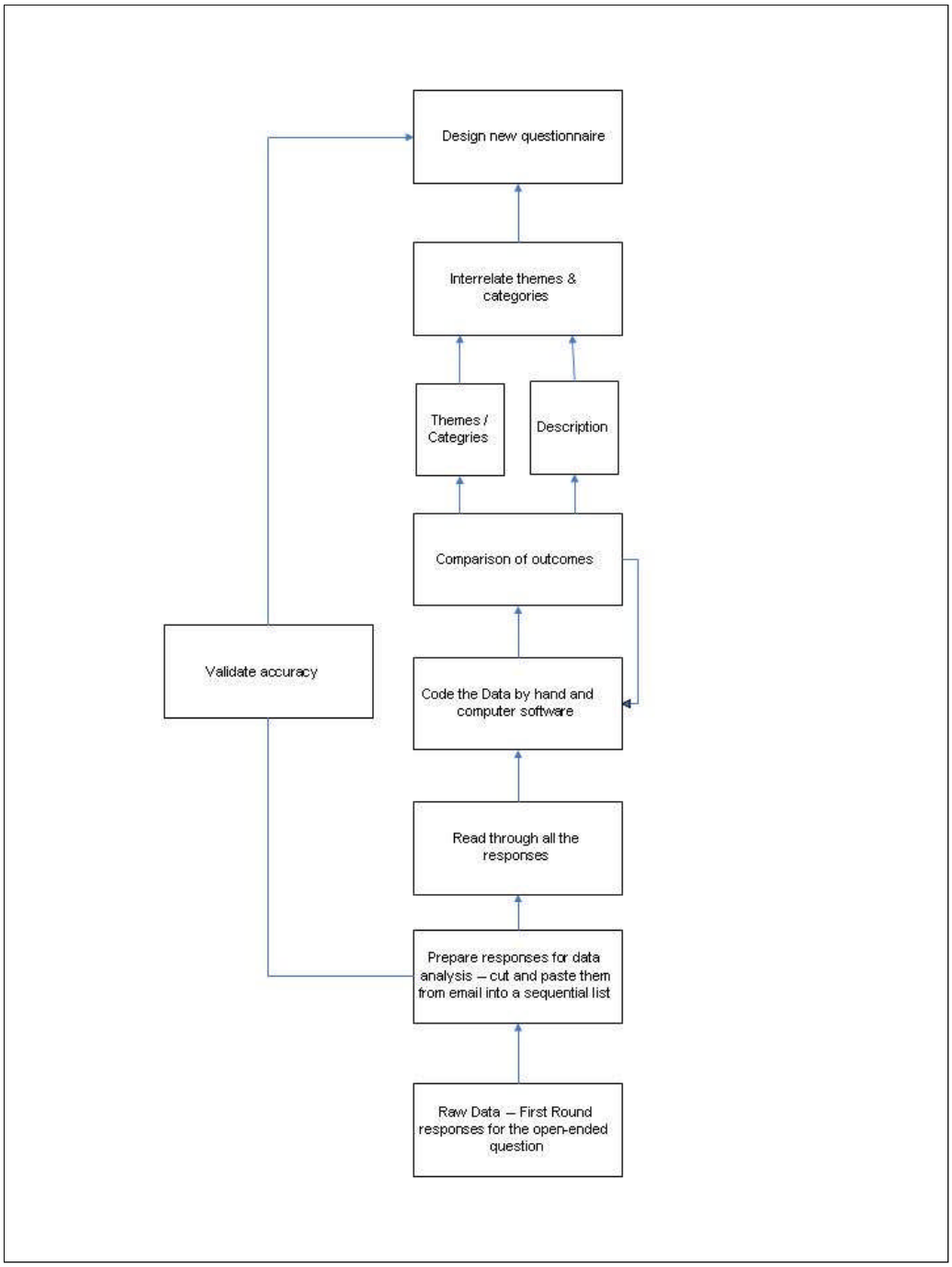


Figure 5: Flow of activities in Round I, adapted from Creswell (2009b)

As shown in the above figure, the responses were first organised and prepared for analysis by sequentially listing the responses according to when they were received. They were then read thoroughly to build a general understanding of the responses and to enable reflection of their meaning. A detailed analysis was then started with the coding process. An inductive coding method was used that is the data was organised

and broken down into an observation, a sentence, a paragraph, and each discrete idea that stood for or represented a usability factor was given a name. Each factor was then compared so that similar factors were grouped according to their conceptual dimension into themes. The coding method used for the first round responses was hence open coding. Coding was performed manually several times to generate the codes afresh followed by a comparison with the last coding session. This approach helped to enhance the reliability of the coding process. Moreover, to make sure that there was no shift in the meaning of codes during the coding process, the data associated with the codes were constantly compared and memos were written about the codes and their definitions. A second researcher was also invited to cross-check the codes, that is to code the responses using the produced set of codes. Practically the same pieces of text were coded with the given codes. This process thus helped to achieve inter-coder agreement. The MAXQDA computer software was also used for another trial at coding so as to identify any mismatch, overlaps or redundancy among the identified codes and to reinforce the reliability of the codes.

4.3.2 Round II

The analysis of this round consisted of reviewing responses to identify the conflicts, agreements and issues raised concerning the need for new factors, the removal of specific factors or the need to merge factors or categories. A comparison was then performed with the responses of Round I so as to understand how the themes would change. Axial coding was used that is the data was assembled in new ways and put back together by making connections between theme and factors.

4.3.3 Round III

The number of ‘Yes’ answers received for each possible response was computed and the comments were consolidated. A summary of the favourite choices that clear the conflicts and the associated comments are provided below.

4.4 Result

In this section, the results of the Delphi are presented. The outcome following each round and the data that feeds into the next round is discussed.

4.4.1 Round I

First, the participants believed that end users need to be in control of their privacy and be able to exercise that control according to the level they desire. They must be able to do so with minimum effort and privacy is usually a secondary goal in online interactions. There was also mention of end users assuming they have a level of privacy. These factors seemed to be associated with end users' characteristics or requirements and were hence grouped under the User theme. The User theme developed from the first round and consisted of the following factors: control, disclosure level, minimum effort, secondary goal and assumption.

This led to the second theme that was about human-computer interaction. The interface must enable end users to understand that while disclosing they are releasing control of their privacy, that is, they need to be aware to whom they are disclosing, and the consequence to privacy. They must also be able to grasp the different possibilities available to maintain their privacy and be able to assess the benefits versus the future risks of disclosing. The interface must also be transparent in informing users about data handling and this information must be made explicit within human-computer interactions. The interface must also cater for different types of end users and the service provider must be responsible and liable to ensure their systems cater for these. The factors forming the Interaction theme are consequently: recipient of disclosure, consequences, privacy possibilities, risks, different user groups, transparent, explicit, service provider liability.

Third, some system usability properties were also identified. They included the need to provide privacy means that are easy to use and standardised privacy interfaces that make it easy for end users to identify privacy options and manage their privacy across systems. Participants also added that privacy should be embedded or implicit within online systems rather than added on. These were grouped under Technology Properties with factors: ease of use, standard methods and embedded privacy.

In addition to usability properties of the system, privacy tool functions that could enhance their usability were also identified. These were default maximum privacy and explicit opt-in to disclose rather than opt-out of disclosure for privacy protection.

The privacy features should also allow minimum data collection, use pseudonyms and be designed in a way such that the business is liable for any misuse. These factors were grouped under Technology Functions: default privacy, explicit opt-in, feedback, pseudonyms, revert back and minimum data collection.

Another key point from the responses was that an attempt to enhance the usability of privacy must include a combination of measures from the user, interaction, technology and legal themes rather than isolated perspectives. The responses of this round highlight that no one single factor could enhance usability of privacy online on their own but should rather be used together.

4.4.2 Round II

In this section, the participants' review of each of the identified themes is discussed. A summary of the outcome of this round is then provided.

User Theme

The list of factors that made up the User theme from Round I included: control, disclosure level, minimum effort, secondary goal and assumption. In Round II, participants believed that end users' requirement for different levels of disclosure should not be considered as a factor for usability enhancement of privacy per se. They also claimed that end users' assumption of a level of privacy online is an issue rather than a factor that is requirement of design for usability enhancement. They added that the issue might be resolved by ensuring end users are aware of what they are sharing, to whom, what happens to their disclosures, and what the future potential risks are. They thought that this solution could be supplemented by forcing service providers to explicitly provide this information.

The fact that end users do not interact online with the primary goal of being private makes privacy a secondary goal for human-computer interactions. Participants stated that privacy should not obstruct or burden the main aim of those interactions and the secondary goal factor might be considered an issue with managing privacy online rather than a design requirement that would impact the usability of online privacy. The factors making up user theme was consequently modified from control,

disclosure level, minimum effort, secondary goal and assumption from Round I to control and minimum effort in Round II.

Interaction Theme

The list of factors that made up the Interaction theme from Round I included: recipient of disclosure, consequences, privacy possibilities, risks, different user groups, transparent, explicit and service provider liability. In Round II, participants gave the control factor very high importance in their ratings. They suggested that control is to be provided in the form of allowing end users to understand and agree who they are sharing their data with, what they are sharing, what the immediate consequences are in terms of how the disclosure is handled and processed and what the potential future risks are. The control factor is hence moved from the user theme to the interaction theme to incorporate recipient of disclosure, consequences and risks.

However, some issues were identified in the responses. For instance, there is a danger that control in design would overburden end users or be obtrusive. It was also highlighted that control could be an unnecessary overhead that would cause end users to resort to default privacy settings. Different end users might also have different control needs such that some may favour convenience over control. However participants provided suggestions for the design of control such as guiding end users so that they can understand the choices that they make and while designs should allow end users to learn about the consequences of disclosure, they should help them make an informed decision rather than frighten them.

The need for interaction design to cater for different user groups received a low importance rating and participants added that it might be too abstract and not make sense in all systems. It was however suggested that the issue might be resolved by having predefined custom levels.

Participants believed that transparency of information processing, explicit awareness of data collection and risk factors are interrelated and the explicit factor is catered by the properties of control. Moreover, explicit disclosure practices refer to transparency also.

Following the review of the Interaction theme, the User theme was modified to include only minimum effort. The Interaction theme developed to include control, privacy possibilities and service provider liability.

Technology Properties Theme

The list of factors that made up the Technology Properties theme from Round I included: ease of use, standard methods and embedded privacy. In Round II, participants suggested that the ease of use factor must be defined with respect to privacy mechanisms to avoid reading as a tautology and not helping design endeavours.

The need for standard interfaces as identified in the first round raised some discussion in the second round. Participants thought that since privacy is context dependent, different interfaces might be needed for different types of systems and services and standard interfaces might also not be convenient for different users. Participants showed concerns that standardisation might lead to high level of vulnerability. The Technology Properties theme thus remains the same following Round II but with some reservations on the implementation approach of these factors.

Technology Functions Theme

The list of factors that made up the Technology Functions theme from Round I included: default privacy, explicit opt-in, feedback, pseudonyms, revert back and minimum data collection. In Round II, the respondents claimed that revert back, minimum data collection and expiration factors were not feasible with the currently available methods of handling personal information. Moreover, it was also suggested that the Technology Functions theme might have emerged due to misunderstanding of the open-ended question of Round I and that these would enhance privacy online rather than usability of privacy. Although usability of privacy is related to enhancing privacy online, 'pseudonymity' for instance, is more a mechanism that provides for privacy than usability. Following participants' review in Round II, the Technology Functions theme, was modified to include only default privacy, explicit opt-in and feedback.

New factors

Participants proposed new factors in Round II. They suggested that a possible solution to the issue that privacy is a secondary goal is to design privacy mechanisms to run in the background so as not to burden end users. The new factor 'background' however posed some dilemmas. Participants claimed that privacy solutions should be visible because if they are not, people will not think about them and hence not use them. Running privacy in the background also poses a problem with the amount of control to provide to end users and the privacy explicitness of designs. Moreover, they added that the decision of how explicit privacy designs should be depends on the types of end users targeted such as whether they value convenience or more control referring to casual versus expert users. Running privacy in the background might however help the minimum effort factor by requiring only a small amount of effort from the user.

A solution for supporting end users' requirements for different disclosure levels and to provide for default privacy without forcing end users to always choose defaults is to design predefined privacy levels that can to some extent be customised. As a result, the two new factors identified in the second round are: background and custom level.

Summary

An important aspect of privacy that came out of this round is that since privacy is dependent on the individual, human computer interactions need to allow users to manage their privacy according to their specific needs. The three elements considered as issues rather than usability factors in Round II (disclosure level, assumption and secondary goal) suggest the need to enable end users to choose and set different levels of privacy and disclosure at different times, to be clear about the privacy provided by the system and the need for a method that integrates privacy interactions within design of online services such that privacy does not burden the main purpose of the system. From the interaction theme, the control afforded to end users was at the centre of the debate. Control is important but should not be obtrusive. A balance is required such that end users are guided to exercise control while learning about the consequences of

different actions and taking into account different user needs. Regarding technology properties, the outcome was that since privacy is context dependent, it would not make sense to have a standardised privacy model or approach that fits all systems. Instead, there is a need to look at the privacy human-computer interactions of different service types. The discussion that occurred due to new factors 'background' and 'custom level', point to the need for privacy to run in parallel to system services and require minimum end user effort. 'Custom level' is hinted as support and guidance to manage control and to provide for different disclosure needs.

4.4.3 Round III

In this section, participants' responses to the conflicts identified in Round II are provided and discussed. The conflicts were presented in the form of questions having a choice of possible answers.

The first conflict and question posed to participants was 'Should privacy run in the background?'. Their preferred outcome from the list of options was that 'privacy solutions should offer predefined privacy options that users can be aware of and control to some extent'. They added that despite running in the background, privacy mechanisms should be flexible enough to allow end users to control their disclosure if they need to, including non-expert end users. Hence while running in the background, it was suggested that privacy designs should provide understanding of how personal data is processed for end users to be aware of their privacy. Also, end users should be able to decide on being informed or not, on what kind of privacy strategy to use and of consequences and impacts. They concluded that there is a need to reduce the learning curve and to provide a better communication method than obtrusion and suggested nudging end users in the 'right' direction by for instance offering a privacy preserving default while allowing users to deviate.

The second question posed to participants in Round III was 'Should privacy designs opt for minimum effort?'. Their preferred outcome was that "predefined privacy levels could provide for minimum effort without too much simplification". The comments for minimum effort referred to its interaction with control as in the previous conflict for the background factor above. Participants were wary that an

interface that requires minimum effort from end users might not allow them to control their privacy and added that the effort required of end users should be balanced with control. Furthermore, they thought that having predefined privacy levels could be a good idea that would help to avoid over simplification of privacy management and also help non tech-savvy end users. However, it was added that predefined settings cannot be generalised to all systems but the design depends on the functions and objectives of systems. It was also mentioned that communication strategies might be required rather than minimum effort.

The third question assessed participants' preference in terms of how control should be provided. Participants selected the four options equally. They thought end users should be guided to understand their choices by making control visible and helping end users to learn about their privacy choices. About the un-obtrusiveness of control, they thought that a smart interface can ensure that control does not interfere with minimum effort. Also, ensuring privacy choices are integrated in the work flow would reduce effort and burden and at the same time make privacy choices clear and understandable.

The fourth question was about the usefulness of standard interfaces that is whether participants thought that standard interfaces could help end users to easily recognise and interpret privacy features. They thought that standards could be adapted to different applications and different groups of people and that vulnerabilities and security problems might arise if standards were not used. Moreover, standards would provide similarities in the form of patterns and choices that can make it easier for end users to comprehend. Also standards would not pose vulnerability threats only if properly done and as standards evolve, the design approach becomes very important and difficult to get right.

In question five, participants were queried for their opinions regarding the use of default privacy settings set to maximum privacy. They thought that security could be bypassed if it was too difficult to achieve a specific goal, hence defaults should be restrictive at first but easy to change to avoid turning off of privacy. Also to avoid

having defaults that obstruct the functionality of systems, there is a need to analyse implementation of default privacy according to context of use.

The discussion that emerged from this round re-iterated the need for privacy to run in the background that is in parallel to the system's services balanced with the need for user control. While the control should be un-obtrusive, it should however provide the possibility for users to decide on being informed and on the mechanisms to choose to manage their privacy. It was further suggested that the learning curve should be reduced with the application of a better communication method than obtrusion. For instance, users could be nudged by privacy preserving defaults that can be changed. By having a smartly designed user interaction, control should be provided that does not interfere with minimum effort.

4.5 Summary

Table 2 shows the list of factors derived from the three rounds of the Delphi study recommended by privacy experts to enhance the usability of privacy online. The table presents a list of key essential factors that should be provided together within privacy design. The themes that categorised the factors during the analysis do not provide benefits to the list at this stage and are consequently taken out.

Table 2: Final list of factors derived from Delphi study

Factor	***Description***
End user control	Includes awareness of disclosure and knowledge of privacy choice
Background	Privacy to run in parallel to system services
Minimum effort	Minimum user effort required to manage privacy
Predefined custom levels	Predefined privacy levels that end users can customise to their needs
Easy	Privacy mechanisms that are easy to use in the context of use
Standard	Standard privacy methods that enable easy recognition of privacy
Default privacy	Maximum default privacy that is easy to alter
Explicit opt-in	Clear about disclosure
Feedback	Feedback of end users' privacy and disclosure

From the table, this study highlighted the need for end user control, the main requirement of online privacy management, to be enabled in designs. Privacy mechanisms should however not interfere with the system services and require only minimum end user effort. It was suggested that such design approach should be carefully thought for each context of use and include elements of helping or nudging end users towards privacy behaviour such as predefined custom privacy levels, standard privacy methods across systems, default privacy, explicit opt-in and feedback.

The requirement for end user control of privacy relates to user involvement and participation in managing their privacy. The direct interaction in managing privacy that is end user privacy behaviour in the context of their online interactions highlights the importance of social psychology for privacy HCI. The latter would enable

exploration of how end users operate in their online environment with regards to privacy and whether designs support control (protection) of privacy and management of disclosures. However firsthand involvement in managing privacy might be tedious and the understanding of how end users behave in response to design elements can also help to propose an approach that alleviates cognitive effort. The following chapter of the thesis explores existing designs for HCI that are supposed to enable privacy behaviour.

4.5 Contributions

This section summarises the contributions of Study 1 to the rest of the research and to the research space. It starts with the substantive contributions and explains innovative aspect of the methodological approach.

4.5.1 Substantive

Study 1 is innovative in enabling identification of usability requirements that is not restricted to a legal or technological perspective. The list can help to guide usability evaluations of privacy designs and help to propose enhancements. However the distinct HCI functions of components of the list can cause conflict in implementation and should be carefully designed. The study also confirmed the direction taken in this research because designs that provide for the suggested requirements would benefit from endeavours aimed at understanding end users' response to privacy designs and their behaviour in the context of their interactions online with regards to their privacy attitudes.

Another contribution of the Delphi study was the discussion of the complexity and challenge of designing usable privacy which was previously identified in the literature review. In addition, the privacy experts suggested a list of ways to cater for the complexity. These suggestions can be viewed to have persuasive characteristics for instance predefined custom privacy levels can provide granular privacy options that would ease end users' privacy by suggesting privacy levels, standard privacy methods across systems would make it easier to detect privacy options, default privacy can act as a persuasive cue or ensure end users have some level of privacy since they might

not alter defaults settings, explicit opt-in can act as a reminder and feedback can serve to reassure or inform end users of their privacy level.

4.5.2 Methodological

The methodological contribution comes from the use of the Delphi approach in HCI research. The iterative survey within the Delphi framework allowed a group of multidisciplinary privacy experts to engage in a small debate about improving usability of privacy online. Not only were privacy experts not queried before but although the Delphi approach has been used in information systems research to untangle complex problems, it has not been used within the online privacy or security research space. As shown in Study 1, the Delphi method provides a valuable approach of collecting and analysing a complex problem and produces rich data.

Chapter 5:

Weaknesses in current privacy approaches

5.1 Introduction

The literature review found that end users cannot use privacy mechanisms effectively online. For usable online privacy, Study 1 proposed the need for end user control coupled with minimum effort among other requirements. These requirements relate to end users' interactions with the privacy design and lead to the second research question which is whether online designs support these requirements (such as end user control). Since these requirements are about end users' interactions with their online environment and their consequent behaviour to manage their privacy, the outcome of Study 1 guides and supports the approach proposed to answer the second research question that is an assessment of whether online designs provide for the social psychological processes of privacy management. The experts who participated in Study 1 also suggested ways of designing privacy that would nudge end users into using privacy mechanisms. However, the list provided by the Delphi is not exhaustive since it was not generated for specific online contexts. While the specific ways of nudging end users could be assessed from online designs, it would be difficult to evaluate privacy designs for end user control and minimum effort requirement without involving end users. This means that the exploratory part of the research aimed at

better understanding whether privacy designs support end users' privacy management processes has to be creatively designed.

The chapter is divided into four main sections that present the four studies designed to answer the second research question (RQ2): 'How usable are existing online privacy mechanisms?'. The research uses analytical evaluations to explore existing privacy design approaches. The first section describes two studies (Studies 2 and 3) aimed at evaluating the most popular social network service, Facebook. Due to weaknesses in the methodology with regards to the context of the study, the second and third sections of the chapter employ a more rigorous approach to answering research question RQ2. Studies 4 and 5 evaluate internet browsers' privacy and E-Commerce websites privacy design respectively. The chapter concludes with the contributions of the analytical evaluation part of the research and the link to the next section of the thesis.

5.2 Evaluation of social network services (Studies 2 & 3)

One of the key processes of enabling end user interaction with privacy design and management of their privacy is awareness of the presence of privacy mechanisms. The first pilot study was a survey, conducted from December 2009 to assess end users' awareness of the privacy mechanisms of Facebook, and to find out whether and how often privacy mechanisms have been used. Another study was designed following the pilot study. It involved a cognitive walkthrough evaluation aimed to find out whether users would be able to use the mechanisms. The survey and analytical usability evaluation enabled exploration of the HCI design of privacy in the social network service for the initial step of managing one's privacy – having the means or privacy mechanisms. This is because for end users to use privacy mechanisms the latter first have to be visible, end users have to know that privacy mechanisms are available and how these can be used to manage their privacy. This section describes the design and findings of Facebook's evaluation.

5.2.1 Study 2 - Survey

The pilot survey study attempted to investigate end users' awareness of the opportunity to use privacy mechanisms to control access to their information and the satisfaction in using the mechanisms. The sections below describe the method including the survey design, the survey analysis and the results.

Method

In this section the method is elaborated. It describes the participants and the survey design.

Participants

The participants of the survey consisted of 9 staff and students of the Department of Informatics and Systems Engineering of Cranfield University. The survey was designed online through Survey Monkey and participants were invited to take part via email. This made the survey easily accessible to participants.

Design

In the first three questions, Westin's Privacy Segmentation Index (Kumaraguru and Cranor 2005) was used to determine the general privacy attitudes of the participants. To find out whether participants were aware of the control they had on their different contents, participants were asked whether they were sure or assumed only them, only their friends, the friends of their friends, their networks or anyone had access to view their profile, to write on their wall, to comment on their pictures and posted contents, to view their albums and photos and to view pictures others posted of them. The survey then investigated whether participants were aware that they could manage the privacy of their profile contents. They were asked to elaborate on how they would protect access or editing of their profile contents on Facebook. Participants were then queried on their frequency of using the privacy features and what they used them for. The last question asked whether they were certain of the controls they applied. The survey is provided in the Appendix C.

Analysis and results

All the participants were found to be privacy pragmatists. A privacy pragmatist, as defined by Westin's Privacy Segmentation Index, is an individual who weighs the benefits of various consumer opportunities and services, protections of public safety or enforcement of personal morality against the degree of intrusiveness of personal information sought or released (Kumaraguru and Cranor, 2005). Although 6 participants claimed to have performed some access control actions, only 2 participants were strongly sure of the outcome of their use of Facebook's privacy whereas 4 were somewhat sure and 2 somewhat not sure. However, of the 6 who were either strongly sure or somewhat sure, only 1 provided a precise response to how they used the privacy features. This allows suggestion that although pragmatists claimed to be sure of the outcome of their actions, they might not clearly understand how the mechanisms could be used.

Moreover, for question 4: 'How sure are you about who can perform each of the following activities on your Facebook profile?', 3 to 6 participants believed that the activities could be performed by only their friends and none of them thought activities could be performed by their networks. This assurance that only one's friends could perform activities on one's profile can be explained by the fact that end users participate in social networks with an audience view in mind as showed by Richter-Lipford et al. (2008) in their study of end users' understanding of privacy settings. In addition, the responses to question 5, 'How would you protect who can access or add to your contents on Facebook?', show that all respondents who answered the question had at least a general knowledge of the availability of security mechanisms in online systems and very few showed specific knowledge for the privacy settings of Facebook.

5.2.2 Study 3 - Cognitive Walkthrough

Following the findings of the pilot survey, a second study was conducted to find out whether end users can be expected to successfully achieve the desired goal that is ensuring the privacy of their personal information while disclosing and interacting in Facebook. A cognitive walkthrough was designed to identify usability issues in the

design of privacy in Facebook. The cognitive walkthrough is a precisely specified procedure for stimulating end users' cognitive processes as they interact with the interface in an effort to accomplish a specific task (Polson, 1992). The sections below describe the design of the cognitive walkthrough followed by its analysis and results.

Design

A cognitive walkthrough evaluates the ease with which a typical user can successfully perform a task using a given design interface (Polson, 1992). A list of specific questions guided the walkthrough such that these reflected a cognitive model that allowed the researcher without extensive training in cognitive psychology to implicitly use the model to analyse the interface. The typical end users and the tasks they would perform, the interface and its responses were described and successful use of privacy mechanisms was defined for the purpose of the walkthrough.

1. Who were the users of the system?

The selected end users for whom this study was conducted were Facebook users who are fluent in using the internet for electronic commerce and social network services. This group of end users was chosen since Facebook was in 2009 and as of now the largest and mostly used social network service globally. Fluency with electronic commerce and social network services use was also assumed since this type of users can be thought to have at least a general prior knowledge of browsing the internet and performing transactions that involve agreeing or consenting to terms of agreements and privacy policies.

2. What tasks were analysed?

Task selection was based on representative tasks (Wharton et al., 1994). Since the aim was to identify issues with usability of the privacy design, that is, issues that might cause ineffective use of the privacy mechanisms included, the criteria used to select representative tasks for the study included:

- Activities most commonly performed on social network services
- Activities resulting in the release of personal information
- Activities claimed to result in privacy issues

- Activities that are beyond the control of end users
- Activities involving the use of privacy mechanisms

Using the above list of criteria, the three selected tasks for analytical evaluation were:

i. Status update

The status update was a social network activity that had resulted in a variety of privacy impacts including jobs lost due to employer access to employees' Facebook profiles (Ostrow, 2009). Also, early in 2010 Facebook added privacy mechanisms to this activity.

ii. Photo-sharing through upload and tag

Bonneau and Preibusch (2009) suggested that photo-sharing on social network services may have been the force driving social network growth, that is an activity much favoured by social network users that increased the amount of interactions and thus the use of the social network services. Photo sharing was also shown through different cases to result in privacy issues such as in the Gilani (2009) case. The problem of sharing and tagging photos of others is exacerbated by the fact that end users who do not benefit from the data protection household exemption, that is, those who do not use the social network only for personal use, can be considered as data controllers.

iii. Comment on others' post

Commenting to other's post though not releasing personal information on one's profile does so on other's profile and the privacy of the information released is highly dependent upon the level of privacy of the profile to which one is commenting. 'Like' of other's post might also release information about one's preferences to people not within one's Facebook 'friends' list, the existence of one's profile and use of social network from which other details can be inferred.

The context for performing the selected tasks was that the end users had more than 150 friends and a default Facebook privacy profile with access to their information as shown in Table 3 below. The number 150 was chosen for the least number of friends for the cognitive walkthrough process since as explained through the Dunbar number

(Dunbar, 2010), it is the cognitive limit to the number of friends one can handle, that is, one can maintain relationships with 150 others and know who each person is and how they relate to each other. It is important in social networks since it relates to 'audience view' sharing as explained by Richter-Lipford et al. (2008) who suggested that end users have a specific and limited audience in mind while sharing personal information.

Table 3: Default Facebook Privacy Settings

Profile information	***Permission***	***Description of profile information***
About me	Everyone	About me refers to the description in one's profile description in one's profile
Personal info	Everyone	Interests, activities, favourites
Birthday	Friends of friends	Date and year of birth
Religious and political views	Friends of friends	Religious and political perspectives
Family and relationship	Everyone	Family members, relationship status, interested in and looking for
Education and Work	Everyone	Schools, universities and workplaces
Photos and videos of me	Friends of friends	Photos and videos you've been tagged in
Photo Albums	Edit settings	Albums of uploaded photos
Posts by me	Everyone	Default setting for status updates, links, notes, photos and videos you post
Allow friends to post on my Wall	Opt-out check	Friends can write on user's profile page
Posts by friends	Friends of friends	Control who can see posts by your friends on your profile
Comment on posts	Only friends	Control who can comment on posts you create

3. What is the correct action sequence for each task?

The action sequence for each of the selected task is described in the next section and involves breaking down the main goal into subordinate goals that flow into actions. The action sequence provides a description of how the end users are expected to view

the task before learning the interface and a description of the sequence of actions that should accomplish the task with the current interface definition. Specific parts of the sequence involving the use of privacy mechanism were chosen for the analysis phase to determine the ease with which end users were expected to use the privacy mechanism in an explorative way.

Analysis and results

During the walkthrough, analysis proceeded by applying the theory of learning by exploration (Wharton et al., 1994) as a story was told and evaluated about whether and why end users would choose the correct action at each step that is by asking the following four questions:

i. Will the user try to achieve the right effect?
ii. Will the user notice that the right action is available?
iii. Will the user associate the correct action with the effect they are trying to achieve?
iv. If the correct action is performed, will the user see that progress is being made toward solution of their task?

For each of the four questions, the common features of success are provided in Table 4 below (Wharton et al., 1994). The three chosen tasks were analysed by answering the four above questions with reference to the control requirement of managing one's privacy.

Table 4: Success features

Questions	*Success Criteria*
Users may know what effect to achieve	Because it is part of their original task Because they have experience using a system Because the system tells them to do it
Users may know an action is available	By experience By seeing some device (e.g. a button) By representation of an action (e.g. a menu entry)
Users may know an action is appropriate for the effect they are trying to achieve	By experience Because the interface provides a prompt or label that connects the action to what they are trying to do Because all other actions look wrong
Users may know things are going ok	By experience By recognising a connection between a system response and what they are trying to do

Task 1: status update with the aim of sharing update with friends only

The description for task one was that end users logged into their profile and were taken to their home page. At the top of this page was a text box displaying "What's on your mind?". End users had to click in the text box and to start typing. They then had to customise access to the typed information. The initial goal was hence to update their profile status with what was on their mind with a group of friends. The action sequence for task 1 is shown in figure 6 below.

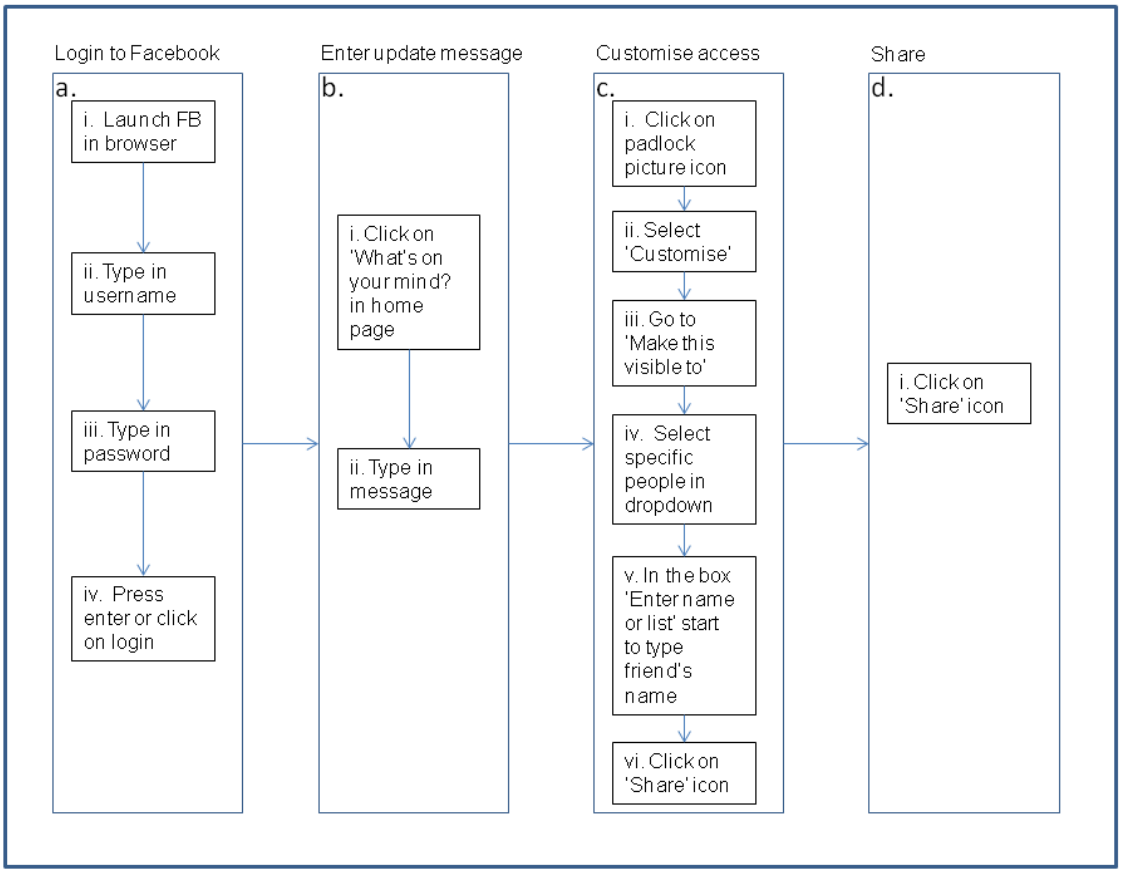


Figure 6: Cognitive walkthrough task 1 action sequence

From task 1, sub-goal c was chosen for the analysis since it involved the use of privacy mechanisms to control access of information. The analysis of action c.i is provided below whilst the analysis for the other actions of c is provided in Task 2's analysis since they are similar. The interface display for action c.i is as shown in the figure below.

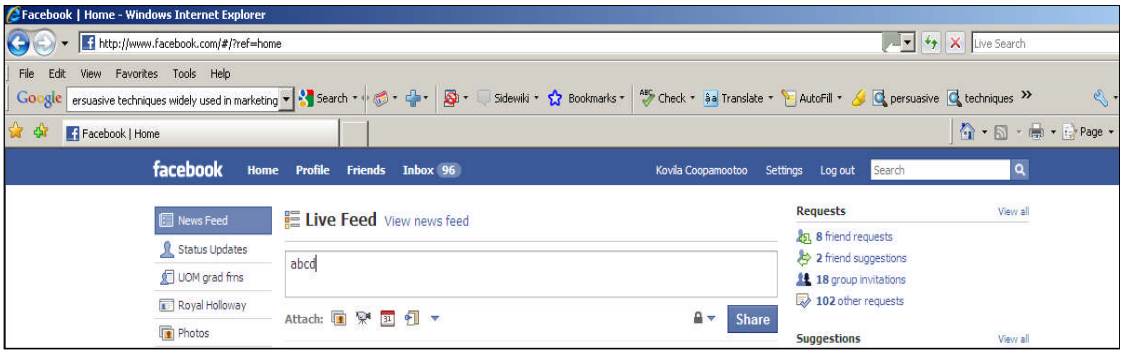


Figure 7: Facebook - Click on Padlock to customise access

For the first question of the analysis, 'Will the user try to achieve the right effect?', end users might not know that clicking the padlock is part of their sub-goal of customising access. A padlock does not provide the label-following strategy to help the user out. That is, there is no link between the end users' task description (customise access of status update) and clicking the padlock icon. Also the system does not tell end users explicitly for instance, 'to share with only these friends click on the padlock to select who to share it with'.

Moreover, since the end users selected for the analysis were fluent in using the internet for electronic commerce transactions and browsing they may think that the padlock picture means the sharing of their update is secure. The padlock icon may thus create a false sense of security by spreading a general and fuzzy secure feeling to end users but it does not initiate any awareness of why it is there, how is can be used and how it can be helpful for privacy. As a consequence, task 1 failed to provide for question i.

For the second question of the analysis, 'Will the user notice that the right action is available?', only end users who can associate a padlock with giving access to whom they want to access their information will know that clicking the padlock is the right action. Task 1 hence failed to provide for question ii.

For the third question of the analysis, 'Will the user associate the correct action with the effect they are trying to achieve?', there is no prompt which tells them so. This meant that Task 1 failed to provide for question iii.

For the fourth question of the analysis, ‘If the correct action is performed, will the user see that progress is being made toward solution of their task?’, the system shows a list with the default privacy setting highlighted and the list of possible choices such as Everyone, Friends and Networks, Friends of Friends, Only Friends and Customise. When selection is clicked or entered, the user will see it as highlighted. Task 1 succeeded in providing for question iv because of the feedback that lets user know that the preferred audience has been selected.

Task 2: Photo-sharing through upload and tag with the aim of sharing photos with specific friends only through internet explorer browser on a desktop or laptop

The description for task 2 is that end users logged into their profile and were taken to their home page. They accessed their wall and clicked on photos tab and created an album. They then customised the access control, uploaded the photos and tagged their Facebook friends to whom the album has been made accessible and after receiving the approval from those friends who would like to be notified before being tagged in a photo. The action sequence for task 2 is shown in figure 5 below.

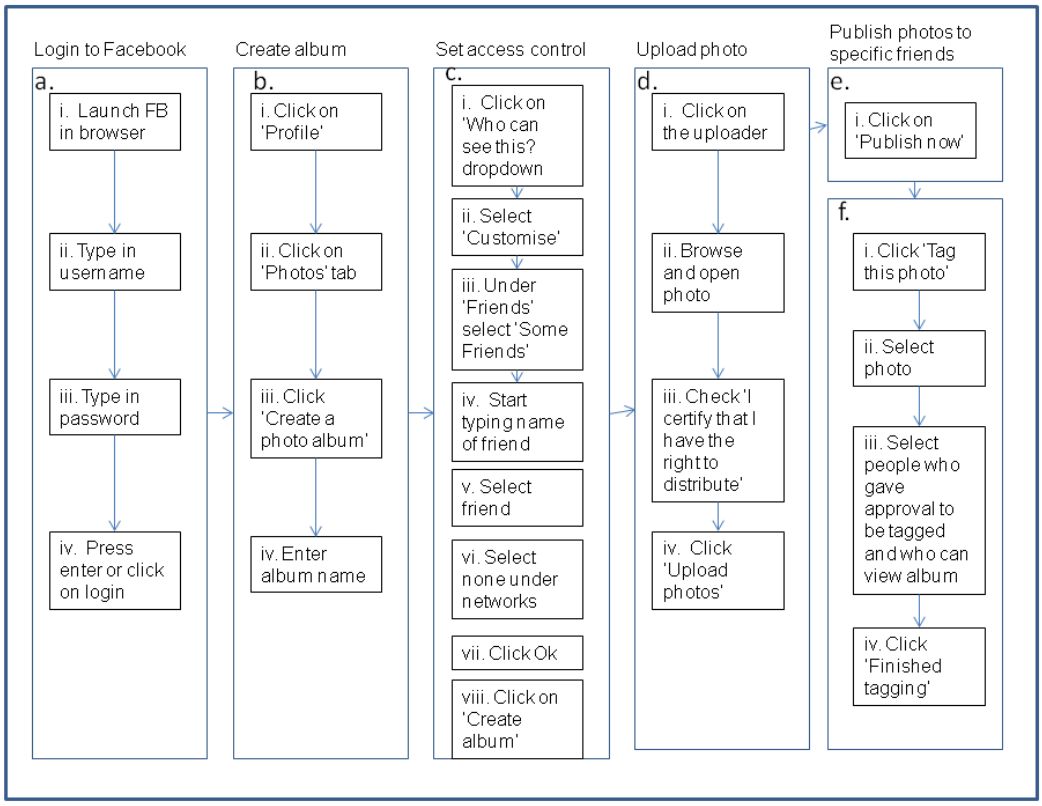


Figure 8: Cognitive walkthrough task 2 action sequence

From task 2, sub-goals c, e, and f were chosen for the analysis since subgoal c involved the use of privacy mechanisms, e involved the publishing of photos and f involved the tagging of people who do not explicitly consent to uploading and tagging photos of them or who may not even be a member of Facebook. The analysis proceeded in the same fashion as for task 1 above. The interface contributing to the analysis is provided in Appendix D.

Task 3: Comment on a friend's post with aim of the comment being viewable only by the friend

The description for task 3 is that end users logged into their profile and were taken to their home page. In the news feed, they clicked on comment beneath a friend's post; left a comment and clicked on 'Comment'. The action sequence for task 3 is shown in figure 9 below.

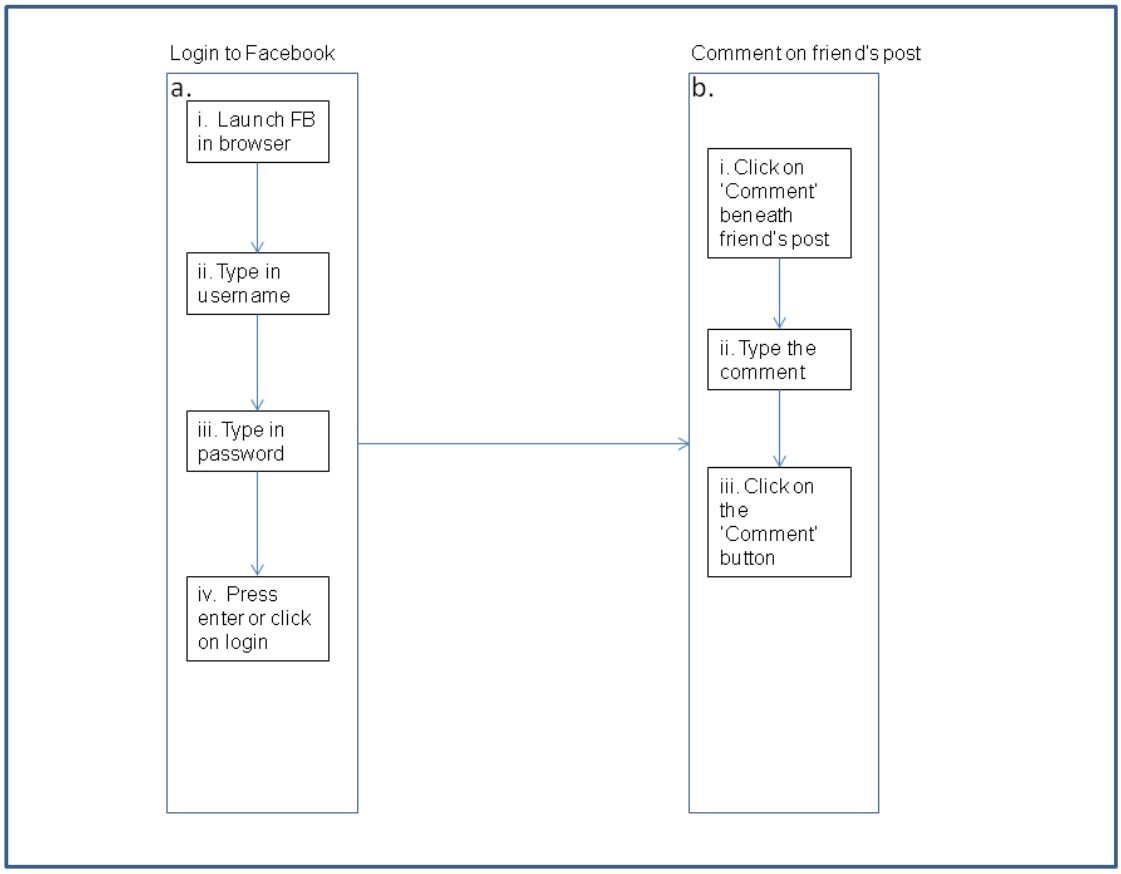


Figure 9: Cognitive walkthrough task 3 action sequence

From task 3, sub-goal b was chosen since it involved the sharing of information beyond one's control. The analysis proceeded in the same fashion as for task 1 above and the interface contributing to the analysis is provided in Appendix D.

The results of the representative tasks' analysis is summarised in the table below. The privacy actions that failed at least one of the four questions are not usable and consequently cause their high level task to be un-usable.

Table 5: Summary of Cognitive Walkthrough results
(F=Failure; S=Success)

		Questions			
Actions	***Action Descriptions***	***Q1***	***Q2***	***Q3***	***Q4***
1.c.i	Click on the padlock picture icon	F	F	F	S
2.c.i	Click on 'Who can see this?' dropdown at the Privacy section	S	S	S	F
2.c.ii	Select 'Customise…'	F	F	S	F
2.c.iii	Under Friends select 'Some Friends'	S	S	S	S
2.c.iv	Click on textbox to start typing name of friend	S	S	S	S
2.c.v	Select the friend or friend list that comes up	S	S	S	S
2.c.vi	Under networks select 'None of my networks' from the dropdown	F	F	F	F
2.c.vii	Click OK to save selections and move to the next action	S	S	S	S
2.c.viii	Click on 'Create Album' to create the album	S	S	S	S
2.e.i	Click on 'Publish now' button	S	F	F	F
2.f.i	Click 'Tag this photo'	F	S	F	F
2.f.ii	Click on Photo	S	S	S	S
2.f.iii	Select those people who provided prior approval to be tagged and to whom the album is accessible	F	F	F	F
2.f.iv	Click 'Finished Tagging'	S	S	S	S
3.b.i	Click on 'Comment' beneath the friend's post	S	S	S	S
3.b.ii	Type the comment	S	S	S	F
3.b.iii	Click on the 'Comment' button	F	F	F	F

5.2.3 Discussion

Although the participants of the survey were people from the Defence and Security School of Cranfield University and might be expected to be familiar with managing security and privacy, they could not explain how they used the privacy mechanisms of Facebook. Also since social network services thrive on disclosure of personal information, the lack of end user awareness of privacy may be the purpose of the design (Bonneau and Preibusch, 2009). The survey study was however limited due to

factors that could not be controlled. For instance, participants' responses about their awareness of privacy mechanisms could be determined by their use of the social network service (and hence a contribution of the HCI design) or by whether participants verified the settings during the survey. Another factor was that participants could have answered what they thought was required of their position through an exaggeration of their awareness. The awareness shown among Facebook end users may also be due to the highly publicised privacy issues and privacy management changes that occurred in the same period the survey was launched and this level of awareness might slope down when privacy issues are not heard of again for some time and with the lack of informed controls in the interface.

From Table 5 above, it was interesting to note that those actions that satisfy all four questions of the cognitive walkthrough analysis have a similarity. They are all part of a task that enable the control of access to information but are not the triggering actions that make end users aware of their availability to decide to use the privacy mechanism. To the contrary it could be suggested that these successful actions help end users to get out of the process of using the privacy mechanisms and help to make the sharing of information successful. Hence while the representative tasks do possess some but not thorough means of ensuring privacy, they do not ensure usable privacy but instead could have been designed as such so as not to encourage the use of the mechanisms.

Moreover, there was a lack of awareness that could allow end users to recognise the availability of privacy mechanisms. This was shown by the high number of failures in questions 1, 2 and 3 for the actions that failed in being usable, that is, the system did not help end users to perform the privacy action, provided a representation of the action or some connection to the action the user was trying to do. Furthermore, most of the actions that failed the evaluation also failed question 4 that is the feedback element. This is because feedback is usually important in a security system to enable verification of the controls applied. Without the feedback in the above actions, end users would not be sure that what the system was allowing them to do is the level of privacy they required. Also, in those actions, feedback would have been useful in

reassuring end users that they are on the right path towards achieving their privacy goal and also making them aware of the importance of these actions.

However the cognitive walkthrough method is limited by evaluator bias and although awareness is a key component of end users' use of privacy mechanisms, it cannot ensure effective online privacy mechanisms on its own. A more systematic and thorough approach of evaluating privacy designs for social-psychological processes of privacy management would be more beneficial to identify the missing components in the design.

5.2.4 Contributions

Substantive

Studies 2 and 3 provided an analysis of Facebook's privacy mechanisms. The contribution of Study 2 is the finding that it was not clear to end users how the privacy mechanisms of Facebook could be used. This was supported by Study 3 that found that the design of the interface did not help end users to identify and learn how to use the privacy mechanisms of Facebook. By enabling a breakdown of the identified tasks into their action sequence and assessing each of the actions, it has been possible to point out which privacy action might require design modifications or be made more persuasive.

Methodological

The methodological contribution to the research space is the cognitive walkthrough analytical evaluation that divided privacy related tasks into their action sequence. This approach helped to identify specific HCI issues in communicating privacy in Facebook.

5.3 Evaluation of internet browsers (Study 4)

In the Delphi study (Study1) experts proposed that end users must be able to control their privacy with minimum effort. They also suggested ways of designing privacy that would nudge end users into using privacy mechanisms. The two previous studies (pilot Study 2 and Study 3) attempted to evaluate Facebook for social-psychological processes of privacy management. They found that the privacy mechanisms of the social network service were not clear to end users since the interface did not enable end users to identify and learn to use privacy mechanisms. Not only was the study prone to researcher bias but the cognitive walkthrough of Study 3 was also limited to awareness and learning to use the privacy mechanisms of Facebook. It did not thoroughly assess the design for elements that would specifically contribute to privacy management.

This section describes a more rigorous method of evaluating online privacy designs through a case-study method that answers research question RQ2, that is, "How usable are online privacy mechanisms?". Communication Privacy Management (CPM) shows the impeccable ability of individuals to manage their privacy in real life. It provides a framework that has been associated with online privacy before (Metzger, 2007). Together with semiotic inspection, CPM provides a more systematic way of evaluating privacy designs for usability requirements. Study 4 analysed the human-computer interaction (HCI) design of the privacy tabs of internet browsers to understand whether end users could be expected to use them. More specifically, semiotic inspection was used together with CPM theory to identify communication breakdowns in the privacy interaction design. It was important to study the usability of privacy mechanisms of internet browsers since apart from providing privacy mechanisms that enable end users to manage their privacy; internet browsers are also the media through which most internet interactions happen. This section starts with the method design followed by the analysis and results before discussing the findings and summarises the contributions of the study.

5.3.1 Methods

Compared to the cognitive walkthrough, the case study design offered a more rigorous analytical evaluation approach. This section portrays the design of the case study procedure followed by a description of the materials used.

Procedure

Guided by the principles of CPM and the procedures of semiotic inspection, a case study was designed to analyse usability through an evaluation of the communicability of the privacy design of internet browsers. Communicability is vital for end users' understanding which in turn contributes to the different components of usability which are ease of use, learnability, memorability, efficiency, minimum errors, acceptability and satisfaction. Semiotic inspection helps to examine the diversity of signs that end users are exposed to while interacting with computing artefacts. The signs present in computer interfaces that were analysed are words, dialog structures and graphic layouts. The three most used internet browsers in 2010 (W3Schools, 2011), that is Internet Explorer 8.0, Firefox 3.6.12 and Google Chrome were evaluated. The data obtained for each browser was then consolidated and analysed before a cross-case analysis was performed.

A case study data collection protocol was designed which consisted of the procedures to follow during data collection and analysis. The backbone of the procedures was the semiotic inspection method consisting mainly of the analysis of privacy related help pages, the static interface of the privacy tab and the dynamic interactions that can be generated following actions from the static interface. Semiotic inspection was systematically carried out in five steps. The first three steps consisted of the inspection of help content, static interface signs and dynamic interaction signs which are the means through which a system communicates to end users. Each of these steps referred to the principles of the CPM to understand whether online privacy was designed and communicated in a way that end users are used to offline as stipulated by the CPM theory. In the fourth step a comparison of the designer-to-user meta-communications identified in the first three steps was performed. In the fifth stage, a substantiated judgement was made of communicative problems that may prevent end

users from effectively using online privacy mechanisms. The flow of the semiotic inspection stages within the case study is shown in figure 10 below. For each internet browser (unit case), data about their communicability of privacy was collected by evaluating each instance of privacy help pages, the static interfaces and the dynamic interactions by analysing the texts and other signs and answering each subordinate question of the CPM principles as detailed in the Methodology Chapter.

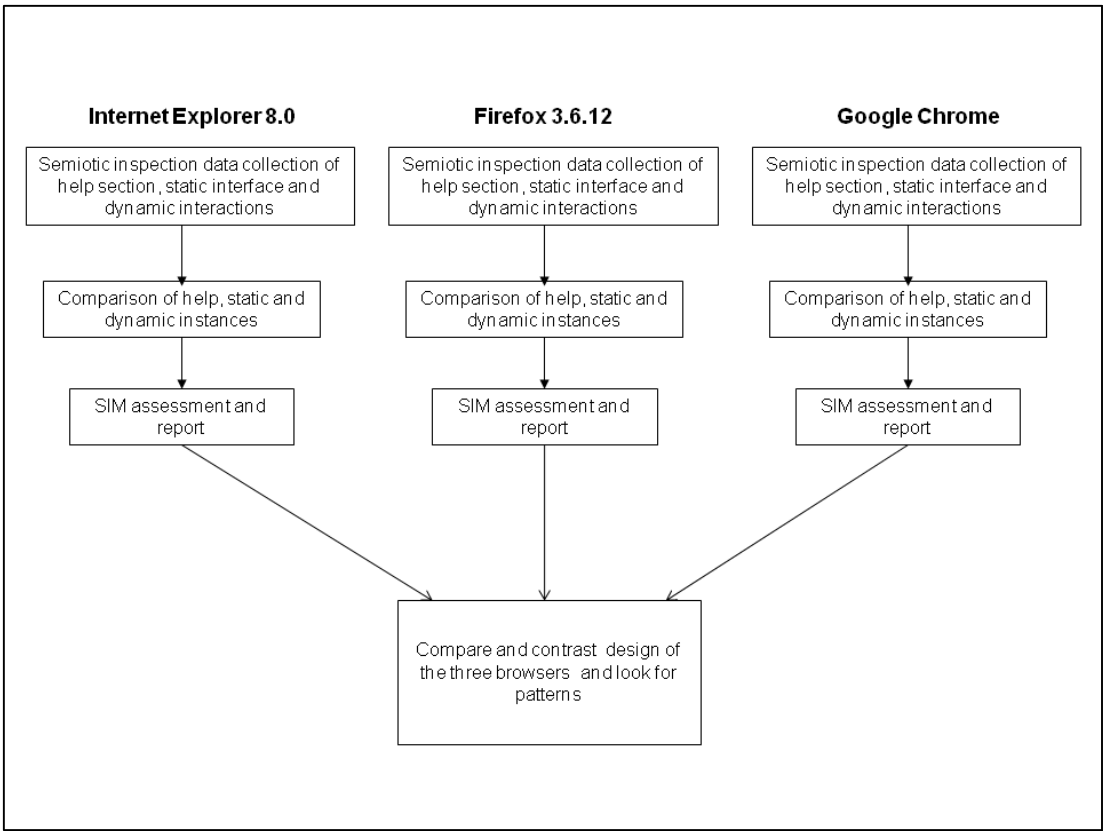


Figure 10: Within-case data collection and analysis and cross-case analysis

Apparatus

The apparatus consisted of the principles of the CPM, as described in the methodology chapter, and the privacy tabs of the three internet browsers Internet Explorer 8.0, Firefox 3.6.12 and Google Chrome. The figures 11, 13 and 15 below show the privacy tabs of each internet browser. These were also the static interface instances. The actions that can be taken from the static interfaces generate the

dynamic interactions. The different dynamic interactions that follow from the static interfaces are shown in figures 12, 14 and 16 below.

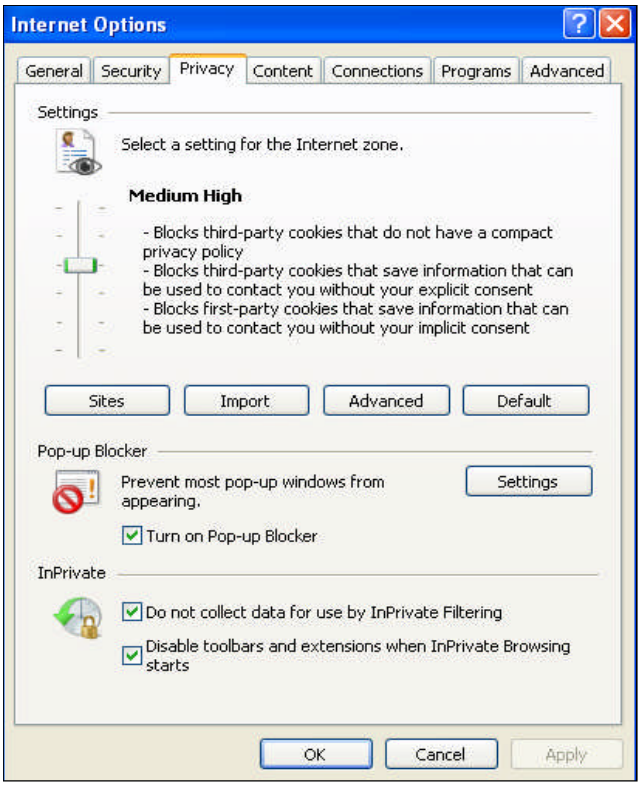


Figure 11: Internet Explorer 8.0 privacy tab

The options that can be selected from the above privacy tab are shown in figure 12. These represent the dynamic interactions of Internet Explorer 8.0's privacy design.

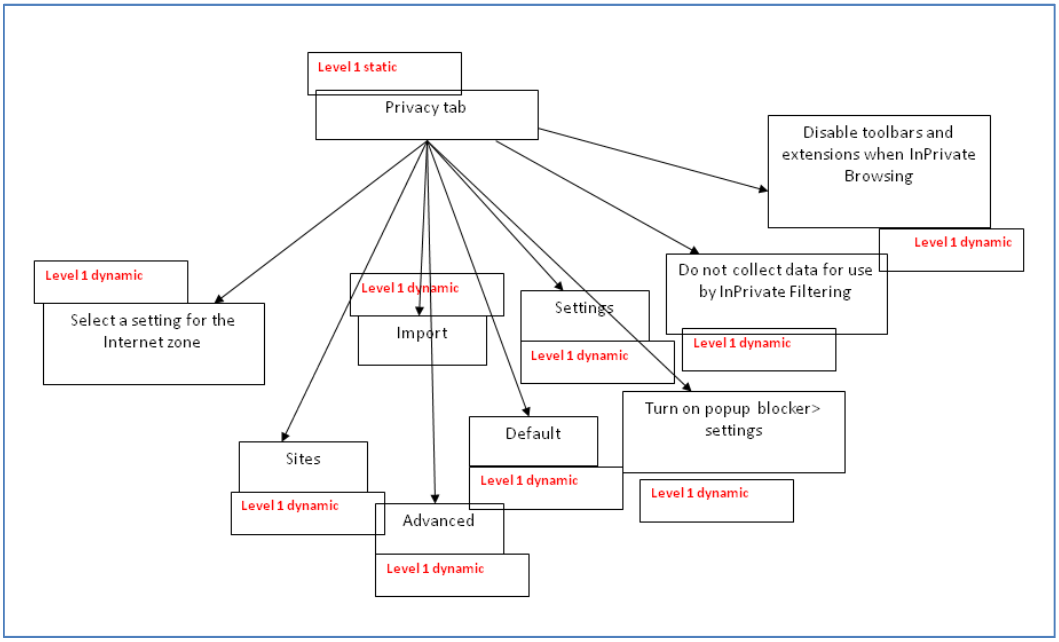


Figure 12: Internet Explorer 8.0 privacy tab's static and dynamic interaction flow

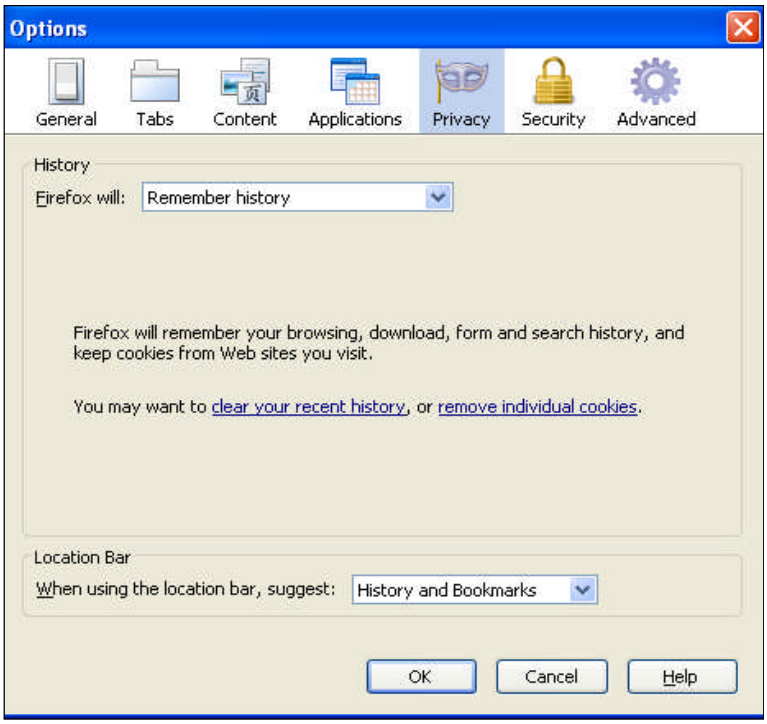


Figure 13: Firefox 3.6.12 privacy tab

The options that can be selected from the above privacy tab are shown in figure 14. These represent the dynamic interactions of Firefox 3.6.12's privacy design.

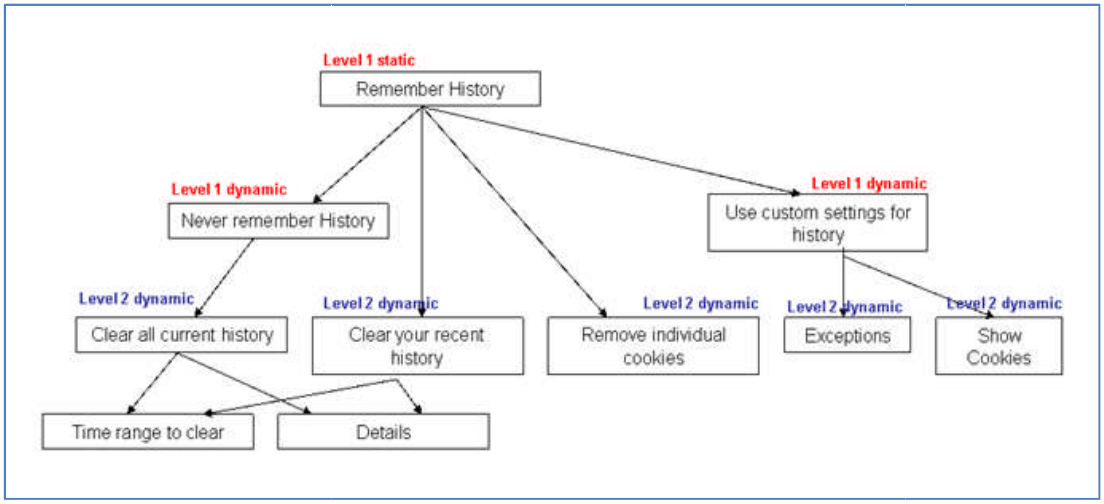


Figure 14: Firefox 3.6.12 privacy tab's static and dynamic interaction flow

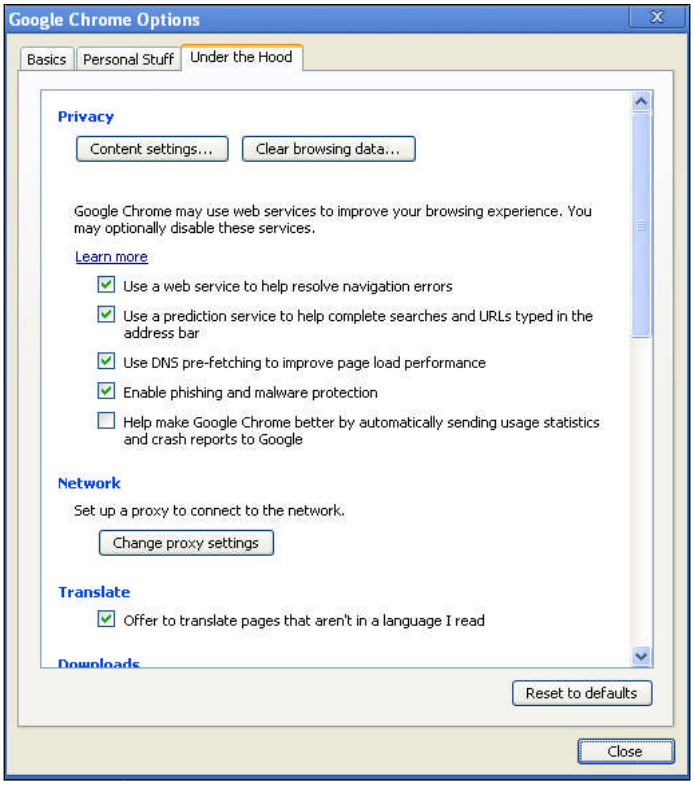


Figure 15: Google Chrome privacy tab

The options that can be selected from the above privacy tab are shown in figure 16. These represent the dynamic interactions of Google Chrome's privacy design.

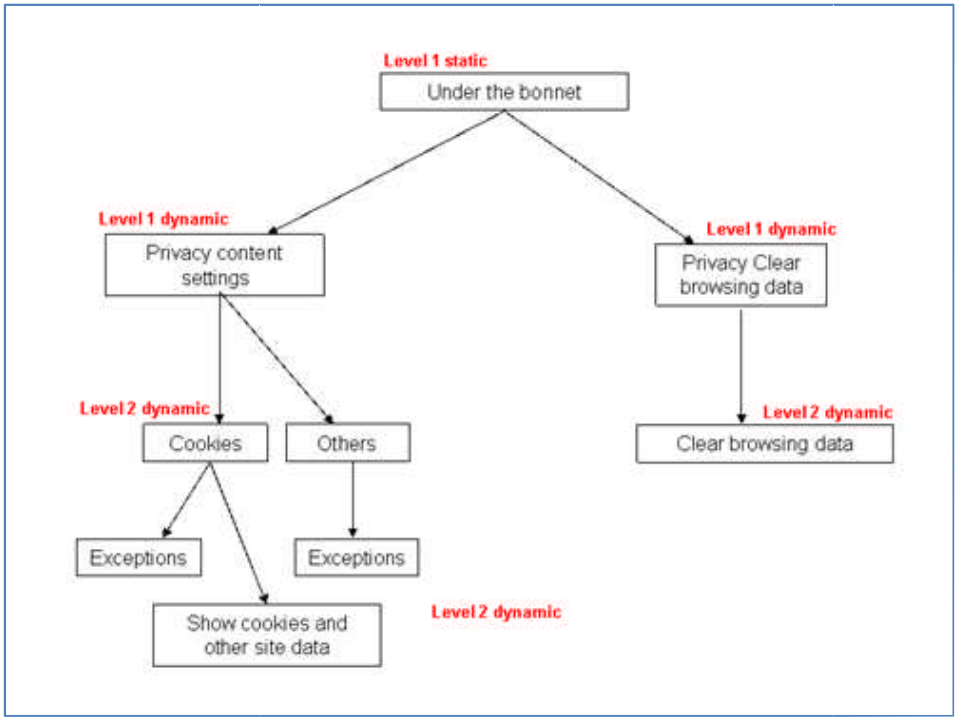


Figure 16: Google Chrome privacy tab's static and dynamic interaction flow

5.3.2 Analysis & Results

This section elaborates on the case study analysis and the results of the study. It starts with the analysis of each unit case followed by a comparison of the three browsers' design of privacy.

Within case analysis

The data collected about the way privacy was communicated through the help pages, static interface and dynamic interactions were consolidated separately. A within-case analysis of the consolidated data (that is comparison between help, static and dynamic communication of privacy) was then performed. The aim was to highlight discrepancies with the principles of CPM which were likely to indicate usability issues.

In the following sections, the analysis for each internet browser is elaborated. The analysis was performed for principles 1, 3, 4 and 5 of CPM. As explained in the Methodology Chapter, analysis for Principle 2 was omitted since it would be difficult to assess help pages, interface and interaction designs for signs that enable end users'

understanding of release of ownership and control of their personal information. To summarise from the Methodology Chapter, Principle 1 asserts that if individuals are aware of disclosure of personal information, they are likely to engage in managing their privacy. During the analysis, the internet browsers were assessed for signs that would enable understanding of disclosure such as what would be disclosed to whom and how. Principle 3 states that individuals have the means to manage their privacy and form privacy rules that are dependent on five different criteria of rule formation. These criteria are gender, age, context, motivation and risk and benefit of disclosure. During the analysis, internet browsers were assessed for the availability of privacy mechanisms, whether the context of disclosure was apparent, whether the system motivated end users to form privacy rules and whether the risks and benefits of disclosure were clear. Gender and age of end users do not depend on the system, they were hence not taken into account in the analysis. Principle 4 states that during privacy rules formation, end users negotiate and coordinate ownership and permeability rights of their personal information. Links of role or coercive nature can be formed with end users' personal boundary. During the analysis, internet browsers were assessed for signs that would enable end users to negotiate who will own their data and how personal information can be shared with others. Principle 5 claims that after disclosure, turbulence to personal boundaries can happen when recipients of personal information do not abide to privacy rules. When turbulence happens, individuals are aware of these and they have the means to deal with the turbulence. During the analysis, internet browsers were evaluated for signs of feedback following disclosure, ways of informing end users in case turbulence happened and ways for end users to manage turbulence.

Internet Explorer

Principle 1: Awareness of disclosure through what is disclosed, to whom and how.

Internet Explorer 8.0 did not communicate Principle 1 of the CPM that is awareness of disclosure, effectively to the end users. This was shown by the contradiction between help pages, the static interface and dynamic interactions, a lack of clarity and

preciseness and the confusing information in the dynamic interactions. Table 6 below gives a summary of how Internet Explorer 8.0 provides for the elements of Principle 1.

Table 6: Would end users be aware of disclosure through Internet Explorer 8.0?

Principle 1	***Help***	***Static***	***Dynamic***
What	✓	x	x
Who	x	x	x
How	x	x	x

The help pages were clear in what would be disclosed but limited to the examples given. The help pages did not inform end users about how they would be disclosing nor to whom whilst the static interface suggested disclosure would happen via cookies without explaining how and what cookies are. The dynamic interactions did not provide support for what would be disclosed while the recipients of disclosure appeared to vary in different instances between websites, third-party cookies or no information. Since the help pages were not directly linked to the static and dynamic parts, the different communication templates would not support each other in helping internet explorer end users in being aware of disclosure.

Principle 3: Means to regulate the flow of information online, awareness of these means and criteria for privacy rules.

Internet Explorer 8.0 did not satisfy the third principle of CPM. This is shown in table 7 below.

Table 7: Does Internet Explorer 8.0 provide means to manage privacy, awareness of means and criteria for rule formation?

Principle 3	***Help***	***Static***	***Dynamic***
Means	✓	✓	✓
Awareness of means	✓	x	x
Motivation cues	x	x	x
Context information	x	x	x
Risk/Benefit	x	x	x

From the help pages, the means were available to manage one's privacy. However, elements that support rule formation as explained in Chapter 2 such as motivating cues, context of disclosure and risk-benefit of disclosure were partly provided or were not clearly present. End users would not understand why to use the privacy mechanisms. Furthermore, for the static interface, means were available to regulate the flow of disclosure but to understand that privacy mechanisms were available end users would have to relate the interface to disclosure which might not be easy. Although the actions possible from the static interface could motivate end users towards privacy rule formation, these effects would be counteracted by a lack of explanation in the interface. The static interface corroborated with the help section in the lack of context and risks and benefits. A similar trend to the static interface was observed in the dynamic interactions, that is means to manage privacy were available but there was no information to relate these to disclosure, there were no cues that could motivate end users to form privacy rules and the context and risk-benefits information were missing. The three media of communication were consistent in providing privacy means without explanation of use, in not motivating to form privacy rules, in having no relation to the context of disclosure and in not enabling a risk-benefit assessment.

Principle 4: Disclosure causes linkages to be set up within boundaries, and requires coordination of ownership and permeability rights.

For Principle 4, there was some consistency in what was communicated between the three meta-communication templates (the help pages, static interface and dynamic interactions), especially between the help section and dynamic interactions. Internet Explorer 8.0 however did not provide for personal boundary negotiation as advocated by Principle 4 of CPM. Table 8 below provides a summary of how Internet Explorer 8.0 provides for the elements of Principle 4.

Table 8: Does Internet Explorer 8.0 provide for awareness of links to end users boundary and negotiation?

Principle 4	***Help***	***Static***	***Dynamic***
Who is linked	✓	✓	✓
Type of links	Role links if end users understand they disclose to service provider in order to benefit from services		
Ownership negotiation	x	x	x
Permeability negotiation	x	x	x

From the help section, it could be understood that first and third party websites would be linked to end users' personal boundary. This was not mentioned in the static interface but was present in the dynamic interactions. Dynamic interactions included recipients of personal information, hence links to personal boundary such as first and third party cookies, pop-ups and websites. If end users can understand what first and third party websites, cookies and pop-ups meant and decided to allow access, the disclosure would enable the service provider to perform its role of providing services. However, if end users do not understand the implications of disclosing to these recipients, the linkages would be of coercive nature. Moreover, the three meta-communication templates provided no clues about who would own the data accessed by cookies, pop-ups and permeability negotiation was completely absent as in the help pages and static interface above.

Principle 5: Awareness of Turbulence

Apart from not enabling end users to coordinate access to their personal boundary as described in the analysis for the previous principle, Internet Explorer 8.0 also did not provide for the possibility to be aware of turbulence to privacy rules as shown in table 9 below.

Table 9: Does internet explorer 8.0 provide for turbulence awareness, means and feedback following disclosure?

Principle 5	***Help***	***Static***	***Dynamic***
Awareness of turbulence	x	x	x
Feedback after disclosure	x	x	x
Means to deal with turbulence	x	x	x

End users would not know about turbulence to their boundaries except for the hint in the help pages about the information bar when the computer is at risk. There was no report of access since disclosure did not happen at any point within all the meta-communication templates. Also, apart from one instance in the help pages, 'How can I keep websites from changing my default search provider?', there was no method to deal with turbulence.

Firefox

Principle 1: Awareness of disclosure through what is disclosed, to whom and how.

Firefox 3.6.12 did not communicate Principle 1 of CPM clearly to end users. By highlighting the management role of Firefox and not showing that disclosure happened or could happen, Firefox contributed to the ineffective use of its privacy mechanisms. Table 10 below offers a summary of how Firefox3.6.12 provides the elements of Principle 1.

Table 10: Would end users be aware of disclosure through Firefox 3.6.12?

Principle 1	***Help***	***Static***	***Dynamic***
What	✓	x	x
Who	x	x	x
How	✓	x	x

Firefox's help pages provided a limited list of what type of personal information would be disclosed to it for management. The help pages indicated that disclosure would be made to Firefox which would happen when visiting websites and when downloading and entering information in forms. The static interface corroborated the managing characteristics of Firefox. The dynamic interactions however provided a list of what would be disclosed without explanation of what the list contents meant. Moreover, since dynamic interactions referred to privacy actions separated from disclosure, end users would not know to whom they would be disclosing and how they would do so.

Principle 3: Means to regulate the flow of information online, awareness of these means and criteria for privacy rules.

Although means were available to manage disclosure, the meta-communication templates (the help pages, static interface and dynamic interactions) were not consistent and Firefox 3.6.12 failed to cater for Principle 3 of the CPM by not making the availability of means clear in its static interface and dynamic interactions. Elements that could help privacy rule formation such as motivating cues, context and risk-benefit information were not consistently present. This is shown in table 11 below.

Table 11: Does Firefox 3.6.12 provide means to manage privacy, awareness of means and criteria for rule formation?

Principle 3	***Help***	***Static***	***Dynamic***
Means	✓	✓	✓
Awareness of means	✓	x	x
Motivation cues	✓	x	x
Context information	x	✓	✓
Risk/Benefit	x	x	x

The help pages provided the means to regulate the flow of information. The clearly displayed text and pictures could help make end users aware of the presence of privacy mechanisms and could also act as a motivating factor. These were however missing from the static interface. As for the dynamic interactions, they might trigger some end user awareness of the presence of privacy means, but the lack of details about their aim could cause end users to fail to recognise their availability. The help section did not point to the context of disclosure whereas the static and dynamic templates only referred to browsing in general.

Principle 4: Disclosure causes linkages to be set up within boundaries, and requires coordination of ownership and permeability rights.

Firefox 3.6.12 did not provide for Principle 4 of CPM. This is shown in table 12 below.

Table 12: Does Firefox 3.6.12 provide for awareness of links to end users boundary and negotiation?

Principle 4	***Help***	***Static***	***Dynamic***
Who is linked	x	x	x
Type of links	Role is end users understand they disclose to service provider in order to benefit from services		
Ownership negotiation	x	x	x
Permeability negotiation	x	x	x

The Help pages and the static interface communicated the same information that is that links were formed with Firefox who managed information for end users. This would be role linkages according to CPM. Firefox would manage information for end users and would be an intermediary. This was not made clear to end users. Firefox also did not provide for boundary coordination as per principle 4 of the CPM. There were also no clues about who would own the disclosures and how they could be shared with others. This could create the false assumption of fully owning one's information.

However one of the dynamic interactions: "exceptions" involved a privacy rule that required coordination. The linkages that could be formed for "exceptions" would be a voluntary link with websites whereas the others were actions that would strengthen role linkages. But as in the help section and the static interface, there were no ownership and permeability rights negotiation.

Principle 5: Awareness of Turbulence

In general Firefox did not provide feedback after disclosure, ways to be aware of turbulence and means to deal with turbulence. This is shown in table 13 below.

Table 13: Does Firefox 3.6.12 provide for turbulence awareness, means and feedback following disclosure?

Principle 5	***Help***	***Static***	***Dynamic***
Awareness of turbulence	x	x	x
Feedback after disclosure	x	x	x
Means to deal with turbulence	x	x	x

There was only one exception among dynamic interactions. If end users selected 'ask me every time', during browsing they would be prompted when websites required more access hence providing awareness of boundary turbulence with the browsing website. However, from analysis for Principle 4, boundary formation would be

established with Firefox. It was hence ambiguous whether disclosure would be made to Firefox or browsing website. Turbulence with Firefox would not be noticed by the end users and that with websites might or might not be seen when browsing.

Google Chrome

Principle 1: Awareness of disclosure through what is disclosed, to whom and how.

Google Chrome was not consistent in its design of principle 1 of CPM. This is shown in table 14 below.

Table 14: Would end users be aware of disclosure through Google Chrome?

Principle 1	***Help***	***Static***	***Dynamic***
What	✓	x	x
Who	✓	✓	✓
How	✓	Infer from block and allow	

Google Chrome communicated Principle 1 of the CPM in its help section. The help section was clear about what would be disclosed to whom and how disclosure would happen. However in the static interface and dynamic interactions, there was a lack of information and clues that could enable end users to understand when disclosure could happen. The static interface only indicated that disclosure was made to Google but not what was disclosed and how. The only information that could be found in dynamic interactions about what would be disclosed was physical location. For some of the interactions information was not provided about recipient of disclosure while for others the recipients were websites and third party cookies. There were no clues for how disclosure could happen.

Principle 3: Means to regulate the flow of information online, awareness of these means and criteria for privacy rules.

Google Chrome was quite consistent in its static and dynamic instances in terms of not providing information that privacy mechanisms were available, not relating to

context of disclosure, and not providing risk-benefit understanding. This is shown in the table below.

Table 15: Does Google Chrome provide means to manage privacy, awareness of means and criteria for rule formation?

Principle 3	***Help***	***Static***	***Dynamic***
Means	✓	✓	✓
Awareness of means	✓	x	x
Motivation cues	✓	x	x
Context information	✓	✓	✓
Risk/Benefit	x	x	x

The help page of Google Chrome provided privacy means and explanations of the need for disclosures only rather than explaining the privacy means together with the disclosures. Motivating cues to form privacy rules was not existent apart from the contents of the video. The context of disclosure was browsing and while benefits of disclosure were highlighted, risks were not. However, Google Chrome provided information about privacy means, motivation factor, some contextual details and risk and benefits information in the video embedded within the help page.

Principle 4: Disclosure causes linkages to be set up within boundaries, and requires coordination of ownership and permeability rights.

The links that would be formed with the personal boundary involved different recipients in the different communication media: browser sites and Google services in the help section, Google Chrome in the static interface and sites and third party cookies in dynamic interactions. The links formed were of role type and were consistent throughout the three meta-communication templates. Moreover, all three media did not allow negotiation of ownership and permeability rights as shown in table 16 below.

Table 16: Does Google Chrome provide for awareness of links to end users boundary and negotiation?

Principle 4	***Help***	***Static***	***Dynamic***
Who is linked	✓	✓	✓
Type of links	Role is end users understand they disclose to service provider in order to benefit from services		
Ownership negotiation	x	x	x
Permeability negotiation	x	x	x

Principle 5: Awareness of Turbulence

Google Chrome did not provide means that would let end users know of turbulence in all three meta-communication templates. However, it can provide feedback when disclosure happens in two dynamic instances if end users selected to be notified whenever a website access their information.

Table 17: Does Google Chrome provide for turbulence awareness, means and feedback following disclosure?

Principle 5	***Help***	***Static***	***Dynamic***
Awareness of turbulence	x	x	x
Feedback after disclosure	x	x	✓
Means to deal with turbulence	x	x	x

Cross Case analysis

Cross-case analysis was performed in order to identify a trend if any among the different cases (internet browsers) in terms of each principle. For instance, the cross case analysis aimed to find out whether the principles were communicated in help pages rather than static interface and dynamic interactions.

Principle 1:

What

A cross-case analysis of the data collected for Principle 1 revealed that internet browsers provided clearer information about what would be disclosed within their help documentation compared to within their static interface and dynamic interactions. In its static interfaces, Internet Explorer 8.0 indicated that cookies and pop-ups would be disclosed. However the meaning of these and their implications were lacking. Firefox on the other hand highlighted the management of history details but not disclosure whereas Google Chrome gave no mention of what would be disclosed. A lack of clear information about what would be disclosed in all the three browsers would make it hard for end users to understand that disclosure would happen. For instance, Internet Explorer ought to explain what cookies and pop-ups are, Firefox ought to clear whether disclosure happens to Firefox or whether the latter is an intermediary and what history details imply. Google Chrome ought to define the type of information (with explanations) that will be disclosed. Dynamic interactions in the three browsers are quite confusing in terms of what would disclosed to one exception only in Google Chrome.

To Whom

Google Chrome provided more information about the recipient of disclosed information compared to Internet Explorer 8.0. Internet Explorer did not explain what cookies and third party cookies are. Moreover in Firefox 3.6.12 there was no information on who would receive the disclosed information since the management role of Firefox was highlighted without disclosure details. However, all three browsers provided slightly more information in the help documentation compared to within the static interfaces and dynamic interactions.

How

Whilst Internet Explorer 8.0 gave no information on how disclosure would happen, Firefox and Chrome provided more information in the help documentation. Firefox

did not provide any in the static and dynamic instances whereas Google Chrome required end users to infer from the words “Block” and “Allow”.

Summary: In general, internet browsers provided limited information about what would be disclosed in their help section but did not provide clear or un-confusing information in their static interfaces and dynamic interactions that is there was no clear information of what would be disclosed to whom in which situation in all of the cases of help, static interface and dynamic interactions. Part of these were scattered around in the different instances and were not consistent. More information was provided in help which was not easily accessible from the static interface and the dynamic interactions. Since privacy and disclosure are in a dialectical tension according to Principle 1, the absence of disclosure information at the point where end users are engaged with the system would make it difficult for end users to understand that they are disclosing personal information and hence cause the use of privacy mechanisms to be redundant.

Principle 3:

Availability and awareness of means

All three browsers provided the means to regulate information flow through their meta-communication media but the problem was with awareness of the availability of these means. The help section of Internet Explorer and Firefox provided awareness of availability of the means but Google Chrome concentrated on explaining the aim of disclosures except in its video. However all three browsers failed to show the existence of these means in the static and dynamic interfaces. Hence if end users had the means but failed to recognise that they were there, they cannot be expected to use them let alone use them effectively.

Motivation to form privacy rules

In some instances of the help documentations only, clear sections and pictures were used that can motivate end users. However, their static and dynamic counterparts did not provide any motivating aspect and if there was any persuasive technique, its effects would be counteracted by the lack of explanations and understanding of why

those options were there. Hence browsers did not motivate end users in privacy rule formation except from the standard explanations in the help section which was not directly linked to the static and dynamic parts.

Context and risk-benefit ratio

Whilst Internet Explorer 8.0 highlighted the context of disclosure to be browsing in general with no specificity in help, Firefox did so in static and dynamic only whereas Google Chrome did so throughout all media. However for the risks versus benefits, none of the media of the different browsers provided information about risk and benefits to enable end users to make an informed decision. (Google Chrome detailed the benefits of disclosure only in order to benefit from services.)

Summary:

Although privacy mechanisms were available, end users would not use them since they would not know whether the means were available and for what purpose they could be used because the static and dynamic interactions did not provide the information that the help section did. Also, although functional persuasive techniques were used in help, during interactions end users would not be motivated. Moreover, since the actions on privacy mechanisms would be conducted out of the disclosure context, the specific contextual element that could help manage privacy was absent. Lack of information about the risks of disclosure compared to the benefits of using privacy mechanisms would make it hard for end users to understand whether to form privacy rules and which types of rules to form according to CPM.

Principle 4:

Who is linked within boundary

While Internet Explorer 8.0 and Google Chrome provided different information about who would be linked within the personal information boundary if disclosure occurs, Firefox suggested that links were formed between the end users and Firefox which hid the reality in that Firefox was only an intermediary.

Type of links formed and awareness that these links are formed

The type of links formed throughout the browsers was role linkages if end users understood that the links were formed and the type of the links that were formed. If end users were not provided information to understand that links are formed, linkages were coercive according to CPM.

Ownership rights and permeability negotiations

There was no ownership and permeability negotiation in the privacy tabs of the browsers. The only option in some media instance was to block completely or not share which imply total ownership and control or nothing. There was no negotiation. While this situation can be explained by the fact that these are a-priori settings, coordination of these rights form part of boundary coordination which is an important part of privacy rule formation according to the CPM.

Summary:

Internet browsers in general did not provide for Principle 4, that is awareness of the type of links formed was quite tricky and there was no boundary coordination and negotiation of ownership and permeability rights. Moreover the type of links formed depended on whether end users can understand that a boundary different from their personal boundary would be formed. The lack of Principle 4 can be explained by the fact that privacy features of internet browsers are to be set a-priori to disclosure interactions and coordination and negotiation with service providers cannot be done until the service is requested.

Principle 5:

Awareness of turbulence

Apart from the exception of one instance of dynamic interactions in Firefox 3.6.12, the internet browsers did not provide for ways to be aware of turbulence to set privacy rules in general.

Feedback after disclosure

Only Google Chrome provided for means to be notified when disclosure happens in two of its instances of dynamic interactions.

Means to deal with turbulence

There was no means to deal with turbulence if ever it happened.

5.3.3 Discussion

For Principle 1, since privacy and disclosure form a dialectical tension (that is, if there was no disclosure, privacy management would not be required and if there was no need for privacy, disclosure of personal information would not matter), for end users to manage their privacy they need to understand that disclosure happens that is what would be disclosed to whom and how. The above analysis showed where more explanations or clues would be useful in ensuring end users can be aware that disclosure would happen (can recognise disclosure). The information provided in help, static and dynamic instances should be consistent and complete. This could be done by making sure all the information is provided in one place or the help pages should be easily accessible from the static and dynamic instances for instance by clearly linking help to the static. This would assist end users to relate the use of privacy mechanisms to disclosing their personal information that would consequently highlight the personal relevance of using the privacy mechanisms. Highlighting personal relevance could trigger the cognitive effort required to associate the interaction with their available privacy attitudes or to enable evaluation in terms of control of access to private information.

Principle 3 is about the means to form privacy rules when people are motivated, understand the context and the risks and benefits of disclosure. For end users to use the privacy mechanisms, they need to be made aware of their presence in static interface and dynamic interactions. This is because if end users are able to link the available privacy mechanisms and how the mechanisms can be used to their own privacy attitudes, they could be more expected to use the mechanisms according to their concerns/attitudes. According to Principle 3, end users also need to be motivated to use the mechanisms, to be able to associate the context of disclosure with the privacy management action and to understand the risks and benefits of disclosing

versus maintaining their privacy. These criteria from Principle 3 can themselves serve as persuasive communication within the design. Linking the mechanisms more to context within interactions would also help to cater for the privacy and disclosure dialectical tension which in itself would serve to highlight end users' own attitudes.

For Principle 4 of the CPM, after private information has been revealed, parties become responsible for co-owning and co-managing the information through linkages, ownership and permeability rights. Hence interaction designs have to provide the possibility to coordinate boundaries by allowing formation of links, and coordination of ownership and permeability rights. The analysis showed that Principle 4 was not catered for by internet browsers. Provision of the previous principles that is making it clear what and to whom disclosure happens and ensuring end users are aware of the usefulness of privacy mechanisms would also contribute towards Principle 4. However high level coordination and negotiation could be implemented that would require more precise tuning at specific service request.

As for Principle 5, providing end users with feedback of disclosure might help them to detect turbulence to their privacy management rules. However, background monitoring of personal information use would better help browser end users to detect turbulence. As a form of persuasive communication, monitoring could consequently enable end users to take actions to match their concerns/attitudes whenever turbulence happens.

These discrepancies in providing the principles of CPM provide an explanation to the findings of previous research that showed that end users' privacy behaviour often do not match their attitudes. Without support for the socio-psychological processes of privacy management, internet browsers do not connect with end users' attitudes and do not enable the portrayal of a mental model that would help end users to express their attitudes into behaviour.

5.3.4 Contributions

Substantive

The substantive contribution of the study is that internet browser privacy mechanisms are not consistent in their communication of privacy information in a way that could help end users to manage their privacy as described by the CPM theory. Clearer information about the disclosure context was provided in the help pages that were difficult to access from the static interface and dynamic interactions. Changes to the communication of information in the design such as coherent information in all instances together with visible and accessible privacy and disclosure cues would help to link end users' privacy attitudes to the use of the privacy mechanisms. The study also showed that more support for the dialectical tension between disclosure and privacy and for the socio-psychological processes of privacy management is required if end users would be expected to manage their privacy effectively. Internet browsers therefore do not provide the processes that would enable end user control of their privacy and the other requirements proposed by the experts of Study 1.

Methodological

The methodological contribution is the use of a rigorous and systematic approach to analyse privacy mechanisms using a communications perspective that assesses communicability of privacy management processes within the HCI designs of internet browsers privacy tabs. The study design enabled exploration of the social-psychological processes of privacy within internet browsers without involving end users that is it did not suffer from ecological validity that can arise from end users' self reports of their privacy behaviour (as shown in section 2.3.2). The approach was also valuable in helping to point out discrepancies in design with regards to the CPM theory right away.

5.4 Evaluation of E-Commerce websites (Study 5)

In the previous section internet browsers were analysed and the study found discrepancies in communication and lack of support for the social-psychological processes of privacy management. This section describes a second case study aimed at evaluating another approach of designing privacy. The case study was also conducted as part of answering research question RQ2, that is, “How usable are online privacy mechanisms?” but by exploring the interaction design of the privacy mechanisms of E-Commerce. E-Commerce websites provide the `notice and choice' privacy approach, that is, end users are provided with a privacy policy which apart from acting as a liability shield for service providers is also supposed to inform end users about their privacy. End users then have a choice of whether to disclose or not. Since it has been said that this approach of designing privacy is not usable or useful (Anton et al., 2004; Jensen and Potts, 2004; Milne and Culnan, 2004; Jensen et al., 2005), exploring `notice and choice' would be valuable to shed more light on why this is the case.

This study analysed the human-computer interaction (HCI) design of the checkout option of three E-Commerce websites to understand whether end users could be expected to manage their privacy while shopping online. More specifically, semiotic inspection was used together with communication privacy management (CPM) theory to identify communication breakdowns in privacy designs.

5.4.1 Methods

This section describes the case study design. It starts with the procedure and is followed with the materials used during the case-study.

Procedure

The case study was designed in a similar fashion to the one in the previous section through the five steps of semiotic inspection and the principles of the CPM. The three most used E-Commerce websites in the UK during December 2010 to February 2011 that is Amazon.co.uk, Play.com and Argos.co.uk (IMRG, 2011) were evaluated. The data obtained for each E-Commerce website was then consolidated and analysed before a cross-case analysis was performed. The flow of the semiotic inspection stages within the case study is shown in figure 17 below.

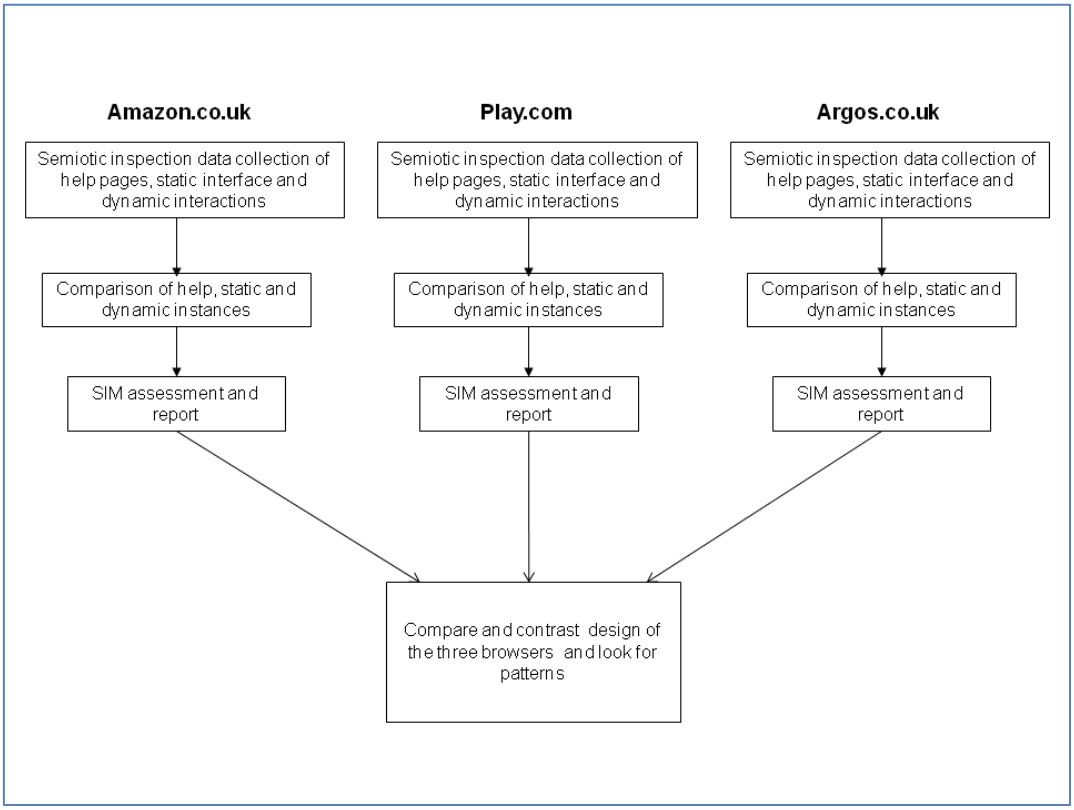


Figure 17: Within-case data collection and analysis and cross-case analysis

Apparatus

The apparatus consisted of the principles of the CPM, as described in the methodology chapter, and the E-Commerce websites. The help pages, static interface and dynamic interactions selected for the evaluation are those that refer to privacy, disclosure or both. For Amazon, the help pages consist of the privacy notice and the privacy paragraph from security whereas for Play and Argos, the help pages refer to their privacy policy. The static interface of Amazon refers to the first interface leading to the 'Checkout' function. For Play and Argos, help pages refer to their privacy policy, static interface refers to first screen of checkout leading to create new account and account sign-in through 'My trolley' interface respectively. The dynamic interactions of the three websites refer to the process of disclosing personal details for checkout. Figure 18, 19 and 20 below show the checkout page for Amazon.co.uk, Play.com and Argos.co.uk respectively.

Figure 18: Amazon first page to checkout

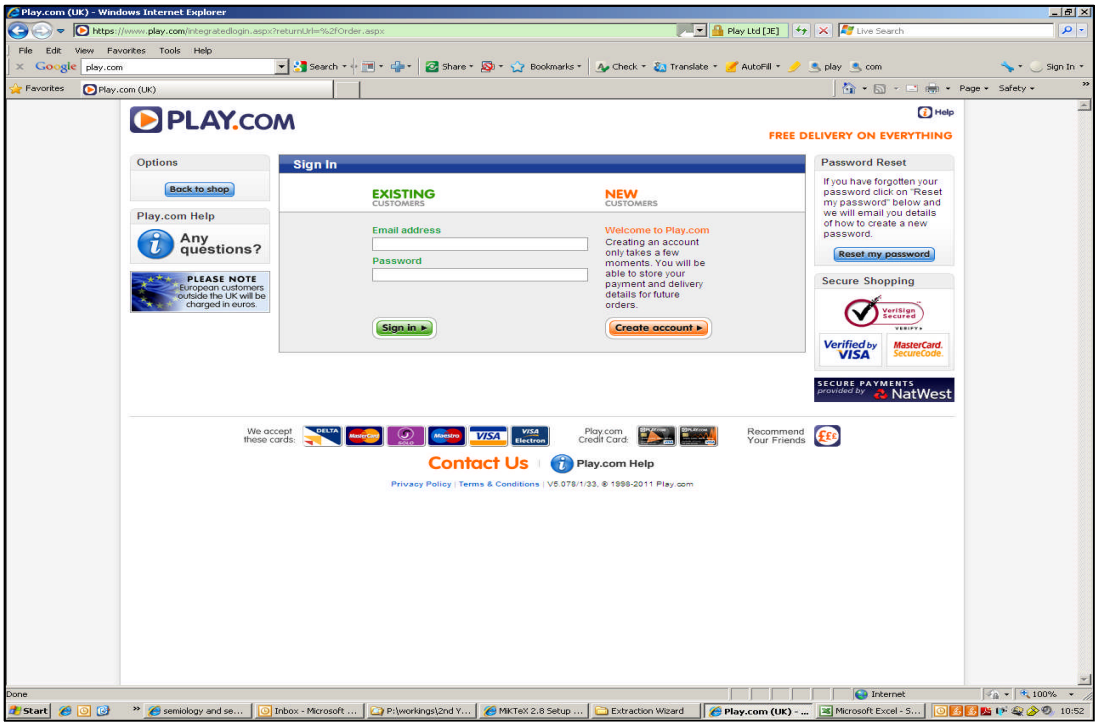


Figure 19: Play.com first page to checkout

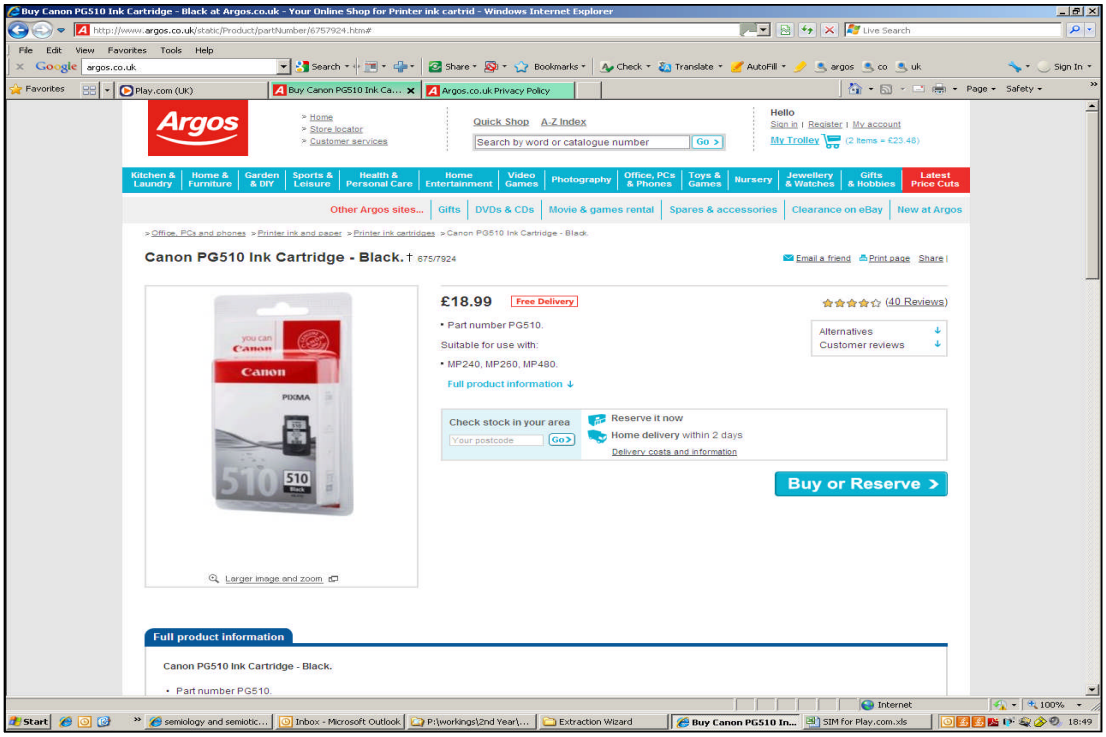


Figure 20: Argos first page to checkout

5.4.2 Analysis & Results

This section elaborates on the case study analysis and the results of the study. It starts with the analysis of each unit case followed by a comparison of the three E-Commerce websites' design of privacy.

Within case analysis

The data collected about the way privacy was communicated through help pages, static interface and dynamic interactions were consolidated separately. A within-case analysis of the consolidated data (that is comparison between help pages, static and dynamic communication of privacy) was then performed. The aim was to highlight discrepancies with the principles of CPM which were likely to indicate usability issues. In the following sections, the analysis for each E-Commerce website is elaborated. Similar to the method design described in section 5.3, the analysis of this study was performed for principles 1, 3, 4 and 5 of CPM.

Amazon.co.uk

Principle 1: Awareness of disclosure through what is disclosed, to whom and how.

Amazon.co.uk did not communicate Principle 1 of the CPM that is awareness of disclosure to the end users effectively. This is because it did so in the help pages and privacy policy but not in the static interface and the dynamic interactions. Table 18 below gives a summary of how Amazon.co.uk provided for the elements of Principle 1.

Table 18: Would end users be aware of disclosure in Amazon.co.uk?

Principle 1	***Help***	***Static***	***Dynamic***
What	✓	x	x
Who	✓	x	x
How	✓	x	x

The help pages were clear in what would be disclosed to Amazon and its affiliates when end users provide information in the different actions mentioned. For their static interface, that is the static screen at checkout that leads to registration or entering of one's details, end users would not understand that they might be about to disclose private information. Also, in its dynamic interactions of checking out (including entering of contact, billing and delivery details); Amazon did not hint towards disclosure.

Principle 3: Means to regulate the flow of information online, awareness of these means and criteria for privacy rules.

Amazon.co.uk did not satisfy the third principle of CPM. This is shown in table 19 below.

Table 19: Does Amazon.co.uk provide means to manage privacy, awareness of means and criteria for rule formation?

Principle 3	***Help***	***Static***	***Dynamic***
Means	x	x	x
Awareness of means	x	x	x
Motivation cues	x	x	x
Context information	✓	✓	✓
Risk/Benefit	x	x	X

Amazon.co.uk only catered for the context of disclosure since it is within an E-Commerce context.

Principle 4: Disclosure causes linkages to be set up within boundaries, and requires coordination of ownership and permeability rights.

Amazon.co.uk hardly provided for Principle 4 of CPM. Following the findings of Principle 1 in which end users would know who they are disclosing to within the help pages, end users would also know who would be linked within their personal boundary through the help pages as shown in table 20 below. This was however not possible in the static interface and the dynamic interactions.

Table 20: Does Amazon.co.uk provide for awareness of links to end users boundary and negotiation?

Principle 4	***Help***	***Static***	***Dynamic***
Who is linked	✓	x	x
Type of links	Role	coercive	coercive
Ownership negotiation	x	x	x
Permeability negotiation	x	x	x

Moreover according to the help pages, the type of links that would be formed with Amazon and its affiliates would be of role type since end users would know who would be linked within their boundary for the purpose of providing them with services. But the links formed in the static interface and the dynamic interactions would be of coercive type since end users would not know who would be linked within their personal boundary.

Principle 5: Awareness of Turbulence

Apart from not enabling end users to coordinate access to their personal boundary as described in the analysis for the previous principle, Amazon.co.uk also did not provide for the possibility to be aware of turbulence to privacy rules as shown in table 21 below.

Table 21: Does Amazon.co.uk provide for turbulence awareness, means and feedback following disclosure?

Principle 5	***Help***	***Static***	***Dynamic***
Awareness of turbulence	x	x	x
Feedback after disclosure	x	x	x
Means to deal with turbulence	x	x	x

Play.com

Principle 1: Awareness of disclosure through what is disclosed, to whom and how.

Play.com was not consistent in communicating Principle 1 of CPM to end users. Play.com would enable end users to be aware of disclosure in its help pages and dynamic interactions but not in its static interface as shown by table 22.

Table 22: Would end users be aware of disclosure through Play.com?

Principle 1	***Help***	***Static***	***Dynamic***
What	✓	x	✓
Who	✓	x	✓
How	✓	x	✓

Play hinted towards disclosure in dynamic interactions by using the following: `provide a valid, active email address', `Enter your postcode', `Date of birth (required for Debit/Credit card authorisation'.

Principle 3: Means to regulate the flow of information online, awareness of these means and criteria for privacy rules.

Play.com was inconsistent in providing means to manage privacy and elements that help towards privacy rule formation. Play provided for user-controlled means that would allow end users to verify the recipient of disclosure in its dynamic interaction. Play also provided for risk-benefit awareness in dynamic interactions as shown in table 23 below. However the help pages and the static interface did not provide for these elements of Principle 3 apart from the context which was obviously about online shopping in the static interface.

Table 23: Does Play.com provide means to manage privacy, awareness of means and criteria for rule formation?

Principle 3	***Help***	***Static***	***Dynamic***
Means	x	x	✓
Awareness of means	x	x	x
Motivation cues	x	x	x
Context information	x	✓	✓
Risk/Benefit	x	x	✓

Principle 4: Disclosure causes linkages to be set up within boundaries, and requires coordination of ownership and permeability rights.

Play.com did not provide for Principle 4 of CPM. This is shown in table 24 below.

Table 24: Does Play.com provide for awareness of links to end users boundary and negotiation?

Principle 4	***Help***	***Static***	***Dynamic***
Who is linked	✓	✓	✓
Type of links	Role	coercive	role
Ownership negotiation	x	x	x
Permeability negotiation	x	x	x

End users of Play.com would know that Play.com and 'reputable third parties' would be linked within their personal boundary throughout the help pages, static interface and dynamic interactions. In the help pages and dynamic interactions, end users would have enough information about disclosure to form role links whereas in the static interface, it would be of coercive nature.

Principle 5: Awareness of Turbulence

In general Play.com did not provide feedback after disclosure, ways to be aware of turbulence and means to deal with turbulence. This is shown in table 25 below.

Table 25: Does Play.com provide for turbulence awareness, means and feedback following disclosure?

Principle 5	*Help*	*Static*	*Dynamic*
Awareness of turbulence	x	x	x
Feedback after disclosure	x	x	x
Means to deal with turbulence	x	x	x

Argos.co.uk

Principle 1: Awareness of disclosure through what is disclosed, to whom and how.

Argos.co.uk was not consistent in its design of Principle 1 of CPM. This is shown in table 26 below.

Table 26: Would end users be aware of disclosure through Argos?

Principle 1	*Help*	*Static*	*Dynamic*
What	✓	x	✓
Who	✓	x	✓
How	✓	x	✓

In the privacy policy, end users would know that they are disclosing to Argos, companies and organisations that administer prize draws and competitions, agents, staff, approved third parties, anyone with whom rights and duties are transferred and cookie contents. This would happen by registering as a user of services provided by Argos and by using Argos website generally. The static interface provided no such information. In the dynamic interactions, end users would know they are disclosing delivery details such as name, address, email address, payment details. They might however not realize that they would also disclose purchase history. Recipient of disclosure would be assumed to be only Argos. End users would know how they would be disclosing due to the comment "By submitting your details, you consent to

their use as set out in our Privacy policy. You'll also be signing up to receive marketing information (such as email, telephone, text) as detailed in our Privacy policy, unless you tick the boxes below."

Principle 3: Means to regulate the flow of information online, awareness of these means and criteria for privacy rules.

Argos did not clearly provide for Principle 3 of CPM. In the help section, end users might have the means to manage their privacy only for the disclosures that happen through cookies but not for the information they would disclose to enable a purchase.

Table 27: Does Argos provide means to manage privacy, awareness of means and criteria for rule formation?

Principle 3	***Help***	***Static***	***Dynamic***
Means	x	x	x
Awareness of means	x	x	x
Motivation cues	x	x	x
Context information	✓	✓	✓
Risk/Benefit	✓	x	x

The context of disclosure was clearly online shopping. The risk and benefit could only be discerned in the help pages in some ways since the risk could be seen as the power Argos has in controlling and managing end users' personal information and the benefits would be benefitting from products and services.

Principle 4: Disclosure causes linkages to be set up within boundaries, and requires coordination of ownership and permeability rights.

Only the first two elements of Principle 4 were provided by Argos as shown in table 28 below. The help pages indicated that end users' personal boundary would be linked to Argos, companies and organisations that administer prize draws and competitions, agents, staff, approved third parties, anyone with whom rights and

duties would be transferred and cookie contents. The static interface and the dynamic interactions only hinted towards links formed with Argos and others.

Table 28: Does Argos provide for awareness of links to end users boundary and negotiation?

Principle 4	***Help***	***Static***	***Dynamic***
Who is linked	✓	✓	✓
Type of links	Role	coercive	role
Ownership negotiation	x	x	x
Permeability negotiation	x	x	x

For the type of links formed, the help pages made it clear that end user information has to be provided for Argos to provide better services. That could also be gathered in the dynamic interactions, that is entering of contact and delivery details would enable purchases to be processed and products to be delivered. However, the static interface would leave end users clueless hence causing coercive links.

Principle 5: Awareness of Turbulence

Argos did not provide means that would let end users know of turbulence in all three meta-communication templates. It also did not provide feedback when disclosure happened.

Table 29: Does Argos provide for turbulence awareness, means and feedback following disclosure?

Principle 5	***Help***	***Static***	***Dynamic***
Awareness of turbulence	x	x	x
Feedback after disclosure	x	x	x
Means to deal with turbulence	x	x	x

Cross Case analysis

Cross-case analysis was performed in order to identify a trend if any among the different cases (E-Commerce websites) in terms of each principle. For instance, the cross case analysis aimed to find out whether the principles were communicated consistently throughout the help pages rather than static interface and dynamic interactions.

Principle 1:

The cross-case analysis for Principle 1 suggests that end users would be aware of disclosure in the privacy policy of the websites and through some hints during checkout (dynamic) but not in the static screen leading to the dynamic interactions in Play and Argos. Amazon gave no hints in dynamic too.

Principle 3:

For Principle 3, all three E-Commerce websites provided the context of disclosure throughout their templates, but only Play provided for user-controlled means that would allow end users to verify the recipient of disclosure in its dynamic interaction. Play also provided for risk and benefit awareness in dynamic interactions whereas Argos did so in its privacy policy only. Hence in general they provided for privacy means in the form of a privacy policy which end users might not understand how to benefit from. Also since the components of the privacy mechanisms (the policy) are not directly linked to the dynamic interactions (where the disclosure happens), they fail to be usable. They also did not consistently communicate risk and benefit that is important for privacy rule formation throughout the templates.

Principle 4:

For Principle 4, the type of linkages that could be formed between end users and E-Commerce websites were mainly role linkages, that is end users would knowingly release personal information to the service providers with the aim to benefit from services. However, in instances where information was not provided about disclosure, the types of linkages were coercive. This was shown in the static interfaces

of all the three websites. Hence, end users would know about their linkages in the privacy policy and some instances of dynamic interactions, that is during the process of disclosure but not before starting the disclosure process.

Principle 5:

None of the E-Commerce websites provided for ways to be aware of mishaps to end users' personal information and no ways to find out about how personal information is processed after disclosure apart from what is available in the privacy policy.

5.4.3 Discussion

For Principle 1, since E-Commerce is a contextual scenario, end users might realise that they are disclosing personal information in their dynamic interactions (although not obvious in Amazon) but it might be difficult for end users to link the disclosure to the use of the privacy mechanisms. This is because although E-Commerce websites provided the privacy policy, it fails at its purpose of providing notice and choice since it is not easily accessible within the static and dynamic interactions or linked within the dynamic interactions. Furthermore the disclosure actions may not be de facto linked to end users privacy attitudes given that the design does not highlight the relevance of initiating privacy actions such as opening the policy. As seen in Principle 3, E-Commerce websites do not provide for user-controlled privacy mechanisms (with the exception of the dynamic interactions of Play). In addition, from Principle 4, end users would assume disclosure is required to benefit from the online service. This means that even if end users know very clearly how disclosure happens, they would not be motivated by the design to use privacy mechanisms such as to open and read the privacy policy to find out about their choices.

5.4.4 Contributions

Substantive

The substantive contribution was the finding that E-Commerce websites did not consistently provide information to help effective use of its privacy mechanisms. They hardly communicated privacy information that could help end users relate

disclosure interactions to privacy choices provided by the websites. The design did not give end users any reason to read the privacy policy. Changes to the communication of information in the design such as coherent information in all instances together with visibility and easy access to privacy features would enhance effectiveness and hence usability of E-Commerce's privacy mechanisms.

Methodological

The methodological contribution was similar as for internet browsers' evaluation. The approach was rigorous and provided valuable insight into the shortcomings of E-Commerce websites' privacy design.

5.5 Conclusion

In this chapter, three methods of designing privacy online were analysed. In the first section, Studies 2 and 3 assessed Facebook's approach of providing privacy management mechanisms. The second section analysed internet browsers privacy tabs within Study 4 and the third section evaluated E-Commerce websites' 'notice and choice' approach within Study 5. Although the three methods of providing privacy online differ in their approach, they all failed to support the social-psychological processes of privacy management within their HCI design.

The survey (Study 2) aimed to determine whether the design of privacy was usable by finding out whether participants were aware of the presence of the mechanisms. It was found that participants might not have been fully aware of the availability of privacy mechanisms, how they could be used and what the impacts of using those could be though they claimed to be sure of their actions. This could be because the privacy design was not obvious enough to the social network end users. The cognitive walkthrough (Study 3) on the other hand helped to provide possible explanations, through a structured and hierarchical task analysis, about why such lack of awareness exists in social network services. The cognitive walkthrough found specific actions that lacked a means of making end users aware that they were available, and how they can contribute to end users' privacy goal. The interface would require some representations that connect the action to end users' goal or some

form of feedback that might help to recognise a connection between a system response and end users' goal. The analysis helped to show that there would indeed be a lack of awareness of privacy mechanisms' availability and potential usefulness in social network services. This could explain why those mechanisms were not widely used and why privacy issues were still common in the press although Facebook had an extensive privacy management interface in 2009.

The case-study design enabled a more thorough evaluation in Studies 4 and 5. A socio-psychological framework was used to guide semiotic inspection. It was found from Study 4 that internet browsers' privacy tabs do not support the dialectical requirement of end users to both disclose and to maintain a level of privacy protection. Consequently although privacy mechanisms are available, end users would be left to imagine disclosure scenarios. This in turn means that end users might not identify the relevance of associating the privacy mechanisms to their possible future disclosures and their privacy attitudes might not be activated and accessed from memory. Therefore highlighting the personal relevance in terms of protection of one's privacy would be beneficial to better help end users place the use of privacy mechanisms within perspective. This would in turn cause activation or enhance the accessibility of end users' privacy attitudes such that there would be a higher likelihood that they can and will use the mechanisms and that their privacy actions would match their concerns. This would also provide the motivational aspect, found lacking in the analysis, that would facilitate the use of the mechanisms or support for coordination of privacy rule such as ownership of disclosed information.

The E-Commerce websites of Study 5 provided the context of disclosure but there was no clear link to privacy mechanisms that is there was no notice and choice within the interaction design. Although the policy provided information about disclosures and possible choices, these were not linked to the dynamic interactions in a way that would encourage end users to go through the policy. End users would therefore not understand the extent of their disclosures and how to benefit from the policy. End users would also have no knowledge of the ownership and permeability of their disclosed information. Therefore, although end users are involved within disclosure actions, a link might still not be triggered to their privacy attitudes and they would not

be able to associate these actions with the functionalities of the privacy approach. Thus highlighting the benefits of being informed about their disclosures and possible choice and the relevance to their privacy would help associate end users' privacy attitudes to the disclosures causing them to more likely take privacy actions that follow their attitudes. This would consequently also improve effectiveness of the mechanisms.

Therefore the proposal in the next chapter of this thesis is to provide the link between disclosure and privacy. Doing so would not only contribute to the processes for managing online privacy but would also activate or facilitate the accessibility of privacy attitudes such that they have a high chance of determining behaviour.

Chapter 6:

Addressing the weaknesses

6.1 Introduction

The literature review of Chapter 2 identified a gap in research. The gap was that previous research has not assessed privacy human-computer interactions through a behavioural lens. It was argued that better understanding of the reasons behind end users' behaviour in response to privacy designs through a social psychological perspective would be beneficial to effective privacy online. Such an approach would guide designs and would help produce implementations that enable end users to more easily connect with their privacy attitudes during interactions such that they can be more able to use the mechanisms to engage in privacy behaviour. This stance was substantiated by the research strategy (section 3.3.2) that elaborated on the structure of attitudes and the link between attitudes and behaviour. Social psychology is of the opinion that attitudes can guide behaviour and the extent and likelihood that they do depends on the strength and accessibility of the attitudes (Fazio and Williams, 1986; Fazio et al., 1986; Augoustinos et al., 2006).

Chapter 5 described the analytical evaluation of existing privacy designs. The outcome of the evaluation was mainly that existing designs do not support the

attitude-behaviour link. The design of privacy in internet browsers was separated from the context of disclosure and the privacy policy in E-Commerce was not easily accessible during disclosure as were the privacy mechanisms of Facebook. Discrepancies were also found in terms of what was communicated within the help pages, static interface and dynamic interactions. Current designs hence make it difficult to ensure that end users can take privacy behaviour such that end users have to imagine their context of disclosure or the privacy protection means and expend tremendous effort if they were to cognitively evaluate their public-private boundary. However designing the dialectical tension that is providing for both disclosure awareness and accessibility of privacy means is tricky since a high privacy salience can upset the online service.

To summarise, the theoretical background underpinning this section of the thesis is that activated and accessible privacy attitudes have a higher likelihood of resulting in privacy behaviour than non-activated and less accessible privacy attitudes (as discussed in section 3.3.2). This view is substantiated by the qualitative part of the research (Chapters 4 and 5) that explained that the link with privacy attitudes can be achieved by ensuring that designs provide the social psychological processes of privacy management. This chapter describes two experimental studies that were conducted to find out whether support for the processes of privacy management through persuasive communication improves the effectiveness of privacy mechanisms within an E-Commerce context. In other words, the chapter aims to find out whether persuasive communication can affect privacy behaviour by influencing attitude activation and accessibility. The studies were designed to answer research question RQ3 that is 'How does persuasive communication affect the effectiveness of online privacy mechanisms?'. The selected context for the studies was E-Commerce since the latter is not only an integral part of retail services but as discussed in the Literature Review Chapter, it has been said to suffer from ineffective privacy designs (Milne and Culnan, 2004; Cate, 2010). Enhancing effectiveness of privacy designs in E-Commerce could help end users to distinguish between services that genuinely protect their privacy from those who don't. It could also help end users to participate in managing their privacy, making them feel more at ease with the service provider.

Due to legal requirements, E-Commerce websites have to provide end users with information about data storage, processing and use. They also have to provide end users with choices about the information they disclose. This method of providing privacy in E-Commerce is often referred to as the 'notice and choice' approach (Spiekerman and Cranor, 2009). Studies have shown that the notice provided through the privacy policy is not effective since the policy is either not opened by end users (Jensen et al., 2005) or if it is, it is not usable or useful (Anton et al., 2004; Jensen and Potts, 2004; Milne and Culnan, 2004; Jensen et al., 2005). Without notice, end users do not have adequate choice hence making the whole approach of providing privacy in E-Commerce inadequate.

The first user study was a pilot designed to compare end users' privacy behaviour when using a prototype website with persuasive messages versus one without such persuasive messages. The second user study was an improved experimental design aimed to assess end users' behaviour under four different persuasive conditions that restricts persuasive messages in the design to one message so as to more systematically assess the effect of persuasive communication on privacy behaviour and hence effectiveness of privacy mechanisms. It also uses more valid measurements of privacy behaviour. In the following sections, the method, results and discussion for each study is presented followed by a summary and a formulation of the contributions of these studies.

6.2 Study 6: Pilot User Study

In this pilot experimental user study, two versions of an E-Commerce website were designed. The first one had a simple checkout page whereas the second one had persuasive cues in the form of suggestions and reminders. This section elaborates on the pilot study design and the results.

6.2.1 Method

In this section, the experiment design is described. The participants, the tools selected and materials designed are specified. The procedure set to participants is also described.

Design

The user study was designed as a within subject experiment that is the participants took part in both the control task and the task with persuasive messages. The independent variable was privacy attitude measured through privacy concern as described by the Privacy Segmentation Index (Kumaraguru and Cranor, 2005). The dependent variables were privacy related activity: whether the privacy policy was opened and whether 'Guest' was selected at checkout instead of 'Register'. The hypothesis derived from RQ3 that is 'How does persuasive communication impact the effectiveness of online privacy mechanisms?' is:

H1: Privacy mechanisms are more effective when persuasive communication is used

Subjects

The study was comprised of a total of 22 participants: 14 of them were affiliated to the Jubilee Centre of Sunderland recruited through UKOnline and the other 8 were members of staff of the Barrington Library of Cranfield University. The participants were explained the purpose of the study without stressing on privacy and were given a consent form to fill. The table below describes the spread of participants across the different age groups and whether they started the study with the control version of the website or the treatment version.

Table 30: Spread of participants for Pilot User Study 1

Age	18-25	26-29	30-39	40-49	50+	Total
Control	3	x	3	1	3	10
Treatment	3	1	1	3	4	12

Materials

The E-Commerce website was designed in two different versions of an online bookstore. The difference between the two versions was within the checkout page. The figure 21 below shows the control condition (without persuasive messages) and is

followed with figure 22 which shows the treatment condition (with persuasive messages).

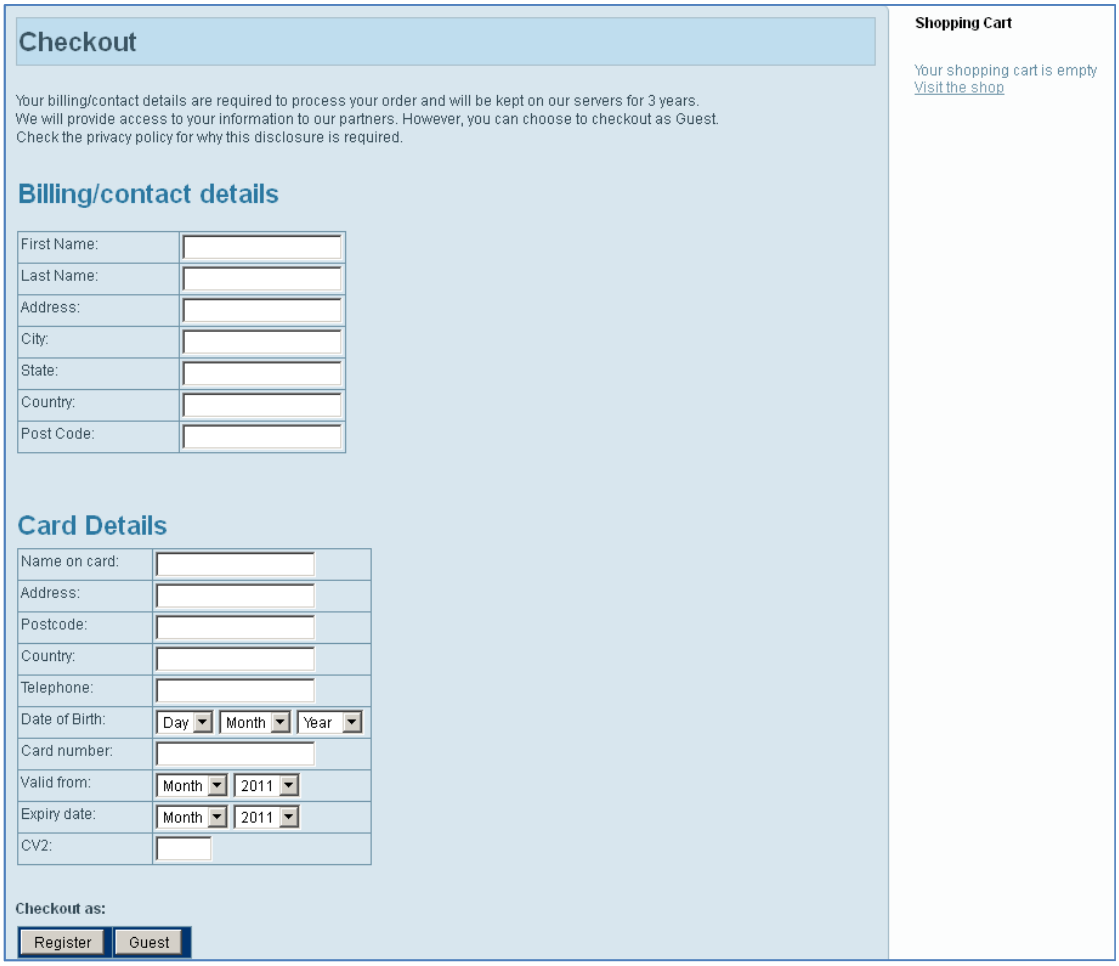


Figure 21: The control checkout page

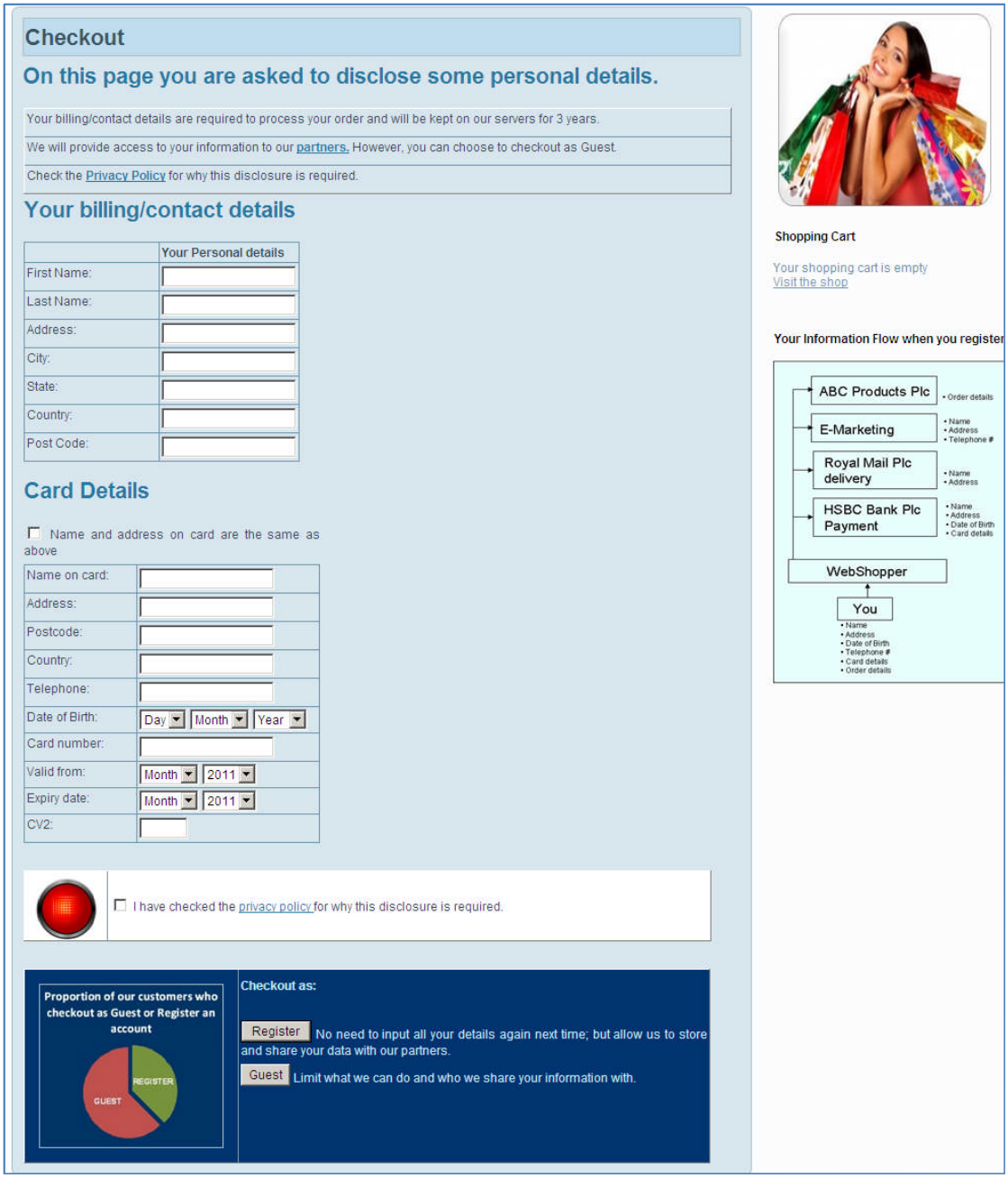


Figure 22: The persuasive checkout page

The other materials of the user study included a pre-test questionnaire that assessed the participants' privacy attitudes and demographic data and a post-test questionnaire aimed towards comparing the two versions of the website. These questionnaires are provided in the Appendix E. Camtasia Studio 7.0 was also used to record participants' interactions during the test.

Procedure

Participants were provided with a procedure to follow in which they were asked to buy a book in control (or treatment) and then asked to buy another book in treatment (or control). The procedure is provided in Appendix E.

About half (10) of the participants started with the control whilst the other half started with the treatment. This was done to avoid any bias effect that might result from taking a specific version of the study first. The experimental task consisted of choosing a product, adding it to the shopping cart and proceeding to checkout. The checkout page opened and the participants were required to fill in their name, address, phone number, e-mail address for delivery and the card details provided in the procedures.

After this exercise, they completed a single post-test questionnaire where they had the opportunity to perform a comparative evaluation of the non-persuasive versus persuasive version of the website. The aim was to find out whether participants identified any privacy difference between the two websites.

6.2.2 Results

Only half of the participants claimed that it was easier to identify privacy features in the persuasive condition. 7 participants opened the policy and only 6 participants identified the 'Guest' versus 'Register' button to be a privacy choice. 14 participants selected 'Guest' in the persuasive compared to 13 in control.

6.2.3 Discussion

The pilot user study did not show improved effectiveness in privacy mechanisms in the persuasive version of the design. This might be because the comparative evaluation was performed by non-expert privacy end users for whom it is difficult to assess privacy designs. Therefore the next version of the user study would not require participants to make comparisons between two versions. Instead participants would take part in only one version of the study in a between subject design. This approach would however require a much larger number of participants for a statistically sound analysis.

Another observation was that participants followed the procedure provided to them very closely and did not explore the interface such that the information flow diagram on the right of the checkout page (figure 22) and other cues were hardly noticed. The participants were also made aware, before taking part in the study, that their interactions on the researcher's computer were being recorded by Camtasia Studio7.0. They also took the study in the presence of the researcher. These aspects of the study design made it difficult for participants to use the website as they would normally do in their usual environment. The next version of the study design would consequently benefit from not having a strict procedure for participants to follow and not placing participants under such close scrutiny.

The other problem with the design of the pilot study was that improved effectiveness of privacy mechanisms was measured in terms of higher number of opened privacy policies, selection of 'Guest' rather than 'Register', whether participants found a privacy choice and their stated evaluation of ease of use. The first three of these measurements would not have much importance in terms of privacy behaviour when considered separately since for instance selection of 'Guest' checkout over 'Register' does not mean that participants did so because of the privacy information provided in the privacy policy. The next version of the design would aim to develop better measures for effectiveness and privacy behaviour.

The persuasive version of the website also had a variety of persuasive cues that not only resulted in a clearly different design from the control but also made it difficult to distinguish between the effects of the different persuasive messages. The next version of the study would hence design more controlled versions of the website that differ in only one element of persuasive messages. Apart from privacy attitudes, other factors related to participants such as age, gender, extent of prior E-Commerce use, education level might also affect privacy behaviour and would be considered within the analysis.

6.3 Study 7: User Study

This study design is an improvement on the previous version. In this experimental study, four versions of an E-Commerce website were designed. The control did not have any persuasive message whilst the three other versions each had a different persuasive message. Privacy behaviour was observed in response to the different types of persuasive conditions and was measured through an aggregate measure of behaviour. This section describes the method and results.

6.3.1 Method

In this section, the experiment design is described. The participants, the tools selected and materials designed are specified. The procedure set to participants is also described.

Design

Persuasive design can include variations to the persuasive message in terms of the source of the message, the positive or negative value associated with the message and the content of the message itself (Petty and Cacioppo, 1986; Petty and Wegener, 1998). The four conditions of the experiment were first, an attractive source suggesting the privacy action within the E-Commerce checkout page. Second, a weak positive value associated with the privacy action is suggested and third, a strong argument that would trigger thinking about the extent and consequences of disclosure and suggesting privacy actions. The control was the absence of a specific persuasive message within a simple checkout page reminding participants to read the privacy policy.

The design was a between subject experiment. This is because privacy behaviour resulting from four different conditions had to be compared and a within subject approach, in which each participant would be subjected to all four conditions, would suffer from carryover effects such as fatigue and practice effects such as enhanced confidence. Also, as shown in the previous section, non-expert privacy participants would have a hard time comparing different versions for privacy. The independent variables were Westin's privacy concern as described by the Privacy Segmentation

Index (Kumaraguru and Cranor, 2005), age, gender, education level and extent of previous E-Commerce use.

The dependent variable was privacy behaviour. It was an aggregate measure of privacy behaviour defined as Behaviour Score. Behaviour Score consisted of two privacy actions and the extent of notice and choice. Privacy actions were observed whilst the extent of notice and choice was gathered from the post-task questionnaire described in the apparatus and materials section below. The extent of notice and choice was designed as shown in Table 31 and 32 below through Notice Level and Choice Level scores. The type of data that could be generated by scores were of ordinal type, that is for instance a value of 2 showed a higher score than a value of 1 but the difference between scores of 2 and 1 and scores of 1 and 0 were not necessarily the same.

Notice Level was given a score level of 0 to 2. The Notice Level was zero when participants did not know what was disclosed to whom. The score increased as more information that might help an individual form privacy rule was identified as shown in Table 31 below.

Table 31: Notice Definition and Scores

Notice components/stages	***Notice score***
Knows neither of (what information is disclosed, who has access to information)	0
Knows 1 of (what information is disclosed, who has access to information)	1
Knows what information is disclosed and who has access to the information.	2

Choice Level was given a score level of 0 to 1. The Choice Level was zero when participants did not identify the means to restrict access and storage of their information. The score increased when participants identified the means and made a decision to take the more restrictive action or not take the more restrictive action as shown in Table 32 below.

Table 32: Choice Level Definition and Scores

Choice level	***Choice score***
Does not know about means to restrict access	0
Know about means, through guest and register buttons and selected guest to protect privacy	1
Know about means, through the guest versus register buttons and decided not to restrict access to protect privacy	1

Two other measures that contributed to the design were privacy-related actions. They referred to whether the privacy policy was opened and to the option selected at checkout as shown in Table 33 below.

Table 33: Actions

Actions	***Score***
Did not open the policy	0
Opened the policy	1
Selected Register at checkout	0
Selected Guest at checkout	1

Therefore, Behaviour Score was the sum of the scores obtained from whether the policy was opened, the Notice Level Score, the checkout selection and the Choice Level Score. This catered for evaluative consistency (described in section 3.3.2) by enabling the comparison of general privacy attitude with an aggregate measure of behaviour. Moreover, the privacy actions (whether policy was opened and the checkout selection) were not considered as privacy behaviour on their own since the fact that policy was opened or guest was clicked did not imply that these were done purposefully for privacy reasons. Literal inconsistency was hence avoided by ensuring that behavioural intentions matched actions.

As explained in the introduction of this chapter (section 6.1) the study's theory was that if designs connect with end users' attitudes, privacy attitudes might be accessed or activated resulting in a higher likelihood of privacy behaviour than designs that do not link with privacy attitudes. This research proposed persuasive communication to trigger this link. The hypotheses derived from research questions RQ3 that is 'How does persuasive communication affect the effectiveness of online privacy mechanisms?' were:

H1: Privacy attitude has an effect on privacy behaviour

H1 refers to the definition of effective online privacy mechanisms given in section 1.2 that is, 'an online privacy mechanism is effective if it enables end users to take privacy actions that match their attitudes'.

H2: Persuasive communication affects privacy behaviour in E-commerce

Moreover, characteristics of the participant such as gender, age, education level and extent of prior E-Commerce use might affect privacy behaviour. The corresponding hypothesis is given in H3.

H3: Other factors have an effect on privacy behaviour.

These factors could also interact with persuasive communication when affecting privacy behaviour. The corresponding hypothesis is as shown by H4.

H4: Other factors interact with persuasive communication to affect privacy behaviour

Subjects

215 participants completed the E-Commerce simulation and answered the post-test questions. The spread of participants across the different conditions were as follows:

Table 34: Distribution of participants across conditions

Persuasive message	***Condition***	***Frequency***
Attractive source	1	63
Positive message	2	51
Strong argument	3	56
None	4	45
	Total	215

Apparatus & Materials

The apparatus and materials consisted of four websites designed in WordPress. The difference between the websites was the message before the check box that aims to trigger end users' opening of the privacy policy. Figure 23 below shows the checkout page and figures 24 to 27 show the different persuasive conditions that is a simple reminder, a reminder with an attractive source, a weak message and strong argument.

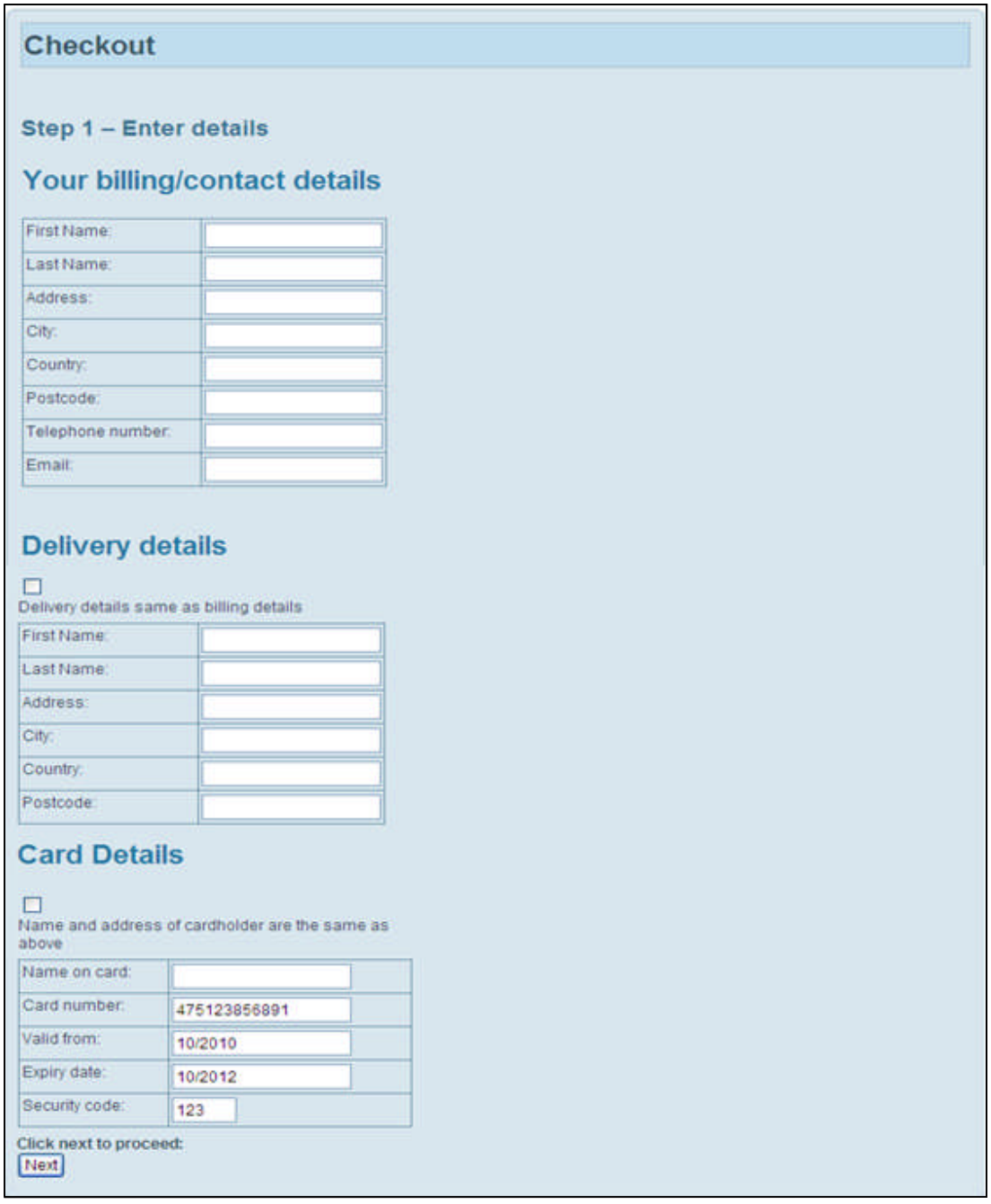


Figure 23: Checkout page without further persuasive message

The 'Next' button of figure 23 leads to a different page that reminds end users to open the privacy policy. Figure 24 shows the fourth condition of the experiment with only the check box and the message 'I have read the privacy policy' without any other further persuasive element. The aim was to find out how a simple reminder would affect behaviour compared with those with more persuasive intent.

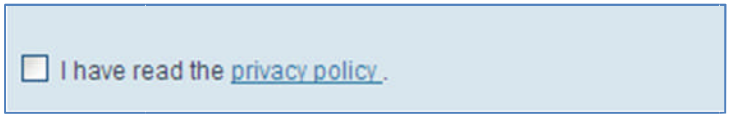


Figure 24: Simple reminder

The first persuasive condition as shown in figure 25 below had an attractive source that suggested reading the policy before checking out. The aim of the attractive source was to act as a cue that would encourage participants to open the policy without the source itself having any specific connection to privacy. This type of source was selected over one with expert or credible links to security and privacy to avoid causing an effect due to trust.

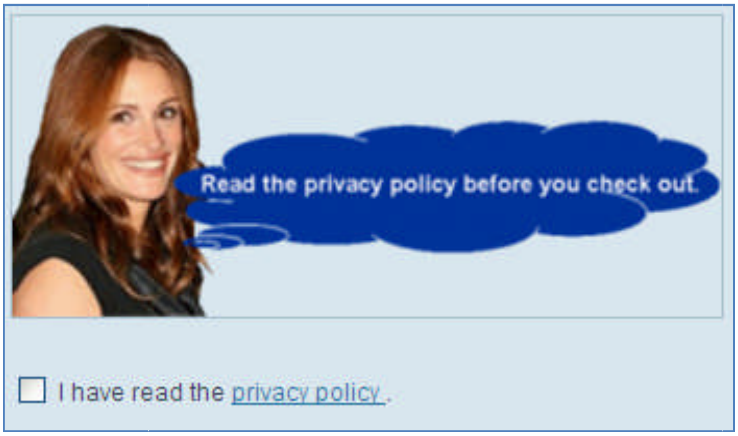


Figure 25: Attractive source persuasive message

The second persuasive condition as shown in figure 26 below had a weak positive message, that could be interpreted differently by different participants, that suggested reading the policy before checking out. The aim was to encourage participants to open the privacy policy to benefit from a comforting online experience. The message is weak since 'comfort' in the context of online privacy would be more vague than the use of 'secure' or 'private' while still being positive. This message also highlights personal relevance and vested interest to participants with 'Do you want a comforting online experience?'.

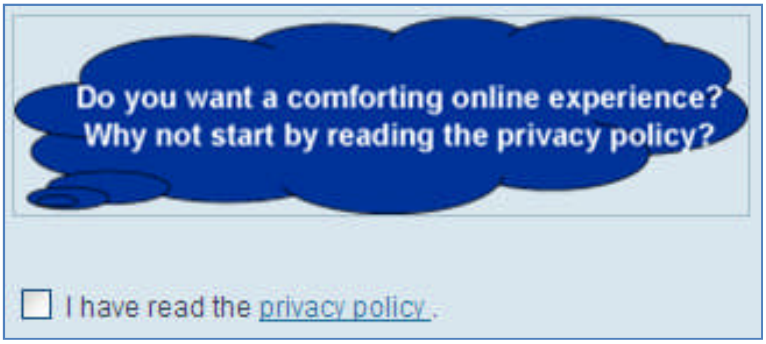


Figure 26: Weak positive persuasive message

The third persuasive condition as shown in figure 27 below had a strong privacy message that highlighted the reasons to open the privacy policy. The message was strong because it did not only stress the importance of reading the policy but also emphasised the personal relevance for the participants. The aim of this message was to act as the argument for participants to elaborate about their privacy and scrutinise the privacy afforded by the system.

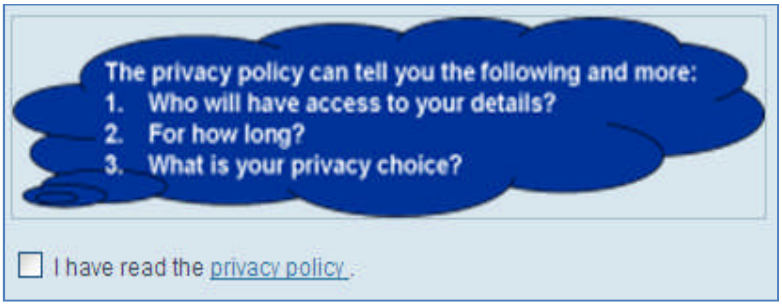


Figure 27: Strong persuasive argument

Participants were invited to take part in the study via e-mail. The e-mail contained a link to one condition of the study designed through Loop11 remote usability tool. Loop11 is a web based un-moderated usability tool that does not enable real time communication with researchers during participation and allowed participants to take part in the study in their own time and environment. This method enabled the involvement of a large number of participants in the study without taking them out of their usual environment to a laboratory environment that could bias their behaviour during the study.

Loop11 facilitated the design of a demographic survey before the task and a post test questionnaire that followed the simulated task. The tool also recorded the user path through the task. This was important because it provided information about whether specific links were chosen or buttons were pressed. The data collected from the study was mainly obtained from demographic questions, records of whether the privacy policy was opened, which option was selected at checkout and the responses to questions following the task. The pre-task questionnaire queried participants about age, gender, education level and extent of E-Commerce use (as shown in Appendix F). The post-test questionnaire assessed participants' privacy attitudes using Westin's Segmentation Index, whether participants knew what information they had just released, whether participants knew who would have access to the information, whether participants knowingly selected the more private option to checkout that is they had a choice and whether participants identified privacy features in the website. Moreover, Loop11 was adequate for the needs of this study as video or audio recordings of user activities were not required.

Procedure

Participants were invited through snowball sampling. They were sent a Loop11 link that opened in their default browser. They received a welcome note to take part in a shopping simulation and were instructed to answer a series of questions before being presented with a task to complete. After completing the tasks, participants were asked questions about the task just completed to assess their appreciation of the level of notice and choice. The welcome note, instructions, questions, task definition were all designed in Loop11. In the welcome note, instructions and pre-task questions, participants were not informed or hinted that the study was about online privacy. This was done to avoid biasing end users' behaviour. The participants were however re-assured at the end of the process that their personal details was not recorded by the system and that the study was anonymous. Screenshots of the procedure including the questions is provided in Appendix F.

The task consisted of choosing a product, adding it to the cart and proceeding to the checkout. The checkout page opened and the participants were required to fill in their

name, address, phone number, e-mail address for delivery. The card details were preset into the checkout page so participants did not have to use their own financial information.

6.3.2 Results

In this section, the data collected is described and explored. The hypotheses are tested and the analysis is described. The results are further explained and discussed in the next section.

Describing the data collected

The dependent variable was Behaviour Score which took values 0, 1, 2, 3, 4, 5. The aggregate measure, Behaviour Score, was calculated by adding the responses of the following observations as shown in table 35 below.

Table 35: Components of dependent variable

Component of behaviour score	***Possible values***
Policy opened	0, 1
Notice Level score	0, 1, 2
Choice Score	0, 1
Checkout selection	0, 1

The independent variables were education level, extent of prior E-Commerce use, concern, age and gender. The values these took and the number of responses received for each are shown in table 36 to 40 below.

Table 36: Education Level

Education level	***Values***	***N***
None	0	8
O-Level	1	24
A-Level	2	25
First degree	3	66
Post graduate degree	4	92
Total		215

Table 37: Extent of prior E-Commerce use

Prior E-Commerce Use	***Values***	***N***
Once	1	12
1-5 /year	2	43
1-5 /3 months	3	67
1-5 /1 month	4	61
>5 / 1 month	5	32
Total		215

Table 38: Privacy concern

Privacy concern	***Values***	***N***
Unconcerned	0	19
Pragmatist	1	137
Fundamentalist	2	59
Total		215

Table 39: Age

Age Group	*Values*	*N*
18-25	1	14
26-29	2	22
30-39	3	53
40-49	4	63
50+	5	63
Total		215

Table 40: Gender

Gender	*Values*	*N*
Male	1	96
Female	2	119
Total		215

Exploring the data

The ANOVA statistical test was used to analyse the collected data. Before testing the hypotheses, the assumptions of ANOVA namely normality of data and homogeneity of variance were verified. The distribution of the individual observations was found to be roughly normal. For the privacy Behaviour Score for the different conditions, the variances were equal for conditions A, B, C and D: $F(3, 211) = .661$, $p>.01$ that is non-significant. Homogeneity of variance was confirmed by the variances. The histogram of behaviour score and the table for the test of homogeneity of variance are provided in Appendix G.

H1: Privacy attitude has an effect on privacy behaviour

Privacy attitude was measured through Westin's Privacy Segmentation Index of privacy concern and took values of 0, 1 or 2 as explained in table 38 above. Privacy

behaviour was measured through the aggregate measure, Behaviour Score and could take values 0, 1, 2, 3, 4 or 5.

A one-way independent ANOVA was performed to determine the effect of privacy concern on privacy behaviour. Privacy concern was found to have a significant effect on privacy Behaviour Score with $F(2, 212) = 4.891$, $p < .05$. The tables below show the SPSS output for the ANOVA.

Table 41: Descriptives for Concern x Behaviour Score

BehaviourScore

Concern	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
0	19	1.95	1.079	.247	1.43	2.47	0	4
1	137	2.50	1.207	.103	2.29	2.70	0	5
2	59	2.76	1.119	.146	2.47	3.05	0	5
Total	215	2.52	1.187	.081	2.36	2.68	0	5

It was also clear from the Descriptives table above, from lower bound and upper bound comparison of mean that participants with Concern = 2 (privacy fundamentalists) had higher mean behaviour score than participants with Concern = 0 (privacy unconcerned). Fundamentalists' lowest mean behaviour score matched unconcerned participants highest mean Behaviour Score.

Table 42: Test of Homogeneity of Variances

BehaviourScore

Levene Statistic	df1	df2	Sig.
1.225	2	212	.296

The above table shows the test for homogeneity of variance, an assumption to be satisfied for ANOVA. The significance level enabled acceptance of the null hypothesis that the variances across the different levels of variable Concern were equal.

Table 43: One-way ANOVA for the effect of concern on behaviour score

BehaviourScore

			Sum of Squares	df	Mean Square	F	Sig.
Between Groups	(Combined)		9.782	2	4.891	3.553	.030
	Linear Term	Unweighted	9.554	1	9.554	6.940	.009
		Weighted	8.974	1	8.974	6.518	.011
		Deviation	.809	1	.809	.587	.444
Within Groups			291.874	212	1.377		
Total			301.656	214			

Table 43 above shows the significant effect of variable Concern on privacy Behaviour Score with $F(2, 212) = 4.891$, $p < .05$. The multiple comparisons table 44 below shows that the privacy Behaviour Score of unconcerned participants (Concern = 0) is significantly different from fundamentalists (Concern = 2) with p=.027. Hence, irrespective of persuasive condition, privacy fundamentalists exhibited a significantly higher behaviour score than privacy unconcerned in this user study. This is depicted in the mean plots graph in figure 28 below.

Table 44: Multiple comparisons for concern

BehaviourScore

(I) Concern	(J) Concern	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
0	1	-.549	.287	.172	-1.24	.14
	2	**-.815***	.310	**.027**	-1.56	-.07
1	0	.549	.287	.172	-.14	1.24
	2	-.266	.183	.439	-.71	.17
2	0	**.815***	.310	**.027**	.07	1.56
	1	.266	.183	.439	-.17	.71

*. The mean difference is significant at the 0.05 level.

Means Plots

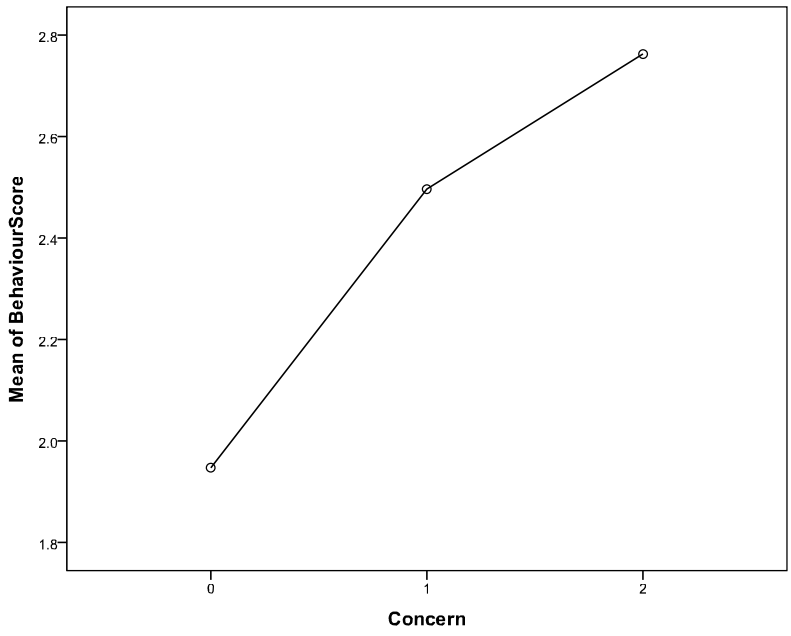


Figure 28: Mean plot of Behaviour score for each level of Concern

H2: Persuasive communication affects privacy behaviour in E-Commerce

The persuasive communication conditions were conditions 1 (attractive source message), 2 (weak message), 3 (strong message) and 4 (no message). Notice and choice was measured by Behaviour Score which took values 0, 1, 2, 3, 4 or 5. The mean Behaviour Score of each persuasive condition 1, 2, 3 and the control were compared to find out how the different persuasive conditions affected privacy behaviour. A one-way independent ANOVA was performed. A significant effect of condition on privacy behaviour score was found with $F(3, 211) = 9.839$, $p < .05$.

The tables 45 to 48 below show the SPSS output for the ANOVA. It is clear from the Descriptives table 45 below, from lower bound and upper bound comparison of mean that participants taking part in conditions 1 (that is with attractive source message) and 4 (that is no message) had much lower privacy Behaviour Score than participants

taking part in conditions 2 (that is with weak message) and condition 3 (that is with strong message). The upper bound mean value of conditions 1 and 4 fell well under the lower bound mean value for conditions 2 and 3.

Table 45: Descriptives of Condition

BehaviourScore

	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
1	63	2.19	1.176	.148	1.89	2.49	0	5
2	51	3.10	1.063	.149	2.80	3.40	1	5
3	56	2.75	1.100	.147	2.46	3.04	1	5
4	45	2.04	1.127	.168	1.71	2.38	0	4
Total	215	2.52	1.187	.081	2.36	2.68	0	5

Table 46: Test of Homogeneity of Variance

BehaviourScore

Levene Statistic	df1	df2	Sig.
.661	3	211	.577

Table 47: ANOVA for Condition x Behaviour score

BehaviourScore

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	37.021	3	12.340	9.839	.000
Within Groups	264.635	211	1.254		
Total	301.656	214			

From the multiple comparisons table below, it can be seen that condition 2, with M = 3.10, gave significantly higher Behaviour Score than condition 1 with M = 2.19, p <.05 and condition 4 with M = 2.04, p <.05. Also condition 3, with M = 2.75 gives significantly higher behaviour score than condition 1 with M = 2.19, p <.05 and condition 4 with M = 2.04, p <.05.

Table 48: Multiple comparisons for the levels of Condition

BehaviourScore

(I) Condition	(J) Condition	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
1	2	**-.908***	.211	**.000**	-1.47	-.35
	3	**-.560***	.206	**.042**	-1.11	-.01
	4	.146	.219	1.000	-.44	.73
2	1	**.908***	.211	**.000**	.35	1.47
	3	.348	.217	.659	-.23	.93
	4	**1.054***	.229	**.000**	.44	1.66
3	1	**.560***	.206	**.042**	.01	1.11
	2	-.348	.217	.659	-.93	.23
	4	**.706***	.224	**.011**	.11	1.30
4	1	-.146	.219	1.000	-.73	.44
	2	**-1.054***	.229	**.000**	-1.66	-.44
	3	-.706*	.224	.011	-1.30	-.11

*. The mean difference is significant at the 0.05 level.

Means Plots

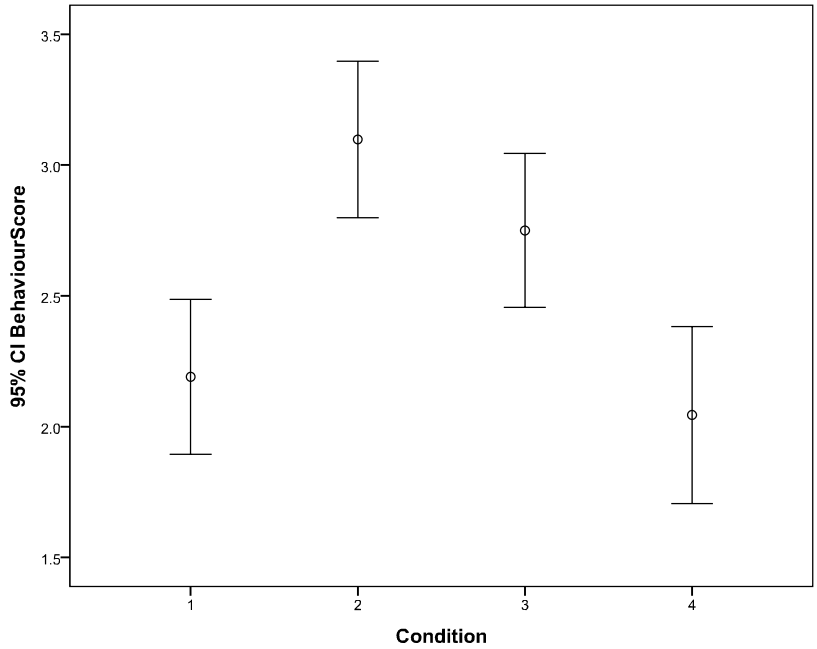


Figure 29: Mean plot of Behaviour score for each level of Condition

The difference in mean behaviour score is clearly shown in Figure 29 above. The mean plot provides a visual representation of the means for each condition and their relationship.

H3: Other factors have an effect on privacy behaviour

All the independent variables were skimmed through to find out if they have an effect on privacy behaviour and whether they interacted with each other to influence behaviour score.

H3.1: E-Commerce use affects privacy behaviour score

A one-way ANOVA found a significant main effect of the extent of prior E-Commerce use on the privacy behaviour score, $F(4, 210) = 2.971$, $p<.05$. This is described in tables 49 to 51 below.

Table 49: ANOVA for E-Commerce use x Behaviour Score

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	16.159[a]	4	4.040	2.971	.020
Intercept	848.902	1	848.902	624.417	.000
EcomUse	16.159	4	4.040	2.971	.020
Error	285.497	210	1.360		
Total	1668.000	215			
Corrected Total	301.656	214			

a. R Squared = .054 (Adjusted R Squared = .036)

Table 50: Mean Behaviour score for each level of E-Commerce use

EcomUse	Mean	Std. Error	95% Confidence Interval	
			Lower Bound	Upper Bound
1	1.667	.337	1.003	2.330
2	2.256	.178	1.905	2.606
3	2.627	.142	2.346	2.908
4	2.590	.149	2.296	2.884
5	2.844	.206	2.437	3.250

The post hoc test, from the multiple comparisons table 51 below, it can be seen that the significant difference is mainly due to the mean Behaviour Score difference between EcomUse = 1 and EcomeUse = 5, that is when extent of prior E-Commerce use is only once versus more than 5 times per month.

Table 51: Comparisons among the different levels of E-Commerce use

(I) EcomUse	(J) EcomUse	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
1	2	-.59	.381	1.000	-1.67	.49
	3	-.96	.365	.092	-2.00	.08
	4	-.92	.368	.129	-1.97	.12
	5	**-1.18***	.395	**.032**	-2.30	-.06
2	1	.59	.381	1.000	-.49	1.67
	3	-.37	.228	1.000	-1.02	.28
	4	-.33	.232	1.000	-.99	.32
	5	-.59	.272	.319	-1.36	.18
3	1	.96	.365	.092	-.08	2.00
	2	.37	.228	1.000	-.28	1.02
	4	.04	.206	1.000	-.55	.62
	5	-.22	.251	1.000	-.93	.49
4	1	.92	.368	.129	-.12	1.97
	2	.33	.232	1.000	-.32	.99
	3	-.04	.206	1.000	-.62	.55
	5	-.25	.255	1.000	-.98	.47
5	1	**1.18***	.395	**.032**	.06	2.30
	2	.59	.272	.319	-.18	1.36
	3	.22	.251	1.000	-.49	.93
	4	.25	.255	1.000	-.47	.98

Based on observed means.

The error term is Mean Square(Error) = 1.360.

*. The mean difference is significant at the .05 level.

The profile plot in figures 30 and 31 below shows that privacy Behaviour Score generally increases with an increase in extent of prior E-Commerce use. However, the error bars graph re-iterates the multiple comparison table in showing that the main difference is caused when extent of prior E-Commerce use is 1 versus 5.

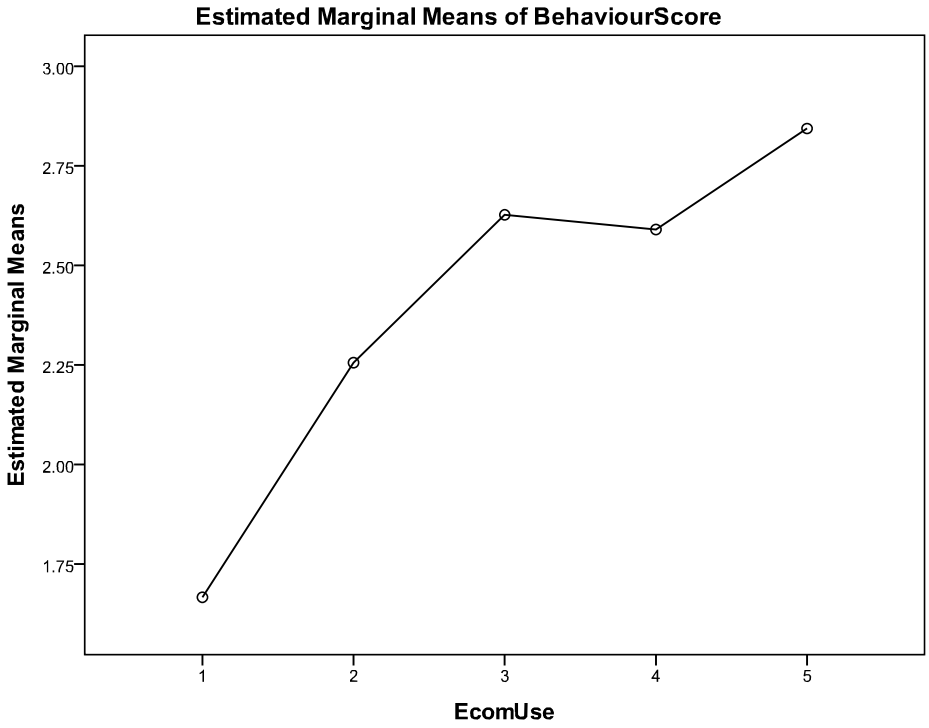


Figure 30: Plot of mean Behaviour Score for each level of E-Commerce use

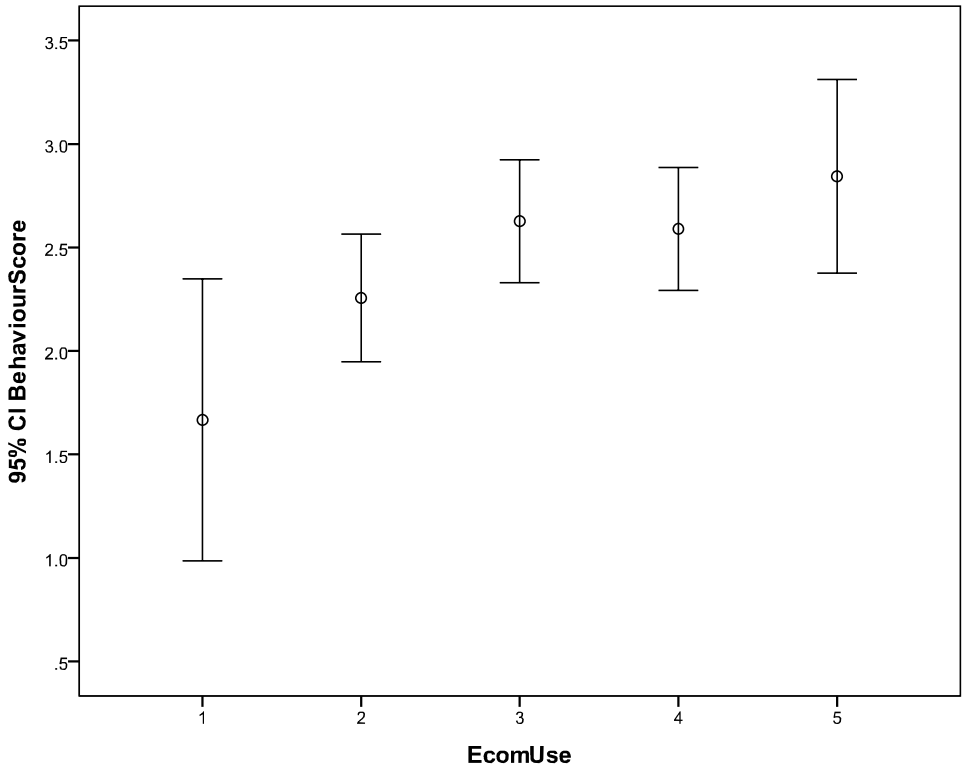


Figure 31: Error bars for Behaviour Score for each level of E-Commerce use

H3.2: Education level interacts with condition in affecting privacy behaviour score

A two-way independent sample ANOVA was run through the GLM univariate option of SPSS. The aim was to determine the interaction effect of persuasive condition and education level in influencing privacy behaviour. There was a significant main effect of persuasive condition on behaviour score, $F(3, 197) = 6.619$, $p<.001$. There was also a significant main effect of education level on behaviour score, $F(4, 197) = 2.598$, $p<.05$.

A significant interaction effect was also observed between persuasive condition and education level on privacy Behaviour Score, $F(10, 197) = 2.075$, $p<.05$. This indicates that participants with different education levels were affected differently by persuasive condition. The analysis is described in tables 52 to 54 below.

Table 52: Two-way ANOVA for the interaction effects of Condition and Education level x Behaviour score

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	77.305[a]	17	4.547	3.993	.000
Intercept	596.048	1	596.048	523.384	.000
Condition	22.616	3	7.539	6.619	.000
EducationLevel	11.836	4	2.959	2.598	.038
Condition * EducationLevel	23.636	10	2.364	2.075	.028
Error	224.350	197	1.139		
Total	1668.000	215			
Corrected Total	301.656	214			

a. R Squared = .256 (Adjusted R Squared = .192)

Table 53: Comparison between the different conditions

(I) Condition	(J) Condition	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
1	2	-.91*	.201	**.000**	-1.44	-.37
	3	-.56*	.196	**.029**	-1.08	-.04
	4	.15	.208	1.000	-.41	.70
2	1	.91*	.201	**.000**	.37	1.44
	3	.35	.207	.561	-.20	.90
	4	1.05*	.218	**.000**	.47	1.64
3	1	.56*	.196	**.029**	.04	1.08
	2	-.35	.207	.561	-.90	.20
	4	.71*	.214	**.007**	.14	1.27
4	1	-.15	.208	1.000	-.70	.41
	2	-1.05*	.218	**.000**	-1.64	-.47
	3	-.71*	.214	**.007**	-1.27	-.14

Based on observed means.

The error term is Mean Square(Error) = 1.139.

*. The mean difference is significant at the .05 level.

Table 53 compares Behaviour Score under conditions 1 to 4 within the interaction model. Significant different in behaviour score is noticed between conditions 1 and 2, 1 and 3, 4 and 2 and 4 and 3.

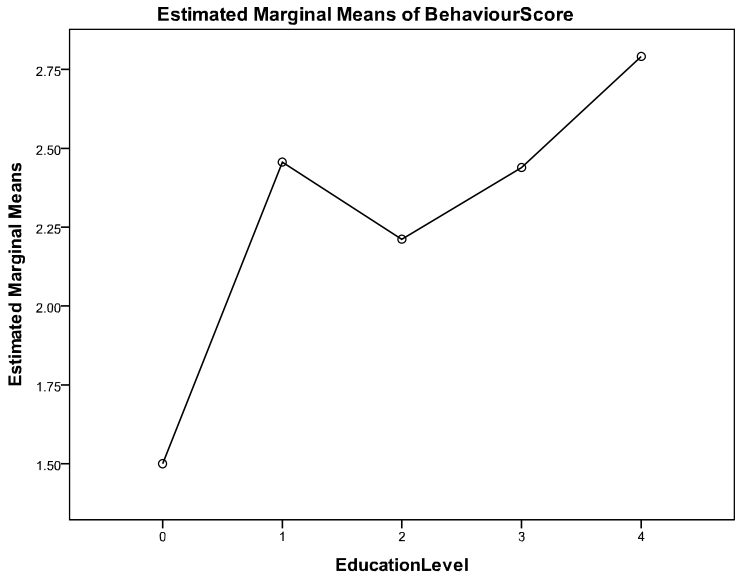


Figure 32: Behaviour score x education level graph for the interaction model

The graph above shows that the mean behaviour score generally increases when education level increases. The table below shows the mean behaviour score for each condition for participants with different education levels. For condition 1 (that is attractive source message) and condition 3 (strong message), privacy Behaviour Score increases with education level. Condition 2 shows fluctuations in Behaviour Score for the different education levels, but it can be seen that participants with O and A level education (education level 1 and 2) had higher Behaviour Score than graduates (education level 3 and 4). However, no such patterns can be discerned for the fluctuations of Behaviour Score in condition 4 (no persuasive message).

Table 54: Mean Behaviour score for each combination of Condition x Education level

Condition	EducationLevel	Mean	Std. Error	95% Confidence Interval	
				Lower Bound	Upper Bound
1	0	1.500	.534	.448	2.552
	1	1.692	.296	1.109	2.276
	2	1.429	.403	.633	2.224
	3	2.550	.239	2.079	3.021
	4	2.579	.245	2.096	3.062
2	0	.[a]	.	.	.
	1	3.333	.616	2.118	4.548
	2	3.800	.477	2.859	4.741
	3	2.500	.308	1.892	3.108
	4	3.194	.192	2.816	3.572
3	0	.[a]	.	.	.
	1	1.800	.477	.859	2.741
	2	2.333	.436	1.474	3.193
	3	2.588	.259	2.078	3.099
	4	3.107	.202	2.709	3.505
4	0	1.500	.534	.448	2.552
	1	3.000	.616	1.785	4.215
	2	1.286	.403	.490	2.081
	3	2.118	.259	1.607	2.628
	4	2.286	.285	1.723	2.848

a. This level combination of factors is not observed, thus the corresponding population marginal mean is not estimable.

6.3.3 Discussion and conclusion

This study simulated an E-Commerce task and did not inform end users before the study that it was aimed at assessing privacy behaviour. This was done to avoid privacy salience that would affect participants' behaviour and make it difficult to determine effects of the conditions of the design. Although the study has the advantage of not taking participants away from their environment to a research laboratory, it could be said to suffer from not being a real life situation. The study did not record the personal details entered by participants and the study was anonymous; it was not possible to determine whether participants entered their own details as they

would in an E-Commerce transaction. Financial details were also preset in the task. However a more real life approach would have been unfeasible within the scope of the research in terms of expense and time and recording of end user data.

In section 6.3.2, the testing of the first hypothesis that is whether privacy attitude has an effect on privacy behaviour, it was found that irrespective of persuasive condition privacy attitude, measured in the experiment through Westin's Privacy Segmentation Index, did affect privacy behaviour, measured through the Behaviour Score. Fundamentalists had significantly higher Behaviour Score than privacy unconcerned. This is because privacy fundamentalists have stronger privacy attitudes that is more accessible privacy attitudes and consequently more easily activated attitudes. These have a higher chance of predicting behaviour compared to less easily activated attitudes such as those of privacy unconcerned end users. Attitude accessibility is also related to the extent to which the attitude is perceived as personally important and relevant which in turn influences the extent to which the person is motivated to devote cognitive resources to evaluate the privacy situation. Furthermore, end users with more accessible attitudes would possibly have higher attitude-relevant knowledge of an issue. These might explain why fundamentalists exhibited more privacy behaviour. This finding is important since designing privacy mechanisms in such a way that allows end users to use privacy mechanisms according to their privacy requirements paves the way for effective use of privacy designs.

However, the sample of 215 participants was not divided into an equal number of privacy unconcerned, pragmatists and fundamentalists. The distribution of privacy attitudes within the sample followed Westin's findings in having a much higher number of pragmatists than unconcerned and fundamentalists (Kumaraguru and Cranor, 2005) but had approximately three times the number of fundamentalists to unconcerned. It would not have been feasible to collect the exact proportion of different types of privacy concern participants as expected by Westin's breakdown since this method would have involved selection of participants according to their privacy concern. Selecting participants using this method would have required querying participants about their privacy attitudes at a much earlier time to the user study to avoid contaminated behaviour and would make it difficult to separate effects

of the experimental conditions from those of the screening questionnaire. Moreover, if the study queried participants about their attitudes at a much earlier time to observing their behaviour, the study would have suffered from evaluative inconsistency as explained in section 3.3.2 in the Methodology Chapter.

Irrespective of their privacy concerns, end users can behave more privately under certain design conditions as found by testing the second hypothesis. The distribution of privacy unconcerned, pragmatists and fundamentalists in the four conditions followed the distribution of the sample population, that is an average of 63% of pragmatists. Condition 1, the attractive source that reminded participants to read the privacy policy generated a significantly lower privacy Behaviour Score than the more positive and personally relevant conditions 2 and 3, but similar effect as the simple reminder of condition 4. This finding shows that having an attractive source, with a reminder of privacy action, that is not personally relevant to end users, do not influence end users towards privacy behaviour by acting as a heuristic cue (as expected from such persuasive messages). This might be because this type of message fails to connect with end users' privacy attitude but instead distracts them from their privacy concerns. This type of design would result in a similar effect to not having a particular message added to the usual reminder and consent check as in condition 4.

Another aspect of the findings was the significantly higher behaviour caused by conditions 2 and 3 compared to conditions 1 and 4. That is condition 2 which was a weak message in terms of privacy but highlighted personal relevance and vested interest by the way the message was framed had a similarly high behaviour score to condition 3 which was a strong privacy argument that also hinted personal relevance. The mean plot of figure 29 also showed that condition 2 caused higher behaviour score than condition 3, although not significant. Since the message in condition 2 started with 'Would you like a comforting online experience?', the effect of condition 2 might be caused by additional elements to personal relevance that biases behaviour such as the fear of losing one's comfort or that comfort is an obvious choice irrespective of privacy concern. It would be further interesting to determine the long

term effects of reinforcing the link between privacy attitudes to behaviour of these two types of messages.

Other factors can also impact end users' online privacy behaviour and consequently the effectiveness of notice and choice in E-Commerce. There was a definite difference in Behaviour Score between those who have used E-Commerce only once before and those who used it at least five times within a month. This might hint that the more individuals use E-Commerce, the more they are aware of the privacy options of the service provider and the more they take privacy actions. Although it does not necessarily mean that they are more able to relate their privacy behaviour to their attitudes, this finding might be because the frequency of prior exposure to an attitude object affects end users' knowledge of the object and their attitude accessibility. These would in turn influence end users' elaboration of persuasive messages that can influence behaviour.

The other finding was that education level of participants interacted with persuasive condition. In conditions 1 (attractive source) and 3 (privacy argument), Behaviour Score increased with education level. That is within condition 1, as education level increased, the message with the attractive source was less of a distraction but more informative and within condition 3, as education increased, the strong privacy argument was seen as being more valuable. An increase in education level might be linked with having more information and hence being better equipped to assess a situation with regards to privacy. However, condition 2 was more effective in biasing the behaviour of participants with an O and A level than graduates.

To summarise, although not involving real life purchases, the study simulated an E-Commerce task that did not happen within a laboratory environment and consequently alleviated the pressure on participants. The study found that privacy attitude has an effect on behaviour when privacy management is linked to the disclosure context with the help of persuasive triggers. It was also found that some persuasive conditions can cause more private behaviour than others while others can distract end users from privacy behaviour. Furthermore education level of end users interacts with condition

of the design in affecting privacy behaviour whilst the extent of prior E-Commerce use affects behaviour on their own.

6.4 Contributions

In this section, the contributions of the study are underlined. The substantive contributions are provided followed by the methodological contributions.

6.4.1 Substantive

A major contribution of this study is the finding that privacy attitude does have an effect on privacy behaviour when privacy management processes are linked to the context of disclosure with the help of persuasive triggers. Under such conditions privacy fundamentalists can take more privacy behaviour than privacy unconcerned as expected from their privacy attitudes.

This finding is important since it is different from those of previous research that found that individuals do not behave according to their concern online and fundamentalists can even behave opposite to their concerns under certain conditions. This study showed that under conditions that make one's attitude more accessible, fundamentalists would behave as expected. It also shows that under these conditions, privacy mechanisms can be more effective and hence more usable.

Another finding was that the messages associated with reminding end users of privacy actions are important in determining privacy behaviour. The framing of the messages can be distracting, have not much to do with privacy but bias towards privacy behaviour or serve as the argument that reinforces privacy behaviour. However, although the design of these messages is important, the study showed that other factors such as end users' education level and their extent of prior E-Commerce use add to the complexity of whether end users would use privacy mechanisms.

6.5.2 Methodological

Study 7's design contributes to user study design within the research space. The first methodological contribution of the study was that it was not conducted within a laboratory environment. Participants were able to take part within their own

environment. This contributed to them taking the simulated E-Commerce task as close as they would normally do. Other contributions involve measurement of privacy behaviour. Privacy behaviour itself was measured compared to other previous research that observed disclosure behaviour as an indication of privacy. The study also compared general privacy concern to an aggregate measure of privacy behaviour to cater for evaluative consistency as opposed to comparing general privacy concern with distinct single behaviour.

Chapter 7: Discussion

7.1 Introduction

Previous research addressed the requirement of ensuring end user privacy online via different angles. They catered for the legal and technological requirements, but online privacy mechanisms remain in-effective in ensuring end users' privacy protection. As reviewed in Chapter 2, possible explanations were found for the in-effectiveness ranging from end users' irrational behaviour, end users' need for immediate gratification, end users' trust in the service provider together with un-usable and unhelpful privacy designs. Enhancements were suggested to design that would facilitate the communication of disclosure information to end users or aid privacy task completion. The effect of these enhancements in aiding end users' understanding of disclosure information and in completing privacy related actions such as opening the privacy policy were explored and end users' choice of different methods of presenting privacy settings and the privacy policy were compared. The role of these enhancements as influence methods that could activate privacy attitudes or make privacy attitudes accessible and as the means to help in providing for the socio-psychological processes of privacy management were however not considered. The role of persuasive triggers in supporting privacy management processes were not looked into and an assessment of whether existing designs provided for these processes in the first place was not done. Previous research did not look into the prospect of using those to link the design with end users' privacy attitudes, that is

research was not conducted in enhancing the effectiveness of privacy mechanisms by enabling end users to take privacy actions that match their privacy attitudes. They consequently also did not look into the effects of different types of influence or persuasive communication methods on privacy behaviour.

Following identification of the research gap, the research within this thesis conducted 7 studies (including 2 pilots) to answer three research questions. The research questions are:

- RQ1: What are the requirements for usable online privacy mechanisms?
- RQ2: How usable are existing online privacy mechanisms?
- RQ3: How does persuasive communication impact the effectiveness of online privacy mechanisms?

This chapter first presents a model that depicts the findings of the research. It then discusses the findings in the context of the research gap and their contribution to the model and examines the extent to which the studies' findings help to answer each of the research questions. It elaborates on the significance of these findings and proposes ways of addressing the limitations in the findings.

7.2 Model of privacy attitude-behaviour link

A model of how persuasive communication supports the attitude-behaviour link within privacy design is introduced following the literature review, exploratory analysis and experimental study of this thesis. The model accounts for the components of attitudes, namely: cognition, affect and behaviour and shows the path through which persuasive communication links privacy attitude to behaviour as shown in figure 33 below. This section describes the main tenets of the model whereas the following sections review the research findings in terms of the model and research gaps.

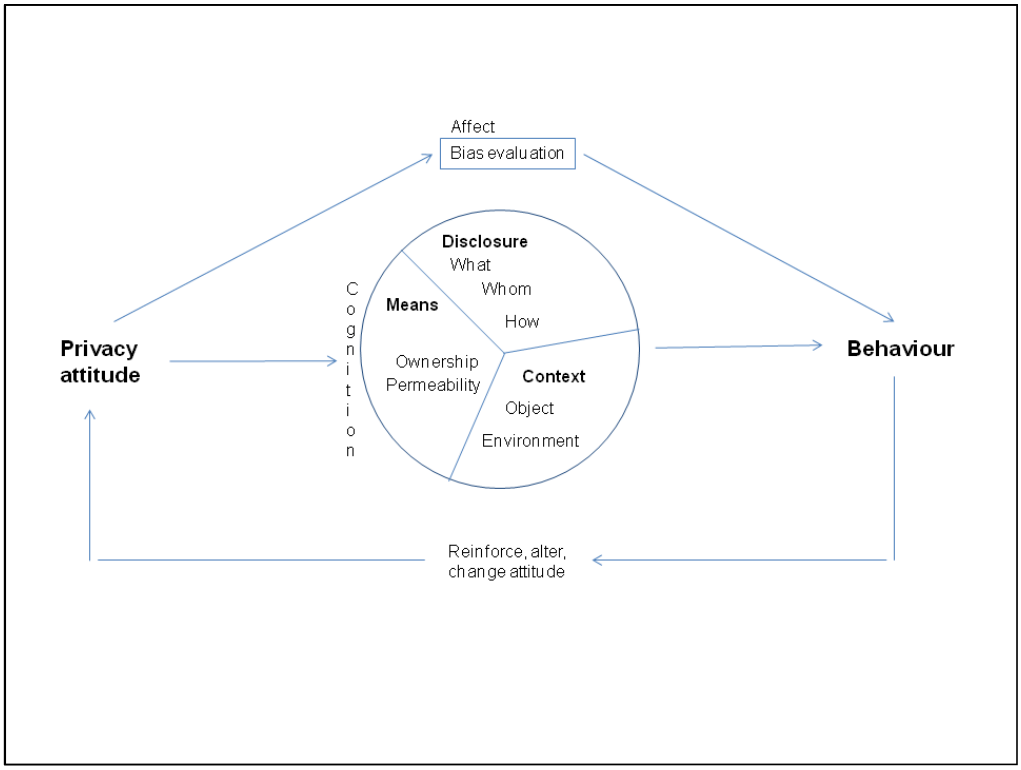


Figure 33: Model of how persuasive communication support the privacy attitude-behaviour link

Privacy attitude is a cognitive construct residing in memory that can be activated if it is linked with a context of disclosure that requires control of access to personal information. In the 'affect' part of the model, automatic activation of privacy attitude can happen with privacy cues within the design that biases attitude object evaluation. For example the presence or absence of privacy representations such as the presence of the privacy policies in Jensen et al. (2005) influenced the choice and consequently behaviour of end users. The presence of privacy cues and the presumed support for privacy protection can also cause a connection with the trust attitude such as in Joinson et al. (2010). This thesis showed that a simple reminder and one with an attractive source provided no support in influencing privacy behaviour but one with a 'comforting experience' message was significantly valuable in triggering privacy behaviour possibly acting as a peripheral cue that biased privacy behaviour.

In the 'cognition' part of the model persuasive communication can trigger information transfer that is present information, symbols and nudges that support the social-psychological processes of privacy management and ease end users' effort in building

a mental picture of their privacy. This type of design can aid or ease evaluation of an object or context in terms of privacy attitudes causing privacy attitudes to be activated or to enhance their accessibility resulting in increased likelihood of them showing in behaviour. The mental model that end users are to build includes principles of CPM that was found to be particularly important in Studies 4 and 5: awareness of disclosure together with availability of means that support ownership and permeability negotiation. As shown by Study 7, persuasive communication can provide the cognition part of the model in the form of an argument that supports privacy evaluation or enhances scrutiny of the context with respect to privacy. In previous research, proposed enhancements to designs such as better presentation of the privacy policy (McDonald et al.,2009; Kelley et al., 2009; Richter-Lipford et al., 2010), better interfaces for specific privacy enhancing technologies (Cranor et al., 2006) and enhanced visual feedback (Richter-Lipford et al., 2008) are example of means that support formation of the mental model by providing better privacy-disclosure information within a context.

7.3 Research question 1

In the literature review, it was found that there was a lack of clear literature on what it means for online privacy to be usable in general. In particular there were no endeavours specifically aimed at exploring usability design requirements for privacy that would guide proposals and evaluations. Such an exploration benefits from a multidisciplinary perspective that does not restrict the process to a legal or technological perspective. This research answered RQ1 that is 'What are the requirements of usable online privacy?' through Study 1.

Study 1 was designed to elaborate on the requirements of online privacy design from a multidisciplinary perspective by involving a group of privacy experts who belong to various research disciplines. Experts were selected over end users to enable a deep reflection on the issue of usability of privacy designs and also because, as was previously found (VOME, 2012b), end users cannot clearly explain privacy and therefore its requirements especially without a context or situation.

This section explains the extent to which the first study answers the first research question and contributes to the model of figure 33. It then explores the significance and implications of these findings for the theory in the research space and the practice of designing usable online privacy. This is followed by identifying the limitations of the findings and suggesting how they can be addressed.

Findings of Study 1

The outcome of Study 1 was a list of requirements, suggested by privacy experts, that is expected to enhance the usability of online privacy. An important element of the list was end user control. It was suggested that end user control should however run in parallel to system services and require minimum user effort. Experts stressed on the complexity and challenge of designing usable online privacy which supports and explains the findings of the literature review that is online privacy designs suffer from a large amount of usability issues. To address the challenge, the experts suggested a list of ways that can help to provide for the conflicting requirements of end user control and minimum effort in balance with system services and advised on carefully considering the context of use during design. These were predefined custom privacy levels, standard privacy methods across systems, default privacy, explicit opt-in and feedback and could be considered as nudges or persuasive element.

Experts' suggestions that, irrespective of context or privacy solution, enabling end user control of what is shared with whom under what circumstances would ensure usability, imply that end users should be directly involved in managing their privacy. This outcome of Study 1 contributes to the model of figure 33 because direct involvement would force or trigger cognitive evaluation of the interactions enabling end users to categorise the interactions as an experience requiring control of access to the self that is in terms of privacy attitudes. Alternatively, the act of being involved in controlling one's privacy might enhance the ease with which end users' privacy attitudes are retrieved from memory that is privacy attitudes might be accessible. Activated or accessible privacy attitudes can be expected to have a high chance of being reflected in behaviour.

Significance and limitations of the findings of Study 1

The findings of Study 1 are significant because such a study, involving the collaboration of a varied group of privacy experts sharing opinions and reviewing those opinions, was not conducted before in the online privacy research space. These findings are also significant for designers who need to find ways to cater for the requirements of usable online privacy. It is also significant to build theory around the ways through which HCI can help to cater for these requirements such as the approach used within this thesis that taps into social-psychology to devise ways for making privacy attitudes active or accessible.

Given that RQ1 is framed as a general question not specific to a context, the qualitative exploration of Study 1 identified the essential but non-exhaustive list of requirements for usable online privacy. Therefore, when applying these requirements, the context of the privacy designs have to be carefully considered to determine the ways of providing for user control with minimum effort while not disrupting system services. For instance, as suggested by the privacy experts, end users could be nudged towards privacy but the nudges should be designed specifically for each context.

7.4 Research question 2

Although end users seamlessly and instinctively manage their privacy offline, they are not able to do so online. The literature review discussed a variety of usability issues associated with online privacy design. Study 1 provided a list of requirements suggested to ensure the usability of online privacy mechanisms. Studies 3, 4 and 5 were designed to assess whether existing privacy designs can be expected to be usable that is whether they provided for the processes that would support the requirements of end user control of their privacy within the bounds of minimum effort that is enable end users to manage their privacy as seamlessly as they are used to offline. They answered RQ2 that is ‘How usable are existing online privacy mechanisms?’.

This section explains the extent to which Studies 3, 4 and 5 answer the second research question and contribute to the model of figure 33. It then explores the

significance and implications of these findings and follows by identifying the limitations of the studies and suggests how they can be addressed.

Findings of Studies 3, 4 and 5

Through a cognitive walkthrough approach designed to find out whether end users would be able to manage their privacy by completing the privacy tasks in Facebook, Study 3 explored whether the design helped end users in identifying and learning to use privacy mechanisms. The study determined whether the interface and interaction design of Facebook would enable a cognitive connection with the effect end users are trying to achieve that is sharing of personal information while protecting their privacy and whether they would be able to link the presence of privacy mechanisms with their privacy requirements. Therefore the study determined whether Facebook contributed to the cognition part of the model of figure 33 that would help to link privacy behaviour with attitudes. Facebook was found to require design modifications for its privacy design to enable end users to do so. However, the cognitive walkthrough method suffers from researcher bias and the design was limited to only the awareness aspect of the social psychological process of privacy management. A more systematic evaluation was consequently designed for studies 4 and 5.

The more systematic approach took the main findings of Study 1 into account that is the requirement for end user control and minimum effort within a context of use. Since it is difficult to evaluate the extent of end user effort required by the design without involving end users in the analytical evaluation, the principles of a social-psychological theory (CPM) that depicts seamless privacy management was mapped to online privacy design. Semiotic inspection was guided by the principles of CPM (Communication Privacy Management) to explicate how privacy designs provided for the processes of privacy management and the social-psychological link to end users' privacy attitudes, that is the connection between attitudes and behaviour as in the model of figure 33. As discussed in Chapter 3 (Methodology), CPM views the process of disclosure as inherently dialectical that is disclosure is seen as the process of revealing private information yet always in relationship to concealing private information. Privacy information is also conceptualised in terms of possession such

that individuals believe they own their private information and consequently have the right to control it. CPM provides the metaphor of boundaries to illustrate that although there is a flow of private information to others; borders mark ownership lines within a boundary management system. This illustration and the simultaneous nature of wanting to tell and also wanting to conceal not only makes CPM theory valuable to understand how people navigate privacy but also makes it helpful to assess whether online interaction designs caters for both processes of revealing and concealing private information. Catering for both of these is essential to enable end user privacy management without disrupting system services. These components of CPM and system services (context) make up the cognition part of the model.

Study 4 evaluated the internet browser privacy tabs and Study 5 E-Commerce websites' notice and choice design. The findings from Studies 4 and 5 showed that two different context of designing privacy, within internet browsers and E-Commerce, suffered from communication breakdowns that would affect end user control. While internet browsers' privacy tabs provided for the mechanisms to protect one's privacy, it does not make the disclosure part of the dialectical tension clear to end users. End users would not be able to picture what would be disclosed to whom and how since the static interface and the dynamic interactions of internet browsers do not provide this support. The lack of support for the disclosure context would make it tricky for end users to cognitively evaluate their private-public boundary hence rendering the availability of the privacy mechanisms not useful in enabling end users to manage their boundaries. As shown in the model, a missing part of the cognition component might hamper the link between privacy attitude and behaviour since it would also be difficult for end users to associate their available privacy attitudes with an imaginary disclosure context. This would result in end users not equipped to protect their privacy, using internet browsers' privacy tabs, to the extent expected by their privacy attitudes. The E-Commerce websites provided the disclosure context but it was not clear who would own the revealed personal information and how it can be further spread to other parties. Although end users' privacy attitudes might be activated during interaction with the websites, there was no clear, visible and relevant means to protect their privacy. According to the model, although privacy attitude is activated, a

lack of means in cognition will not enable end users to react with privacy behaviour. That is end users would not be able to associate their disclosure of private content to the use of the provided notice and choice and not be able to see the relevance of these to their privacy leading to their inability to exercise their privacy boundary management.

Apart from providing for the dialectical grounds for disclosure of private information and privacy protection, designs should also ensure consistent information is communicated via help documentation, static interfaces and dynamic interactions. The designs should enable end users to grasp the personal relevance and vested interest in using privacy mechanisms. These could contribute to more easily accessible attitudes that have a higher chance of reflecting in behaviour through either the cognition or affect part of the model. However, the effort or hassle value must not overburden end users. For instance in the case of internet browsers privacy tabs, end users must be able to access their privacy attitudes during each browsing activity without straining end users. These conditions might be practically impossible to achieve without the use of persuasive communication which can facilitate or enable the cognitive effort required to evaluate a given circumstance as requiring privacy protection and ease the access and activation of end users' privacy attitudes to exercise privacy protection.

Significance and limitations of the findings of Studies 3, 4 and 5

The findings of Studies 3, 4 and 5 are significant in demonstrating why privacy mechanisms are reputed to be in-effective that is by not enabling end users to behave according to their privacy attitudes. The findings of Studies 3, 4 and 5 are also significant for the research space since they suggest the need for further research that would explore and cater for the dialectical tension required within privacy design. However providing the dialectical tension might not be an easy task since enabling end user privacy management should not disrupt system services. Too high privacy salience can cause end users to shun away from disclosing any personal information and consequently affect service provision.

More research is needed to understand privacy interactions as a form of human-computer interactions. The real-life conceptual framework (CPM) was mapped onto privacy HCI and identified key issues. Although (CPM) was helpful for the purpose of the evaluation, a revised privacy management framework within HCI that accounts for the limitations and constraints of the online environment could be useful. Moreover, although Studies 3, 4 and 5 answered RQ2 from an effectiveness and communication perspective of usability, there is however a variety of other perspectives through which usability can be assessed and these might be useful for future research. The perspective selected by this research however contributed to identifying communication breakdowns in the different context that can be useful when designing more persuasive privacy. Studies 3, 4 and 5 also only considered three contexts within which privacy management are embedded. Further research might provide valuable insight when evaluating stand-alone privacy solutions within different contexts.

7.5 Research question 3

The literature review identified a research gap that is that previous research has not looked into the contributions of persuasive communication on assisting the activation and accessibility of end users' privacy attitudes. This would ease privacy attitude's reflection on privacy behaviour and effectiveness of online privacy mechanisms would be improved as shown in the model.

To ease cognitive effort, provide the dialectical tension (found to be absent in Studies 3, 4 and 5), enable depiction of a mental model, and moderate the attitude-behaviour relationship, persuasive communication is proposed. Persuasive communication can trigger, bias or ease cognitive evaluation such as highlighting the personal relevance or personal interest, or by diverting attention, persuasive communication can enable user control of disclosed private information. As shown in the model, this would link privacy behaviour with attitudes. Given that the ability to behave according to one's privacy attitudes is an indication of the effectiveness of privacy mechanisms, Study 7 observed privacy behaviour under different conditions to find out whether those conditions contribute to privacy behaviour and answered RQ3 that is 'How does

persuasive communication impact the effectiveness of online privacy mechanisms?'. This section discusses the findings of Study 7 in terms of the research gap and the proposed model.

Findings of Study 7

Study 7 answered RQ3 by showing that persuasive communication can affect the usability of online privacy mechanisms by enabling end users to behave according to their privacy attitudes. This was shown by privacy fundamentalists scoring more private behaviour than privacy unconcerned. Privacy fundamentalists have strong privacy attitudes (because they consistently evaluate a situation as requiring privacy protection), and have higher privacy attitude accessibility than privacy unconcerned. They have a higher likelihood that their privacy attitude will be automatically activated from memory upon mere encounter with the attitude object and may more easily detect the need to exercise privacy or be prepared to spend cognitive effort. Attitude accessibility also determines the extent to which the attitude is perceived as personally important and relevant which in turn influences the extent to which the person is motivated to devote cognitive resources to evaluate the privacy situation. Furthermore, end users with more accessible attitudes would possibly have higher attitude-relevant knowledge of an issue. This might also explain why fundamentalists exhibited more private behaviour. Therefore under favourable conditions stronger privacy attitudes will predict behaviour. The significance is that designs should be carefully thought of or implemented such that available attitudes are retrieved from memory and associated with the context of use.

The study also showed end users' privacy behaviour response was different for each message. Some persuasive conditions (design conditions) were observed to cause more private behaviour than others or to distract end users from privacy behaviour. Condition 1, the attractive source seemed to distract participants from privacy behaviour while significantly higher behaviour was caused by conditions 2 and 3. Condition 2 was a weak message in terms of privacy but highlighted personal relevance and vested interest by the way the message was framed. It had a similarly high behaviour score to condition 3 which was a strong privacy argument that also

hinted personal relevance. Conditions 2 and 3 show different routes from attitude to behaviour within the model.

Study 7 also highlighted the contribution of education level and extent of prior E-Commerce use on privacy behaviour. There was a definite difference in behaviour score between those who have used E-Commerce only once before and those who used it at least five times within a month. This might hint towards a link between extent of E-Commerce use and privacy behaviour such that higher frequency of E-Commerce use led to more private behaviour. This might be bacause the frequency of prior exposure to an attitude object affects end users' knowledge of the object and their attitude accessibility. These would in turn influence end users' elaboration of persuasive messages that can influence behaviour.

Education level was also found to affect privacy behaviour. Under two conditions, higher education level was linked with higher behaviour score. Therefore individuals who have more information or knowledge of online privacy would also benefit from conditions that appeal more in terms of socio-psychological processes for managing privacy.

Significance and limitations of the findings of Study 7

These findings are significant because they showed that privacy behaviour can vary and consequently also effectiveness of online privacy mechanisms under different persuasive design conditions. Some persuasive condition can ease activation of available privacy attitude or enhance accessibility more that is help end users to categorise the experience in terms of their attitude from memory or to retrieve the attitude from memory more easily than others. This is done by easing end users' allocation of cognitive resources required to evaluate the situation or bias evaluation or provide the arguments necessary such that attitudes prediction of behaviour is also facilitated. Therefore some persuasive communication can help end users to manage their privacy with relative ease whereas other conditions are less helpful. This is because when a person has a highly accessible attitude, that attitude is quickly and relatively effortlessly retrieved from memory when the person is exposed to the corresponding attitude object.

The study is also significant in showing that having an attractive source who reminds end users of a privacy action and reminders that are not personally relevant to end users, do not influence end users towards privacy behaviour by acting as a heuristic cue (as would be expected from such persuasive messages). This might be because this type of message fails to associate end users' attitude with the experience or facilitate retrieval of attitude from memory but instead distracts them from their privacy concerns. This type of design would result in a similar effect to not having a particular message added to the usual reminder and consent check as in condition 4 and should be avoided in designs.

The findings of this study are important for the research space to trigger further research in the use of persuasive communication on privacy attitude accessibility and activation. It also suggests the benefit of considering the social psychological relationship between attitude and behaviour for privacy design and HCI design in general.

Study 7 is limited because only one aspect of usability that is effectiveness was under investigation. It was also limited to the context of E-Commerce. Further research could investigate persuasive communication in other contexts of privacy design. The user study was also designed with only four different persuasive conditions. A more thorough investigation might investigate other persuasive conditions.

Chapter 8: Conclusions

8.1 Introduction

Privacy is a human right but effectiveness of online privacy mechanisms is a real world problem that upsets the assurance of end users' privacy protection. Privacy being an interactional process, privacy behaviour online is a response to components of the design. Privacy behaviour is therefore highly dependent on HCI. Moreover, although it has been shown that end users' privacy behaviour rarely match their privacy attitudes online, no empirical effort has harnessed the capability of HCI designs to link privacy attitudes with behaviour.

This thesis explored the requirements for usable online privacy and assessed online privacy designs. The findings were that existing designs do not provide for the social psychological processes that would activate privacy attitudes or make privacy attitudes accessible. These findings support the research approach of aiming to connect privacy attitudes with behaviour via the design. The research provided empirical evidence that privacy behaviour depends highly on the framing of messages in the design and contributes to the development of a better communication approach through the use of persuasive technology.

This chapter presents and reflects upon the contributions of the research conducted in this thesis and proposes future directions of research. It starts by restating the

research problem and follows by highlighting the contributions of the thesis. It then critically reviews the research before concluding with proposals for future research.

8.2 The problem restated

In section 2.6, the research gap was identified. Previous research has not identified the requirements of usable online privacy from a multidisciplinary perspective that could help to guide usability evaluations and proposals for enhancements. Although online privacy designs were evaluated and enhancements proposed, previous research has not identified issues with online designs' contributions to the social psychological processes of privacy management. They have also not proposed better ways of contributing to these processes.

The research within this thesis addressed the research gap. Privacy is a tacit behavioural concept ingrained within real life communication and the research takes the challenge of enabling HCI designs to mediate the link between end users' privacy attitudes and the evaluation of an online context as requiring management of privacy and disclosure that enables end users to engage in privacy behaviour. However HCI designs of privacy not only have to connect with end users' privacy attitudes but also to run in parallel to system services, to provide for system usability requirements such as ease of use and to cater for requirements of privacy such as user control and intuitiveness.

Means aimed to invoke privacy attitudes such as persuasive communication can cause different effects such as enhancing privacy behaviour or distracting end users from privacy behaviour. This is because they can ease or trigger cognitive evaluation of a situation; provide the arguments to support a course of action or bias behaviour. The thesis answered the following research questions:

- RQ1: What are the requirements of usable online privacy?
- RQ2: How usable are existing online privacy mechanisms?
- RQ3: How does persuasive communication affect the effectiveness of online privacy mechanisms?

8.3 Contributions of Thesis

This section re-asserts the contributions of the thesis to the research space. It presents the contributions of the thesis by reviewing the findings in answering each of three research questions and the approach designed to answer the research questions.

8.3.1 Substantive

In the substantive contributions section, the findings of the research in the process of answering the three research questions are recapitulated. The contributions are valuable in promoting better privacy designs and motivating further understanding of the social psychological dimension of the online privacy management process. The section starts with the usability requirements suggested by privacy experts followed by the outcome of assessing online designs and concludes with privacy behaviour under the influence of persuasive communication.

Requirements for usable online privacy

The outcome of iteratively reviewing experts' opinions was a list of usability requirements for online privacy. The main aspect of the list was the necessity of the privacy design to provide for end user control of personal information while demanding minimum end user effort. The privacy experts explored these contradictory requirements of privacy design that is made even more challenging with the need of privacy mechanisms to co-exist with system functions such as collecting personal information to enable provision of services. The privacy experts suggested ways of dealing with the challenges such as predefined custom privacy levels, standard interfaces, default privacy, explicit opt-in and feedback. These suggestions are examples of persuasive communication methods that can motivate towards or facilitate privacy behaviour.

Assessment of usability of online privacy mechanisms

By answering the second research question, the thesis contributed to exploring whether end users could be expected to use existing privacy mechanisms effectively, that is whether online designs enabled the social psychological process of privacy management. Studies 2 to 5 provided the findings that assisted the design of a model

depicting how persuasive communication can support the link between privacy attitudes and behaviour and enforce effective online privacy.

- Pilot Study 2 (in Chapter 5) showed that the use of the privacy mechanisms of Facebook was not clear to end users. This was supported by Study 3 that found that the design of the interface did not help end users to identify and learn how to use the privacy mechanisms of Facebook that is did not provide a cognitive connection with privacy. By enabling a breakdown of the identified tasks into their action sequence and assessing each of the actions, it was possible to point out where modifications, that would help end users relate their disclosure actions to the privacy possibilities, would be required within the design.
- Another finding was that privacy mechanisms are not consistent in their communication of privacy information that could help end users to manage their privacy effectively. Study 4 (in Chapter 5) showed that internet browsers provided clearer privacy information in the help pages that were difficult to access from the static interface and dynamic interactions. Also the dialectical tension between disclosure and privacy was absent that is privacy mechanisms were not linked to a disclosure context leaving end users to imagine the context. This would make it difficult for end users to assess their private-public boundary such that using the privacy mechanisms to manage privacy according to their attitudes is made unfeasible. According to the evaluation's analytical criteria, changes to the communication of internet browsers' privacy information such as coherent information in all instances together with visibility and easy access to privacy mechanisms would enhance effectiveness and hence usability of the privacy design of internet browsers.
- In a similar analytical evaluation of E-Commerce websites within Study 5 (in Chapter 5), it was found that the websites hardly communicated privacy information that could help end users relate their disclosure interactions to the privacy choices provided by the websites. They also did not consistently provide information such that more privacy information was provided in the privacy policy and practically none within the disclosure context. The

interaction flow of the checkout function did not give end users any reason to read the privacy policy. It was concluded that E-Commerce privacy design would be more effective if the interaction flow was linked with the privacy means such that privacy attitudes can be activated and the personal relevance and vested interest in using the privacy mechanisms is highlighted. Activated or accessed privacy attitudes also have a higher likelihood of being transferred into behaviour.

These findings were important in proposing a model of how persuasive communication (figure 33) can help to make the connection between privacy attitudes and behaviour. It either enables an 'affect' link that biases end users towards privacy behaviour or facilitates provision of the 'cognition' component that supports the social psychological processes of privacy management.

Privacy behaviour within persuasive privacy design

A major contribution of the experimental part of the thesis in Study 7 (of Chapter 6) is the finding that privacy attitude does have an effect on privacy behaviour and under persuasive conditions privacy mechanisms can be more effective and hence more usable. Moreover under conditions that make one's attitude more accessible, privacy fundamentalists do take more privacy behaviour than privacy unconcerned as expected from their privacy attitudes. This finding is important since it is different from those of previous research that found that end users do not behave according to their concern online.

Another finding was that the messages associated with reminding end users of privacy actions are important in determining privacy behaviour. The framing of the messages can either be distracting and result in poor privacy behaviour or have not much to do with privacy but still bias towards privacy behaviour or serve as the argument that reinforces privacy behaviour. This is depicted by the 'affect' and 'cognition' of the model of figure 33. The study also showed that other factors such as end users' education level and their extent of prior E-Commerce use add to the complexity of whether end users would use privacy mechanisms.

Therefore whilst showing that persuasive communication can help to bridge the gap between privacy attitudes and behaviour, the thesis also shows that effectiveness and consequently usability of online privacy mechanisms can be improved. It however also hints that further research is needed to understand how influencing the socio-psychological link between attitudes and behaviour can further help HCI designs.

8.3.2 Methodological

The thesis' methodology contributes to research design within the online privacy research space. A panoply of HCI research methods were designed through a mixed method approach that started with grounded theory to gain insight into the complexity of usable online privacy. It was followed by analytical evaluation of existing design through a social-psychological framework of privacy management. The thesis also involved social-psychological understanding of the relationship between attitudes and behaviour that guided the design of a quantitative empirical investigation. This section describes how the methodology design is innovative to the research space.

The first methodological contribution is the design of the exploration for requirements of usable online privacy that produced rich data. A multidisciplinary group of academic and professional privacy experts were involved in a small debate within a Delphi structure that involved iterative reviews of experts' opinions. The participants were anonymous to each other and the analysis was performed through grounded theory coding techniques. Delphi has been used before in information systems research to untangle complex problems but not within the online privacy or security research space.

The second contribution was the systematic evaluation design within a case-study approach aimed to analyse the communicability of HCI designs of privacy mechanisms. It used the principles of a real world framework of privacy management; Communication Privacy Management which describes the processes used by individuals to seamlessly manage their privacy, to find out whether privacy online is designed in a similarly effective way. The approach helped to maintain the researcher's interpretation bias to a minimum.

The third methodological contribution of the research was the design of an experimental user study that involved a simulated task within a real world setting rather than a laboratory environment that takes end users away from their usual environment. This contributed to participants taking the simulated E-Commerce task as close as they would normally do. Participants were not informed beforehand that it was a privacy study to avoid biasing their behaviour. Moreover privacy behaviour itself was measured and general privacy concern was compared to an aggregate measure of privacy behaviour to cater for evaluative consistency. This is an enhancement on previous research that observed disclosure behaviour as an indication of privacy.

8.4 Critical review

In this section, the research presented in this thesis is critiqued. Limitations with the research approach are identified and discussed. The section starts with the sampling approach and ends with the ethical issues.

Sampling

The analytical evaluations were conducted in 2009 and 2010. Since then Facebook has changed continuously. Internet browsers have also added features such as 'Do Not Track'. The problem with these technologies is that they keep evolving due to new technological advances and to user needs and it would not be possible to evaluate each version of changes. However, the analytical evaluation presents an assessment for Facebook and the privacy tab only for internet browsers at a point in time. InPrivate browsing was not considered since only selecting private browsing mode does not actually protect end users (Aggarwal et al., 2010) or ensure they can manage their privacy. The thesis also only reviewed social network service, internet browsers and E-Commerce websites which are popular contexts or media of disclosure, rather than stand alone privacy mechanisms. This was because it was difficult to gain access to and evaluate other mechanisms such as those that provide for pseudonymity within a disclosure context. Also only one context was designed within the user experiment.

The E-Commerce context was chosen for the experiment since the design of privacy within such an essential business service has been claimed to be ineffective.

Evaluation did not involve real world scenario

The assessment of the impact of persuasive communication involved an E-Commerce context but involved a simulation rather than a real world scenario. It could be argued that the findings would be different if it was designed within an existing live E-Commerce website. Although the experimental study simulated a real world scenario as close as possible, the only way to ascertain that the findings would replicate in the real world would be to compare the findings of study 7 with those designed on a service provider's website. This could be done in future research that would cater for the resources required.

Ethical aspect

Participants of the experimental studies were not informed of the true aim of the study beforehand that is they were not informed that the study is specifically aimed at observing and assessing their privacy behaviour. This characteristic of the design was a necessity since any mention of privacy would have affected participants' responses and behaviour making it more difficult to ascertain whether the observed behaviour was due to persuasive conditions in the design. However, the study designs made sure that any personal information entered during the study, such as name and address, was not being saved by the website and the usability software used for data collection. Study 6 obtained consent from participants who were explained the full purpose of the study at the end of their participation. Study 7 clearly reassured participants about the anonymity of the process at the end of the study.

8.5 Further research directions

This section elaborates on research ideas that emanate from the current research. These can form the foundation for future research in the field.

Habit formation

Study 7 investigated the one time effect of persuasive communication on privacy behaviour. Further research could determine the impact of the persuasive message on other E-Commerce interactions in a longitudinal study. It would also be valuable to determine how the strength of the persuasive message (with respect to privacy) affects current and future privacy behaviour. This would enable exploration of the cascading effects of persuasive messages on end users' privacy decision making and ability to distinguish between service providers.

Effect of prior experience and education on privacy behaviour

End users who have suffered a privacy breach might be more careful in their online behaviour because of recently activated or more accessible privacy attitudes. An understanding of the relation between the type of previous experience (and extent of personal affliction) and privacy behaviour could help in designing effective and long term programmes aimed at educating end users of online privacy risks. Following-up on the research, further research could also dig into the mechanisms of the interaction between education level and persuasive communication and explore the possibility of designing systems that would not disfavour certain group of users.

Type of cognitive processing involved

Determining whether privacy fundamentalists, pragmatists and unconcerned individuals use central or peripheral processing with respect to the type or strength of persuasive message would help privacy designers and service providers to ensure end users are informed and receive the same level of service irrespective of their privacy concern. Future research could investigate how different types of privacy concern end users cognitively process persuasive messages and the impact of these cognitive processes on their behaviour.

Real world service provider

The research can be extended to explore its benefits within a real world service provider's website. This will help to apply and compare the findings of the research within a practical context.

Security, health and energy conservation context

Persuasive communication research is popular in health and energy conservation contexts. However the specific approach of activating and improving accessibility of attitudes as a link to behaviour can be further investigated. Information security would also benefit from this perspective to not only further investigate usable security methods but also to better understand and mitigate social engineering threats.

References

Ackerman, M. S. and Cranor, L. (1999) 'Privacy Critics: UI interfaces to safeguard users' privacy'. *ACM Conference on Human Factors of Computing Systems*, Pittsburg, Pennsylvania, 15-20 May 1999, 2, New York: ACM, pp. 258-259.

Acquisti, A. (2004) 'Privacy in electronic commerce and the economics of immediate gratification', *5th ACM conference on Electronic commerce*. New York, 17-20 May. New York: ACM, pp. 21-29.

Acquisti, A. and Grossklags, J. (2005a) 'Privacy and Rationality in individual decision making'. *IEEE Security and Privacy*, 3(1), pp. 26-33.

Acquisti, A. and Grossklags, J. (2005b) 'Uncertainty, ambiguity and privacy', *4th Annual Workshop on the Economics of Information Security*. Harvard University, MA, 1-3 June.

Acquisti, A. and Gross, R. (2006) 'Imagined communities, awareness, information sharing and privacy on the Facebook', *6th Conference on Privacy Enhancing Technologies*. Cambridge, UK, 28-30 June. Berlin: Heidelberg: Springer-Verlag, pp. 36-58.

Adams, A. and Sasse, M. A. (1999) 'Privacy issues in ubiquitous multimedia environments: wake sleeping dogs, or let them lie?', in: Sasse, M. A. and Johnson, C. (eds.), *7th IFIP Conference on Human-Computer Interaction - INTERACT'99*, Edinburgh Conference Centre, Scotland, 30th August - 3rd September, Amsterdam: IOS Press .

Adams, A., Sasse, M. A. and Lunt, P. (2005) 'Social empowerment and exclusion: a case study on digital libraries'. *ACM Transactions on Computer-Human Interaction*, 12(2), pp. 174-200.

Adams, A., Lunt, P. and Cairns, P. (2008) 'A qualitative approach to HCI research', in Cairns, P. and Cox, A. L. (eds.) *Research Methods for Human-Computer Interaction*, 1st edn. Cambridge, UK: Cambridge University Press, pp. 138-157.

Aggarwal, G., Bursztein, E., Jackson, C. and Boneh, D. (2010) 'An analysis of private browsing modes in modern browsers', *19th USENIX Security Symposium*, Washington D.C., 11-13 August. Berkeley, CA: USENIX Association, pp. 6-23.

Agre, P. E. and Rotenberg, M. (1997) 'Technology and Privacy: The New Landscape', *Harvard Journal of Law & Technology*, 11(3), pp. 325. Cambridge, MA: MIT Press.

Ajzen, I. and Fishbein, M. (1977) 'Attitude-behavior relations: A theoretical analysis and review of empirical research'. *Psychological bulletin*, 84, pp. 888-918.

Ajzen, I. and Fishbein, M. (2005) 'The influence of attitudes on behavior', in Albarracin, D., Johnson, B. T. and Zanna, M. P. (eds.) *The handbook of attitudes and attitude change*, NJ: Erlbaum, pp. 173-221.

Allport, G. W. (1935) 'Attitude', in Murchison, C. (ed.) *A handbook of social psychology*, 2nd edn., Worcester, MA: Clark University Press, pp. 798-844.

Altman, I. (1975) *The Environment and Social Behaviour: Privacy, Personal Space, Territory and Crowding*. Monterey, California: Brooks/Cole Publishing.

Anonymizer (2012) *Anonymizer*. Available at: http://www.anonymizer.com/ (Accessed 01 August 2012).

Antón, A. I., Earp, J. B., Bolchini, D., He, Q., Jensen, C. and Stufflebeam, W. (2004) 'Financial privacy policies and the need for standardization'. *IEEE Security and Privacy*, 2(2), pp. 36-45.

AT & T Corp. (2006) *Privacy Bird*. Available at: http://www.privacybird.org/ (Accessed August 2012).

Augoustinos, M., Walker, I. and Donaghue, N. (2006) 'Attitudes', in Augoustinos, M., Walker, I. and Donaghue, N. (eds.) *Social Cognition: An integrated introduction*, 2nd edn. London, UK: Sage Publications, pp. 112-134.

Austin, L. (2003) 'Privacy and the Question of Technology'. *Law and Philosophy*, 22(2), pp. 119-166.

Bargh, J. A. and McKenna, K. Y. A. (2004) 'The internet and social life'. *Annual review of psychology*, 55, pp. 573-590.

Belloti, V. and Sellen, A. (1993) 'Design of privacy in ubiquitous computing environments' in de Michelis G., Simone C., and Schmidt K. (eds.). *3rd Conference on European Conference on Computer-Supported Cooperative Work*, 13 – 17 September, Milan, Italy. Norwell, MA: Kluwer Academic Publishers, pp. 77-92.

Bettman, J. R., Payne, J. W. and Staelin, R. (1986) 'Cognitive considerations in designing effective labels for presenting risk information'. *Journal of Public Policy and Marketing*, 5(1), pp. 1-28.

Bevan, N., Kirakowski, J. and Maissel, J. (1992) 'What is usability?', in: Bullinger H.J. (ed.) *International conference on HCI*, Stuttgart, September 1991. Elsevier.

Birnie, S. A. and Horvath, P. (2002) 'Psychological predictors of internet social communication'. *Journal of computer mediated communication*, 7(4).

Blandford, A., Cox, A. L. and Cairns, P. (2008) 'Controlled experiments', in Cairns, P. and Cox, A. L. (eds.) *Research methods for human-computer interactions*, 1st edn. UK: Cambridge University Press, pp. 1-16.

Bloustein, E. (1964) 'Privacy as an aspect of Human Dignity: An answer to Dean Prosser'. *New York University Law Review*, 39, pp. 962-1007.

Bonneau, J. and Preibusch, S. (2009) 'The Privacy jungle: On the market for Data Protection in Social Networks', *8th Workshop on the Economics of Information Security*. University College London, England, 24-25 June 2009.

Borg, R. (2007) 'The power of persuasion: How empathy and sincerity work wonders for you', in *Persuasion: The art of influencing people*, 2nd edn., UK: Pearson Education Limited, pp. 1-12.

Bork, R. (1990), *The Tempting of America: the political seduction of the law*. New York: Simon and Shuster.

boyd, d. (2004) 'Friendster and publicly articulated social networking', *Conference on Human Factors and Computing Systems* , Vienna, Austria , 24-29 April. New York: ACM pp. 1279-1282.

Brin, D. (1998) *The Transparent Society: Will Technology force us to choose between Privacy and Freedom?*. Reading , MA: Addison-Wesley.

Brooke, J., Bevan, N., Brigham, F., Harker, S. and Youmans, D. (1990) 'Usability statements and standardisation: Work in progress in ISO', in Diaper, D., Gilmore, D. J., Cockton, G., et al (eds.), *3rd International Conference on Human-Computer Interaction*, Cambridge, UK, August 27-31, The Netherlands: North-Holland Publishing Co. Amsterdam, pp. 357-361.

Buckley, J.(1974) 'Privacy Act of 1974', *Public Law* 93-579

Campbell, D. T. (1963) 'Social attitudes and other acquired behavioral dispositions', in Koch, S. (ed.) *Psychology: a study of a science.* New York, McGraw - Hill, pp. 94-172.

Caroll, J. M. (1997) 'Human-Computer Interaction: Psychology as a science of design'. *International Journal of Human-Computer Studies*, 46(4), pp. 501-522.

Cate, F. H. (2010) 'The limits of notice and choice'. *IEEE Security & Privacy*, 8(2), pp. 59-62.

Chandler, J. (2009) 'Privacy versus national security: clarifying the trade-off', in Kerr, I., Steeves, V. and Lucock, C. (eds.) *Lessons from the identity trail: anonymity, privacy and identity in a networked society*. New York; Oxford University Press Inc., pp. 121-138.

Chappell, D. (2006) *Introducing Windows Cardspace*. Available at: http://msdn.microsoft.com/en-us/library/aa480189.aspx (Accessed 01 August 2012).

Chaum, D. (1982) '*Blind signatures for untraceable payments*', in Advance in Cryptology: Proceedings of the CRYPTO '82, pp. 199-203.

Cialdini, R. (1998), *Influence: The Psychology of Persuasion*, Revised edn. New York: HarperCollins Publishers.

Cialdini, R. (2000), *Influence: Science and practice*, 4th edn., Boston: Pearson.

Coopamootoo, P.L. and Ashenden, D. (2011) 'Designing usable online privacy mechanisms: What can we learn from real world behaviour?', in S. Fischer-Hübner et al. (Eds.) *Privacy and Identity 2010, IFIP Advances in Information and Communication Technology*, 352, pp. 311–324.

Council of Europe (1950) *European Convention on Human Rights, Art. 8*. Europe.

Corbin, J. and Strauss, A. (2008) *Basics of Qualitative Research*, 3rd edn. Thousand Oaks, California: Sage Publications.

Cranor, L., Guguru, P. and Arjula, M. (2006) 'User interfaces for privacy agents'. *ACM Transactions on Computer-Human Interaction*, 13 (2), pp. 135-178.

Creswell, J. W. (2009a) 'Mixed Methods procedures', in *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*, 3rd edn. Thousand Oaks, California: Sage Publications, pp. 203-227.

Creswell, J. W. (2009b) 'Qualitative procedures', in *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*, 3rd edn. Thousand Oaks, California, Sage Publications, pp. 173-202.

Cross, M. (2008) *OpenID*. Available at: http://www.openid.co.uk/ (Accessed 01 August 2012).

de Souza, C. S., Leitao, C. F., Prates, R. O. and da Silva, E. J. (2006) 'The Semiotic Inspection Method', *7th Brazilian Symposium on Human Factors in Computing Systems*. Natal, RN, Brazil, 19-22 November. New York: ACM, pp. 148-157.

de Souza, C. S., Leitao, C. F., Prates, R. O., Bim, S. A. and da Silva, E. J. (2010) 'Can inspection methods generate valid new knowledge in HCI? The case of semiotic inspection'. *International Journal of Human-Computer Studies*, 68, pp. 22-40.

Derby, B. M. and Levy, A. S. (2001) 'Do food labels work? Gauging the effectiveness of food labels pre- and post- NLEA', in Bloom, P.N. and Gundlach, G.T. (Eds.) *Handbook of Marketing and Society*. Thousand Oaks, CA: Sage Publications, pp. 372-398.

Detica and Cabinet Office (2011) *The Cost of Cyber Crime*. Available at http://www.cabinetoffice.gov.uk/sites/default/files/resources/the-cost-of-cyber-crime-full-report.pdf (Accessed 31 October 2012)

Dix, A., Finlay, J., Abowd, G. D. and Beale, R. (2004) 'Interaction', in *Human-Computer interaction*, 3rd ed. Harlow, England: Pearson Education Limited, pp. 124-162.

Dourish, P. (1993) 'Culture and Control in a media space', in de Michelis G., Simone C., and Schmidt K. (eds.). *Third Conference on European Conference on Computer-Supported Cooperative Work*, 13 – 17 September, Milan, Italy. Norwell, MA, USA: Kluwer Academic Publishers, pp. 125 - 137.

Dumas, J. (2007) 'The great leap forward: The birth of the usability profession (1988-1993)'. *Journal of Usability Studies*, 2 (2), pp. 54-60.

Dunbar, R. (2010) *How many friends does one person need?: Dunbar's number and other evolutionary quirks*. London: Faber and Faber.

Eagly, A. H. and Chaiken, S. (1993) *The psychology of attitudes*, 1st edn.. Belmont, CA: Wadsworth Publishing.

Enterprise Privacy Group (2008) *Privacy by Design: An overview of Privacy Enhancing Technologies* . Available at: http://www.ico.gov.uk/upload/documents/pdb_report_html/pbd_pets_paper.pdf (Accessed on 10th July 2009)

European Parliament (1995) *Directive 95/46/EC of the European Parliament and the Council*. Available at: http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf (accessed 14 March 2012).

European Union (2003) *The Privacy and Electronic Communications (EC Directive) Regulations 2003*. Available at: http://www.legislation.gov.uk/uksi/2003/2426/contents/made (Accessed 01 Mar 2012).

Fazio, R. H. (1986) 'How do attitudes guide behavior?', in Sorrentino, R. M. and Higgins, E. T. (eds.) *Handbook of motivation and cognition: Foundations of social behavior*. New York: Guildford Press, pp. 204-243.

Fazio, R. H. (1989) 'On the power and functionality of attitudes: the role of attitude accessibility', in Pratkanis, A. R., Breckler, S. J. and Greenwald, A. G. (eds.) *Attitude structure and function*. Hillsdale, N.J.: Lawrence Erlbaum Associates, pp. 153-179.

Fazio, R. H., Sanbonmatsu, D. M., Powell, M. C. and Kardes, F. R. (1986) 'On the automatic activation of attitudes'. *Journal of personality and social psychology*, 50, pp. 229-238.

Fazio, R. H. and Williams, C. J. (1986) 'Attitude accessibility as a moderator of the attitude-perception and attitude-behavior relations: an investigation of the 1984 Presidential Election'. *Journal of personality and social psychology*, 51, pp. 504-514.

Fazio, R. H. and Zanna, M. P. (1981) 'Direct experience and attitude-behavior consistency'. *Advances in experimental social psychology*, 14, pp. 161-202.

Federal Trade Commission (2000) *Privacy Online: Fair Information Practices in the Electronic Marketplace*. Available at: http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (Accessed 01 March 2012).

Fishbein, M. and Ajzen, I. (1974) 'Attitudes towards objects as predictors of single and multiple behavior criteria'. *Psychological Review*, 81, pp. 59-74.

Fishbein, M. and Ajzen, I. (1976) *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research.* Reading, MA: Addison-Wesley.

Flesch, R. (1848) ‘A new readability yardstick’. *Journal of applied psychology*, 32 (3), pp. 221-233.

Fogg, B. J. (1998) ‘Persuasive computers: Perspectives and research directions’, in Karat, C., Lund, A., Coutaz, J. and Karat, J. (ed.), *SIGCHI conference on Human factors in Computing Systems*, 18 – 23 April. Los Angeles, California: ACM Press/ New York: Addison-Wesley Publishing Co., pp. 225 - 232.

Fogg, B. J. (2003) ‘Introduction: Persuasion in the digital age’, in *Persuasive Technology: Using Computers to Change What We Think and Do*. San Francisco: Morgan Koffman Publishers, pp. 1-13.

Fried, C. (1970) *An Anatomy of Values: Problems of personal and social choice*. Cambridge, MA: Harvard University Press.

Gerstein, R. (1978) ‘Intimacy and Privacy’. *Ethics*, 89, pp. 76-81.

Gideon, J., Cranor, L., Egelman, S. and Acquisiti, A. (2006) ’Power Strips, Prophylactics, and Privacy, Oh My!’, *2nd Symposium on Usable privacy and security*, Pittsburgh, Pennsylvania, 12 – 14 July, NY, USA: ACM New York, 14, pp. 133 - 144.

Gilani, N. (2009) *Wife blows MI6 chief’s cover on facebook*. Available at: http://www.timesonline.co.uk/tol/news/uk/article6639521.ece (Accessed 14 January 2010).

Glaser, B. G. and Strauss, A. (1967) *The discovery of grounded theory*. New York: Aldine de Gruyter.

Govani, E. and Pashley, H. (2007) ‘Student awareness of the privacy implications when using Facebook’. Available at: http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf (Unpublished manuscript accessed on 1 March 2009)

Gross, R. and Acquisiti, A. (2005) ‘Information revelation and privacy in online social networks’, *2005 ACM workshop on Privacy in the electronic society*, Alexandria, Virginia, 7 November, New York: ACM, pp. 71-80.

Gulcu, C. and Tsudik, G. (1996) ‘Mixing E-mail with Babel’, *Network and distributed security Symposium*, San Diego, CA, 22-23 February. Washington, D.C.: IEEE Computer Society, pp. 2-16.

Hertzum, M. and Jacobsen, N. E. (2001) ‘The evaluator effect: A chilling fact about Usability Evaluation Methods’. *International Journal of Human-Computer Interaction*, 15, pp. 183-204.

Higgins, E. T. (1996) ‘Knowledge activation: accessibility, applicability and salience’, in Higgins, E. T. and Kruglanski, A. W. (eds.) *Social Psychology: Handbook of Basic Principles*. New York: Guildhall Press, pp. 133-166.

IMRG and Experian Hitwise (2011) *Hot Shops List February 2011*. Available at: http://www.imrg.org/ImrgWebsite/User/Pages/Press%20Releases-

IMRG.aspx?pageID=86&parentPageID=85&isHomePage=false&isDetailData=true&itemID=4625&specificPageType=5&pageTemplate=7 (Accessed 08 March 2011).

Information Commissioner's Office UK (2009) *Privacy Impact Assessment Handbook 2.0*. Available at: http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html (accessed 11 Nov 2012).

ISO (1998) 'Part II: Guidance on usability (ISO 9241-11:1998)' in *Ergonomic requirements for office work with visual display terminals (VDTs). Available at http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=16883 (Accessed on 01 June 2009)*

Itrona, L. D. and Pouloudi, A. (1999) 'Privacy in the Information Age: Stakeholders, Interests and Values'. *Journal of Business Ethics* , 22(1), pp. 27-38.

Jensen, C. and Potts, C. (2004) 'Privacy policies as decision making tools: an evaluation of online privacy notices', *Proceedings of the SIGCHI Conference on Human factors in Computing Systems*. Vienna, Austria, 27-29 April. New York : ACM, pp. 471-478.

Jensen, C., Potts, C. and Jensen, C. (2005) 'Privacy practices of internet users: self-reports versus observed behavior'. *International Journal of Human-Computer Studies*, 63 (1-2), pp. 203-227.

Joinson, A. N. and Paine, S. (2007), 'Self-disclosure, privacy and the internet', in Joinson, A. N., McKenna, K. Y. A., Postmes, T., et al (eds.) *Oxford Handbook of Internet Psychology*. Oxford: Oxford University Press, pp. 237-252.

Joinson, A. N., Reips, U., Buchanan, T., Paine, S. and Carina, B. (2010) 'Privacy, trust and self-disclosure online'. *Human Computer Interaction*, 25(1), pp. 1-24.

Jordan, P. W. (1998) *An introduction to Usability*. London: Taylor and Francis.

Kelley, P. G., Bresee, J., Cranor, L. F. and Reeder, R. W. (2009 'A "nutrition label" for privacy', *5th Symposium on usable privacy and security*. Mount View, CA, USA, 15-17 July. NY, USA: ACM, pp. 1-12.

Kirakowski, J. and Corbett, M. (1988) 'Measuring user satisfaction', In Jones, D.M. and Winder, R. (Eds.) *People and Computers, IV*. Cambridge, England: Cambridge University Press, pp. 329-338.

Kumaraguru, P. and Cranor, L. (2005) *Privacy Indexes: A survey of Westin's Studies*. CMU-ISRI Technical Report. Available at: http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf (Accessed on 10 June 2009)

LaPiere, R. T. (1934) 'Attitudes vs. Actions'. *Social Forces*,13, pp. 230-237.

Leslie, J. C. (1996) 'Operant Conditioning', in *Principles of behavioral analysis*, Amsterdam: Harwood Academic Publishers, pp. 21-55.

Lincoln, Y. S. and Guba, E. G. (1985) *Naturalistic Inquiry*. Beverly Hills, CA: Sage Publications.

MacKinnon, C. (1989) *Toward a feminist theory of the state*. Cambridge, MA: Harvard University press.

Macleod, M., Bowden, R. and Bevan, N. (1998) 'The MUSiC Performance Measurement Method'. *Behaviour and Information Technology*, 16(4-5), pp. 279-293.

Margulis, S. T. (2003), 'On the status and collaboration of Westins's and Altman's Theories of Privacy', *Journal of Social Issues*, 59(2), pp. 411-429.

McDonald, A., Cranor, L., Reeder, R. and Gage Kelley, P. (2009) 'A Comparative study of online privacy policies and formats', *9th International Symposium on Privacy Enhancing Technologies*. August 05 - 07, 2009, Seattle, WA, I. Goldberg and M. J. Atallah (eds.), Berlin, Heidelberg: Springer-Verlag, pp. 37 - 55.

McGuire, W. J. (1985) 'Attitudes and attitude change', in Lindzey, G. and Aronson, E. (eds.) *The Handbook of Social Psychology*. New York: Random House, pp. 233-346.

Metzger, M. (2007) 'Communication Privacy Management in Electronic Commerce'. *Journal of Computer-Mediated Communication*, 12(2). Available at: http://jcmc.indiana.edu/vol12/issue2/metzger.html (Accessed 01 March 2010)

Miller, G. R. (1980), 'On being persuaded: some basic distinctions', in Roloff, M. E. and Miller, G. R. (eds.) *Persuasion: New directions in theory and research*. Beverly Hills, CA: Sage Publications, pp. 11-28.

Milne, G. R. and Culnan, M. J. (2004) 'Strategies for reducing privacy risks: why consumers read (or don't read) online privacy notices'. *Journal of interactive marketing*, 18 (3), pp. 15-29.

Miltenberger, R. G. (2011) *Behavior modification: principles and procedures*, 3rd edn. Belmont, CA: Wadsworth Publishing.

Miyazaki, A. and Krishnamurthy, S. (2002) 'Internet seals of approval: effects on online privacy policies and consumer perceptions'. *Journal of Consumer Affairs*, 36(1), pp. 28-49.

Nass, C. and Moon, Y. (2000), 'Machines and mindlessness: social responses to computers', *Journal of social issues*, 56(1), pp. 81-103.

Nass, C. I., Steuer, J. and Tauber, E. R. (1994) 'Computers are social actors', in Adelson, B., Dumais, S. and Olson J. (ed.), *Conference on Human Factors in Computing Systems: Celebrating interdependence*, Boston, Massachusetts, 24 – 28 April, New York: ACM, pp. 72-78.

Noor, K. (2008) 'Case Study: A Strategic Research Methodology'. *American Journal of Applied Sciences*, 5(11), pp. 1602-1604.

Norris, G., Hurley, J.R., Hartley, K. M., Dunleavy, J.R. and Ball, J. D. (2000) *E-Business and ERP: transforming the enterprise*. New York: John Wiley & Sons, Inc.

Oinas-Kukkonen, H. and Harjumaa, M. (2008a) 'A Systematic Framework for Designing and Evaluating Persuasive Systems', in Oinas-Kukkonen, H., Hasle, P., Harjumaa, M., Segerståhl, K., and Øhrstrøm, P., (ed.), *3rd International Conference on Persuasive Technology*, Oulu, Finland, 04 – 06 June. Heidelberg, Berlin: Springer-Verlag, 5033, pp. 164-176.

Oinas-Kukkonen, H. and Harjumaa, M. (2008b) 'Towards deeper understanding of persuasion in software and information systems', *1st International Conference on Advances in Computer-Human Interaction*, Sainte Luce, Martinique, 10-15 February, 2008. Washington, D.C.: ACHI. IEEE Computer Society, pp. 200-205.

O'Keefe, D. J. and Delia, J. D. (1981) 'Construct differentiation and the relationship of attitudes and behavioral intentions'. *Communications Monograph*, 48, pp. 146-157.

Okoli, C. and Pawlowski, S. D. (2004) 'The Delphi method as a research tool: an example, design considerations and applications'. *Information and Management*, 42(1), pp. 15-29.

Ostrow, A. (2009) *Facebook fired: 8% of US companies have sacked social media miscreants. A*vailable at: http://mashable.com/2009/08/10/social-media-misuse/ (Accessed 14 January 2010).

Palen, L. and Dourish, P. (2003) 'Unpacking" privacy for a networked world', *Proceedings of the CHI Conference on Human Factors in Computing Systems, 2003.* Ft. Lauderdale, Florida, USA, ACM, NY, USA, pp. 126-136.

Pace, S. (2004) 'A grounded theory of the flow experiences of web users'. *International Journal of Human-Computer Studies*, 60, pp. 327-363.

Patrick, A. S. and Kenny, S. (2003) 'From privacy legislation to interface design: implementing information privacy in human-computer interactions', 2003 *Privacy enhancing technologies workshop*, Dresden, Germany, 26-28 March. LNCS, 2760, pp. 107-124.

Perloff, R. M. (2010a) 'Attitudes: Definition and Structure', in Bathgate, L., Solano, N., Ghezzi, K., et al (eds.) *The dynamics of persuasion: communication and attitudes in the 21st century*, 4th edn. Maddison Avenue, New York: Routledge, pp. 40-79.

Perloff, R. M. (2010b) 'Introduction to persuasion', in Bathgate, L., Solano, N., Ghezzi, K., et al (eds.) *The dynamics of persuasive: communication and attitudes in the 21st century*, 4th edn., Maddison Avenue, New York: Routledge, pp. 3-39.

Petronio, S. (2002) *Boundaries of privacy: dialectics of disclosure*. Albany: State University of New York Press.

Petronio, S. (2010) 'Communication Privacy Management: What do we know about Family Privacy Regulation?'. *Journal of Family Theory and Review*, 2(3), pp. 175-195.

Petty, R. E. and Cacioppo, J. T. (1986) 'The elaboration likelihood model of persuasion', *Advances in experimental social psychology*, 19, pp. 123-205.

Petty, R. E. and Wegener, D. T. (1998) 'Attitude change: multiple roles for persuasion variables', in Gilbert, D. T., Fiske, S. T. and Lindzey, G. (eds.) *The Handbook of Social Psychology*, 4th edn. New York: McGraw-Hill, pp. 323-390.

Pollach, I. (2007) 'What's wrong with online privacy policies?'. *Communications of the ACM*, 50(9), New York: ACM, pp. 103-108.

Polson, P. G. (1992) 'Cognitive Walkthroughs: a method for theory-based evaluation of user interfaces'. *International journal of Man-Machine Studies*, 36(5), pp. 741-773.

Posner, R. (1981) *The Economics of Justice.* Cambridge, MA: Harvard University Press.

Preece, J. (2001) 'Sociability and usability in online communities: determining and measuring success'. *Behaviour and Information Technology*, 5(5), pp. 356.

PRIME WP06.1 (2008), *HCI Guidelines, D06.1.f*, Pettersson, J.S. Edn. Available at: https://www.prime-project.eu/prime_products/reports/arch/pub_del_D06.1.f_ec_wp06.1_v1_final.pdf. (Accessed 10 January 2010)

Rachels, R. (1975) 'Why Privacy is important?'. *Philosophy of Public Affairs*, 4, pp. 323-333.

Rapp, C. (2010) 'Aristotle's Rhetoric', in Zalta, E. N. (ed.) *The Stanford Encyclopedia of Philosophy*, Spring 2010. Available at: http://plato.stanford.edu/archives/spr2010/entries/aristotle-rhetoric (accessed on 27 November 2009).

Razavim, M. N. and Iverson, L. (2006) 'A grounded theory of information sharing behavior in a personal learning space', *Proceedings of CSCW 2006.* New York: ACM Press, pp. 459-468.

Regan, D. T. and Fazio, R. H. (1977) 'On the consistency between attitudes and behaviour: Look at the method of attitude formation'. *Journal of experiment social psychology*, 13, pp. 28-45.

Regan, P. (1995) *Legislating Privacy: Technology, Social Values and Public Policy*. North Carolina: The University of North Carolina Press.

Rengger, R. (1991) 'Indicators of usability based on performance', in Bullinger, H. J. (ed.) *Human aspects in computing: design and use of interactive systems and work with terminals*. Amsterdam: Elsevier, pp. 656-660.

Richter-Lipford, H., Besmer, A. and Watson, J. (2008) 'Understanding Privacy settings in Facebook with an audience view', in Churchill, E. and Dhamija, R. (eds.) *Proceedings of the 1st Conference on Usability, Psychology, and Security*. San Francisco, California, 14 April. Berkeley, CA: USENIX Association, pp. 1-8.

Richter-Lipford, H., Hull, G., Latulipe, C., Besmer, A. and Watson, J. (2009) 'Visible flows: contextual integrity and the design of privacy mechanisms on social network sites', *International Conference on Computational Science and Engineering*. Vancouver, Canada, 29-31 August 2009. Washington, D.C.: IEEE Computer Society, 4, pp. 985-989.

Richter-Lipford, H., Watson, J., Whitney, M., Froiland, K. and Reeder, R. W. (2010) 'Visual vs. compact: A comparison of privacy policy interfaces', *CHI 2010: Input, Security, and Privacy Policies.* Atlanta, Georgia, USA, 10-15 April, New York: ACM, pp. 1111-1114.

Rieman, J., Franzke, M. and Redmiles, D. (1995) 'Usability Evaluation with the Cognitive Walkthrough', *CHI '95 Conference Companion on Human Factors in Computing Systems*. Denver, Colorado, 7-11 May. New York: ACM, pp. 387-388.

Rosenberg, M. J. and Hovland, C. I. (1960) 'Cognitive, affective, and behavioral components of attitudes', in Hovland, C. I. and Rosenberg, M. J. (eds.) *Attitude organisation and change*. New Haven: Yale University Press, pp. 1-14.

Schoeman, F. (1984) *Philosophical Dimensions of Privacy: An Antology*. England: Cambridge University Press.

Schuman, H. and Johnson, M. P. (1976) 'Attitudes and behaviors'. *Annual review of psychology*, 2, pp. 161-207.

Shackel, B. (1991) 'Usability - Context, framework, definition, design and evaluation', in Shackel, B. and Richardson, S. J. (eds.) *Human Factors For informatics Usability*, New York: Cambridge University Press, pp. 21-37.

Sivacek, J. and Crano, W. D. (1982) 'Vested interest as a moderator of attitude-behaviour consistency'. *Journal of personality and social psychology*, 43, pp. 210-221.

Skulmoski, G. J., Hartman, F. T. and Krahn, J. (2007) 'The Delphi Method for Graduate Research'. *Journal of Information Technology Education*, 6, pp. 1-21.

Solove, D. J. (2006) 'A taxonomy of privacy'. *University of Pennsylvania Law Review*, 154(33), pp. 477-560.

Spiekermann, S., Grossklags, J. and Berendt, B. (2001) 'E-privacy in 2nd Generation E-commerce: Privacy preferences versus actual behaviour', *3rd ACM Conference on Electronic Commerce*, Tampa, Florida, USA, 14-17 October. New York: ACM, pp. 38 - 47.

Spiekermann, S. and Cranor, L. (2009) 'Engineering Privacy'. *IEEE Transactions on Software Engineering*, 38(1), pp. 67-82.

Stiff, J. B. and Mongeau, P. A. (2003) 'Examinig the attitude-behaviour relationship', in *Persuasive Communication*., 2nd edn. New York: The Guildford Press, pp. 55-77.

Strandburg, K. J. (2005) 'Privacy, Rationality, and Temptation: A Theory of Willpower Norms'. *Rutgers Law Review*, 57(4):1237.

Strater, K. and Richter, H. (2007) 'Examining privacy and disclosure in a social networking community', *3rd symposium on Usable privacy and security*. Pittsburgh, Pennsylvania, 18 - 20, July. New York: ACM, pp. 157 - 158.

Sturmey, P., Ward-Horner, J., Marroquin, M. and Doran, E. (2007) 'Operant and respondent behavior', in *Functional analysis in clinical treatment*, 1st edn. Academic Press, pp. 23-50.

Sweeney, L. (2002) ‘k-anonymity: a model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, 10(5), pp. 557-570.

Teddlie, C. and Tashakkori, A. (2003) ‘Major issues and controversies in the use of mixed methods in social and behavioural sciences’, in Tashakkori, A. and Teddlie, C. (eds.) *Handbook of mixed methods in social and behavioral research*. Thousand Oaks, California; Sage Publications, pp. 3-50.

Thomson, J. (1975) ‘The right to privacy’. *Philosophy and public affairs*, 4, pp. 295-314.

Tor Inc. (2012) *The Onion Router*. Available at: https://www.torproject.org/ (Accessed 01 August 2012).

UK Government (1998) Data Protection Act 1998, UK. Available at: http://www.legislation.gov.uk/ukpga/1998/29/contents (Accessed on 14 March 2012)

Van Blarkom, G. W., Borking, J. J. and Verhaar, P. (2003) ‘PET’, in Van Blarkom, G. W., Borking, J. J. and Olk, J. G. E. (eds.) *Handbook of privacy and privacy-enhancing technologies*. The Hague, Netherlands: College bescherming persoonsgegevens, pp. 33-53.

Van der Geest, T., Pieterson, W. and De Vries, P. (2005) ‘Informed consent to address Trust, control, and privacy concerns in user profiling’. *10th International Conference in User modeling*, Edinburgh, Scotland, 24-29 July.

Velmurugan, M. S. (2009) ‘Security and trust in e-business: problems and prospects’. *International journal of electronic business management*, 7(3), pp. 151-158.

W3C (2007) *Platform for privacy preferences*. Available at: http://www.w3.org/P3P/ (Accessed 04 August 2012).

W3Schools (2011) *Web statistics and trends*. Available at: http://www.w3schools.com/browsers/browsers_stats.asp (Accessed 10 March 2011).

Watson, J., Whitney, M. and Richter-Lipford, H. (2009) ‘Configuring audience-oriented privacy policies’,*2nd ACM Workshop on Assurable and Usable Security Configuration*. Chicago, Illinois. New York: ACM, pp. 71-78.

Warren, S. D. and Brandeis, L. (1890) ‘The right to privacy’. *Harvard Law Review*, 4, pp. 193-220.

Westin, A. (1967) *Privacy and Freedom*. New York: Athenaeum.

Westin, A., Harris, L. and Associates (1991) *Harris-Equifax consumer privacy survey*. Atlanta, GA: Equifax Inc.

Wharton, C., Rieman, J., Lewis, C. and Polson, P. (1994) ‘The cognitive walkthrough method: a practitioner's guide’, in Nielsen, J. and Mack, R. L. (eds.) *Usability inspection Methods*. New York: John Wiley & Sons, pp. 105-140.

Whitten, A. and Tygar, J.D.(1999) 'Why Johny can't encrypt: a usability evaluation of PGP 5.0', *Proceedings of the 8th USENIX Security Symposium*, Washington, D.C., 23-26 August. Berkeley, CA: USENIX Association, 8, pp.14 – 29.

Wiethoff, M., Arnold, A. G. and Houwing, E. M. (1991) 'The value of psycho physiological measures in human-computer interaction', in Bullinger, H. J. (ed.). *4th International Conference on Human Computer Interaction*, Stuttgart, September 1991, Elsevier.

Yin, R. K. (2009) *Case Study Research Design and Methods*, 4th edn. Thousand Oaks, California: Sage Publications.

VOME (2012a) *Visualisation and Other Methods of Expression*. Available at: http://www.vome.org.uk/about/ (accessed 01November 2012).

VOME (2012b) *What does online privacy mean to you?* http://www.vome.org.uk/2012/25-people-1-question-what-does-online-privacy-mean-to-you/ (accessed 01November 2012).

Publications by the author

Coopamootoo, P.L. and Ashenden, D. (2011) 'Designing usable online privacy mechanisms: What can we learn from real world behaviour?', in S. Fischer-Hübner et al. (Eds.) *Privacy and Identity 2010, IFIP Advances in Information and Communication Technology*, 352, pp. 311–324.

Coopamootoo P.L and Ashenden D. (2011) 'A systematic evaluation of the communicability of online privacy mechanisms', in A. Marcus (Ed.): *Design, User Experience, and Usability. Theory, Methods, Tools and Practice*, LNCS 6770, pp. 384-393.

Appendix A

Appendix A expands on Chapter 4 and the Study 1. It provides the questionnaire for the second round of the Delphi study as presented to participants.

Round II questionnaire

In this section, the list of identified factors that have the potential to enhance the usability of privacy online for each of the above categories is provided.

Please indicate whether you agree with the factors by pointing how important those are according to you on a scale of 0 to 7; 0 being least important and 7 being most important and you agree completely. If you have comments or additions to the provided lists, please fill in the comment section.

1. User

Factors	Explanation	Importance Level						
		1	2	3	4	5	6	7
Control	Users are autonomous individuals who require control of their activities and hence their disclosure and privacy. Enabling user control can enhance the usability of privacy online.							
Disclosure Level	Users have different disclosure levels pertaining to different relationships in different contexts. Usable privacy designs must allow for different disclosure levels.							
Minimum Effort	Users expect to be able to exercise their privacy with minimum effort. Privacy designs should require the least effort possible.							
Secondary Goal	Privacy is a secondary goal within online interactions hence not constantly and explicitly thought of. Designing privacy such that it is not obtrusive to the primary goal would help towards ensuring usability.							
Assumption	Users assume they are provided with a level of privacy; hence online designs should ensure provided privacy levels are made very explicit.							

Comments:

2. Interaction

Factors	Explanation	Importance Level						
		1	2	3	4	5	6	7
Who	Interactions designed in a way to enable users to understand who handles and has access to their disclosures would enhance the usability of privacy online.							
Consequences	Interactions designed in a way to enable users to understand the immediate consequences of disclosing would enhance the usability of privacy online.							
Risks	Interactions designed in a way to enable users to understand the future risks to them in disclosing would enhance the usability of privacy online.							
Possibilities	Interactions designed in a way to enable users to understand the possibilities available in maintaining privacy would enhance the usability of privacy online.							
Different User Groups	Interactions designed in a way to enable different groups of users to understand disclosures and privacy would enhance the usability of privacy online.							
Transparent	Clear, transparent and easy to see through disclosure/privacy interactions would enhance the usability of privacy online.							
Explicit	Clear and precisely expressed data processing practices would enhance the usability of privacy online.							
Service Provider Liability	Service providers made liable to explain data processing, consequences and future risks of disclosure clearly and in an understandable manner would enhance the usability of privacy online.							

Comments:

3. Technology

3.1 Technology Properties

Factors	Explanation	Importance Level						
		1	2	3	4	5	6	7
Ease of Use	Ease of use would enhance the usability of privacy online.							
Standard	Standardised interfaces/interactions would enhance the usability of privacy online.							
Embedded	Privacy features embedded within system/technology would enhance the usability of privacy online.							

Comments:

3.2 Technology Functions

Factors	Explanation	Importance Level						
		1	2	3	4	5	6	7
Default Privacy	Privacy defaults set to strict privacy would enhance the usability of privacy online.							
Explicit Opt-In	Explicit opt-in for disclosures would enhance the usability of privacy online.							
Feedback	Feedback of what has been disclosed, to whom and the level of privacy applied would enhance the usability of privacy online.							
Pseudonyms	Different pseudonyms for different privacy purposes (pseudonym management, different levels of anonymity) would enhance the usability of privacy online.							
Revert Back	Allowing correction or deletion of one's data would enhance the usability of privacy online.							
Minimum Data Collection	Ensuring minimum data collection would enhance the usability of privacy online.							
Expiration	Providing an expiration date for data disclosed would enhance the usability of privacy online.							

Comments:

4. Legal

Factors	Explanation	Importance Level						
		1	2	3	4	5	6	7
Legal framework	A legal framework that clearly defines liability and fit with the evolving demands of privacy online would enhance the usability of privacy online.							

Comments:

Appendix B

Appendix B expands on Chapter 4 and the Study 1. It provides the questionnaire for the third round of the Delphi study as presented to participants.

Round III questionnaire

The collected responses from Round II have been collated and analysed. We also reviewed the coding of Round I responses again with respect to the comments and importance levels of Round II. A combination of these two processes helped us to review the initial list of factors identified. We however also identified a few conflicting points regarding several factors.

While we understand that answering each of these questions might require further research, we would like to invite you to answer the below with Yes or No. If you have comments or other sub-questions please fill in the comments section.

Please consider the following questions with respect to the usability of online privacy tools/features where usability,

1. as defined from ISO 9241:Part11, is "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" and/or
2. as described by academics, is the "learnability, efficiency, memorability, error and satisfaction"

The conflicts identified are:

1. **Should privacy features/tools run in the background?**

	Questions	**Yes**	**No**
a.	Should users be protected against themselves, hence give them very little or no control by having privacy to run in the background?		
b.	Or should it offer some predefined privacy options that users can be aware of and control to some extent?		
c.	Or should privacy be obtrusive for users to think about it and act privately because else they will not?		

Comments:

2. Should privacy designs opt for minimum effort?

(The issue raised for minimum effort was that it might lead to over-simplification and hence the danger of neglecting user needs. And also if systems have high benefits, users might accept more effort.)

	Questions	**Yes**	**No**
a.	Should all privacy systems opt for minimum effort as a usability measure?		
b.	Could predefined privacy levels provide for minimum effort without too much simplification?		

Comments:

3. The control factor, to whom, what, how and potential risks, is very important but

	Questions	**Yes**	**No**
a.	Is guidance for understanding the choices users make a prerequisite to control?		
b.	Can control be un-obtrusive?		
c.	Can we provide fine-grained control plus pre-defined levels without the user being tempted to use defaults all the time?		
d.	Can we have control that does not interfere with the minimum effort factor?		

Comments:

4. **Can standard interfaces help users easily recognise and interpret privacy features**

	Questions	**Yes**	**No**
a.	Without the standard approach being a vulnerability?		
b.	That suit different types of systems, grouped into categories?		
c.	That suit expert and novice users?		

Comments:

5. **Would having the default set to maximum privacy, that is, no disclosure**

	Questions	**Yes**	**No**
a.	Enhance usability of online privacy tools?		
b.	Or cause the turning off of all privacy features to maximum disclosure?		

Comments:

Appendix C

Appendix C provides additional material for the evaluation of Facebook. It gives the survey designed for pilot Study 2.

Facebook survey

Survey applicable to Facebook users only

1. How strongly do you agree or disagree to the following statement?
   "Consumers have lost control over how personal information is collected and used by companies."

   ○ Strongly agree ○ Somewhat disagree

   ○ Somewhat agree ○ Strongly disagree

2. How strongly do you agree or disagree to the following statement?
   "Most businesses handle the personal information they collect about consumers in a proper and confidential way."

   ○ Strongly agree ○ Somewhat disagree

   ○ Somewhat agree ○ Strongly disagree

3. How strongly do you agree or disagree to the following statement?
   "Existing laws and organisational practices provide a reasonable level of protection for consumer privacy today."

   ○ Strongly agree ○ Somewhat disagree

   ○ Somewhat agree ○ Strongly disagree

4. How sure are you about who can perform each of the following activities on your Facebook profile?

	I assume only my friends	*Not sure/Don't know*	*I am sure only me*	*I am sure only my friends*	*I am sure my friends of friends*	*I am sure my networks and my friends*	*I am sure anyone*
View your profile	○	○	○	○	○	○	○
Write on your wall	○	○	○	○	○	○	○
Comment on your pictures and posted contents	○	○	○	○	○	○	○
View your albums and photos	○	○	○	○	○	○	○
View pictures others tagged of you	○	○	○	○	○	○	○

5. How would you protect who can access or add to your contents on Facebook?

6. Which of the following most closely reflect how often you have restricted who can search, view or write on your Facebook profile?

○ Never ○ More than once ○ Very often

○ Once ○ Often

Answer the questions below only if the answer to question 6 is not ‘Never’.

7. If the answer to question 6 is not‘Never’, what did you protect on your profile?

8. If the answer to question 6 is not‘Never’, how strongly are you sure or not sure of the outcome?

- ○ Strongly sure
- ○ Somewhat sure
- ○ Somewhat not sure
- ○ Strongly not sure

Appendix D

Appendix D provides additional material for the evaluation of Facebook. It adds to the cognitive walkthrough description of Study 3.

Cognitive walkthrough

Task 2: Photo-sharing through upload and tag with the aim of sharing photos with specific friends only through internet explorer browser on a desktop or laptop

Sub-goal c: Set access control

The interface display for actions c.i and c.ii is as shown in the figure below.

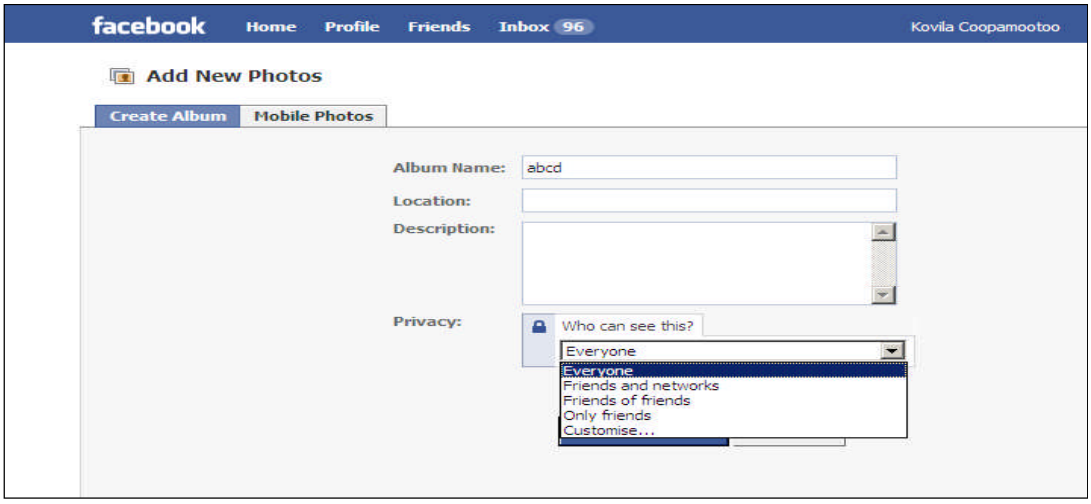


Figure 34: Click on who can see this and select Customise

Task 3: Comment to friend's post with aim of the comment being viewable only by the friend

The interface display for actions b.ii and b.iii is as shown in the figure below.

Figure 35: Type comment and click on Comment button

Appendix E

Appendix E contains the pre-test questionnaire and the post-test questionnaire for pilot user Study 6. These are followed by the procedure set to participants.

Pre-test Questionnaire

Please fill in the following questionnaire.

1. Name: _____

2. The age group you belong to is:

- ☐ 18 -25
- ☐ 26 -29
- ☐ 30 -39
- ☐ 40 - 49
- ☐ 50 +

3. Your gender is:

☐ Male ☐ Female

4. The highest level of education you completed is:

☐ None

☐ GCSE or O-Level

☐ A-Level or equivalent

☐ First degree (university or vocational)

☐ Postgraduate degree (Masters or PhD, Postgraduate Diploma or Certificate or vocational equivalent)

☐ Other – please specify: _____

5. You often use the internet for

☐ Email

☐ Online shopping

☐ Social network (e.g. Facebook, Twitter, etc)

☐ Web Development/Design

☐ Other – please specify: _____

6. For each of the following statements, how strongly do you agree or disagree?

Statements	Strongly agree	Somewhat agree	Somewhat disagree	Strongly disagree
Consumers have lost control over how personal information are collected and used by companies.				
Most businesses handle the personal information they collect about consumers in a proper and confidential way.				
Existing laws and organisational practices provide a reasonable level of protection for consumer privacy today.				

Post-test Questionnaire

SECTION 1

	Website 1									Website 2								
		1	2	3	4	5	6	7			1	2	3	4	5	6	7	
1. Website was	terrible								wonderful	terrible								wonderful
2. Website was	difficult								easy	difficult								easy
3. Website was	frustrating								satisfying	frustrating								satisfying
4. Website was	dull								stimulating	dull								stimulating
5. Reading characters on the screen	hard								easy	hard								easy
6. Highlighting simplifies task	not at all								very much	not at all								very much
7. Organisation of information	confusing								very clear	confusing								very clear
8. Use of terms through website	inconsistent								consistent	inconsistent								consistent
9. Presence of terminology related to task	never								always	never								always
10. Position of messages on screen	inconsistent								consistent	inconsistent								consistent
11. Learning to operate the website	difficult								easy	difficult								easy
12. Exploring new features by trial and error	difficult								easy	difficult								easy
13. Performing tasks is straightforward	never								always	never								always
14. Designed for all levels of users	never								always	never								always

SECTION 2

1. Who will have access to the information that you entered?

Website 1	**Website 2**

2. What personal information has the site asked for?

Website 1	**Website 2**

3. What option did you select to checkout? Why?

Website 1	**Website 2**

4. Were there any privacy options in the website?

Website 1	**Website 2**

5. How confident are you that you were able to set the level of privacy you required?

Website 1

Least Most confident

1 2 3 4 5 6 7

Website 2

Least Most confident

1 2 3 4 5 6 7

6. How easy was it to find privacy features?

Website 1

Difficult Easy

1 2 3 4 5 6 7

Website 2

Difficult Easy

1 2 3 4 5 6 7

7. What online privacy breaches are you aware of (that you or someone you know suffered, or that you heard about)?

_____

_____

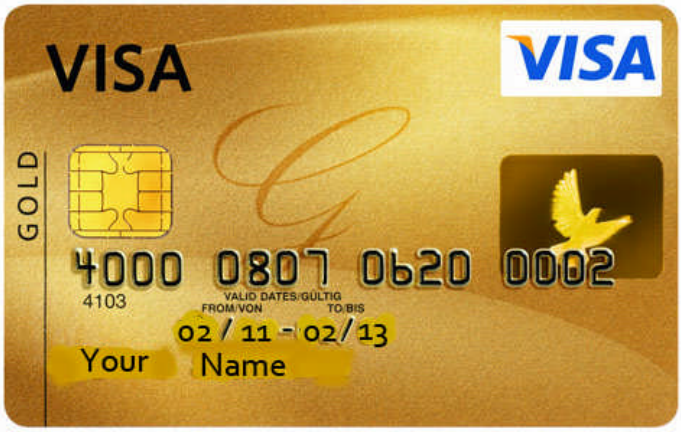
_____

Procedure

Please follow the following instructions:

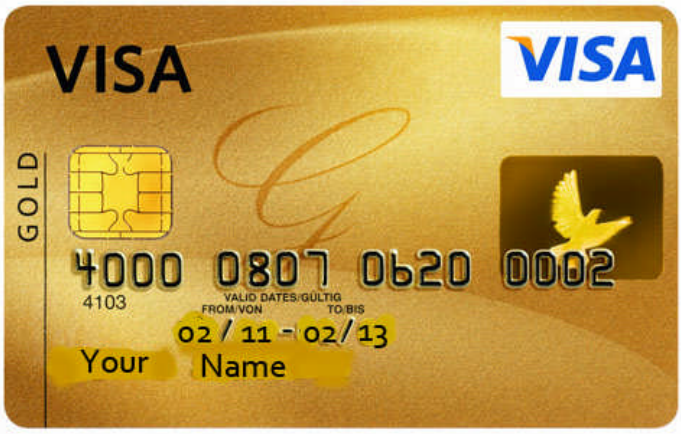
Go to site 1

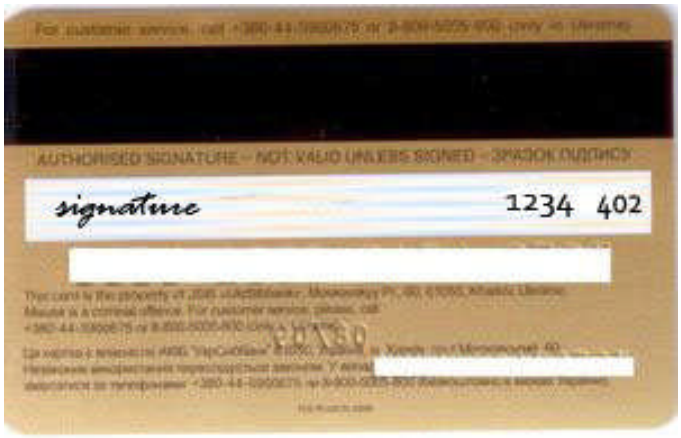
1. Go to Products
2. Select Books
3. Add “Gulliver’s Travels” to cart
4. Select “Go to Checkout”
5. Fill in the Checkout page and proceed accordingly
6. Use the credit card details below.
7.



Go to site 2

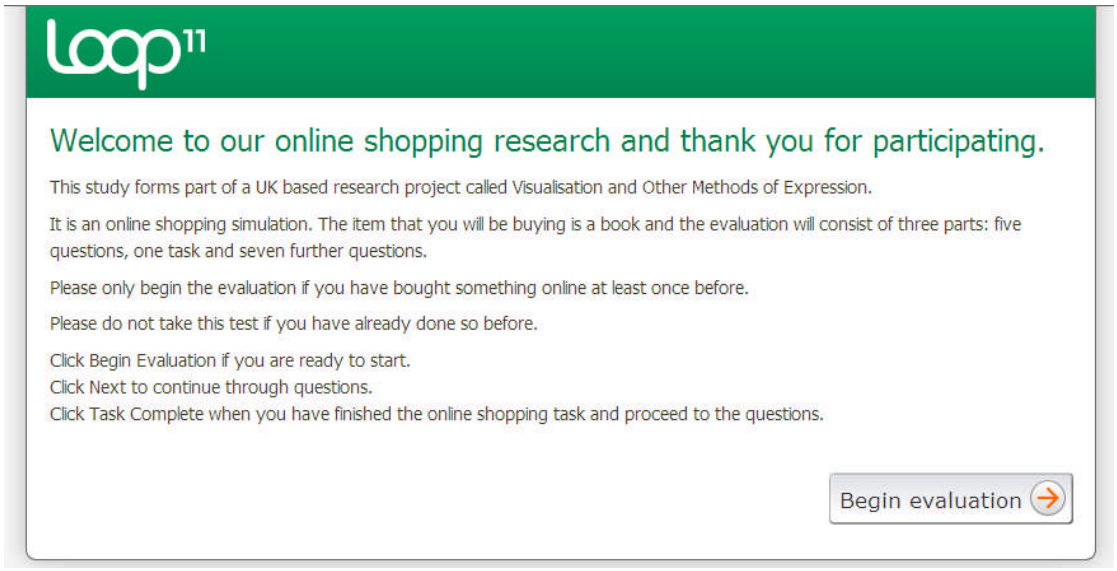
8. Go to Products
9. Select Books
10. Add “Oliver Twist” to cart
11. Select “Go to Checkout”
12. Fill in the Checkout page and proceed accordingly
13. Use the credit card details below.



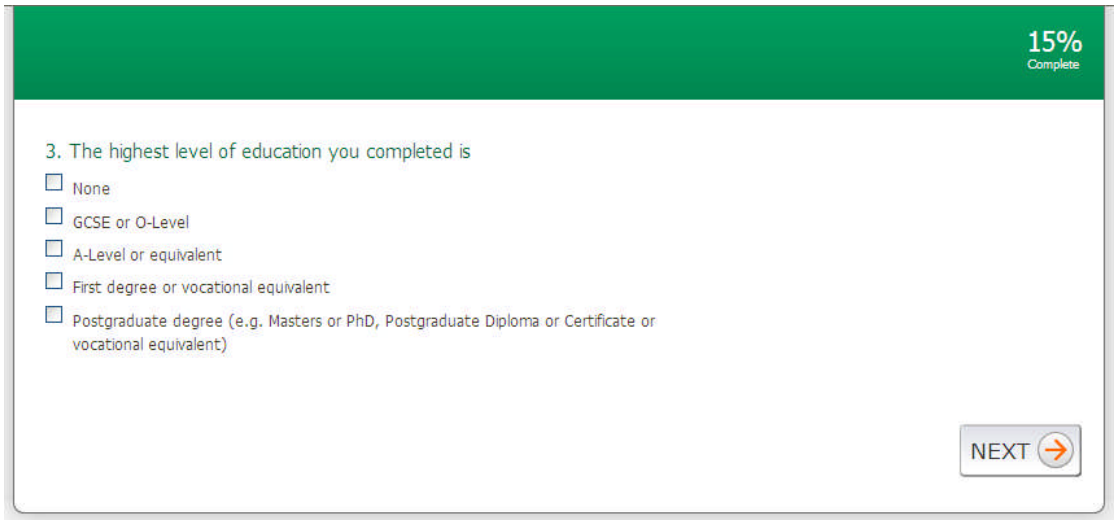


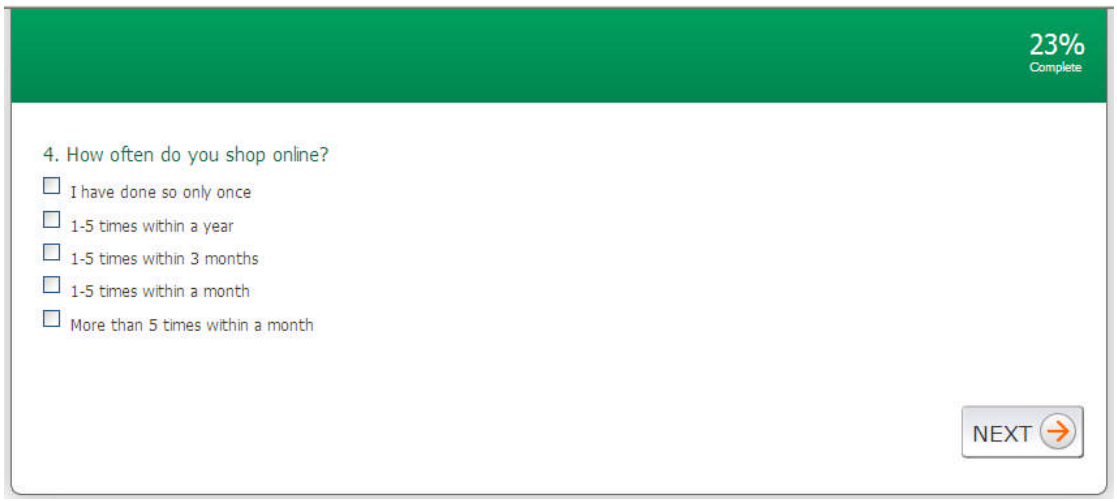
Appendix F

Appendix F provides the screenshots that shows the questionnaires and procedure for user Study 7.

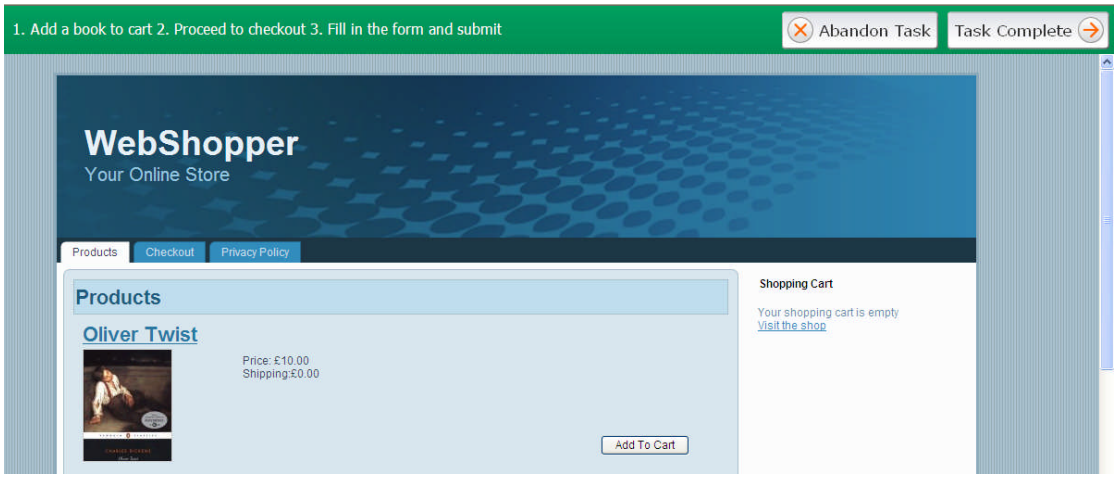



8%
Complete
2. Your gender is
Male
Female
NEXT


15%
Complete
3. The highest level of education you completed is
None
GCSE or O-Level
A-Level or equivalent
First degree or vocational equivalent
Postgraduate degree (e.g. Masters or PhD, Postgraduate Diploma or Certificate or vocational equivalent)
NEXT


23%
Complete
4. How often do you shop online?
I have done so only once
1-5 times within a year
1-5 times within 3 months
1-5 times within a month
More than 5 times within a month
NEXT


31%
Complete
5. In which country do you currently reside?
NEXT


1. Add a book to cart 2. Proceed to checkout 3. Fill in the form and submit
Abandon Task
Task Complete
WebShopper
Your Online Store
Products
Checkout
Privacy Policy
Products
Oliver Twist
Price: £10.00
Shipping:£0.00
Add To Cart
Shopping Cart
Your shopping cart is empty
Visit the shop

46%
Complete

1. For each of the following statements, how strongly do you agree or disagree?

Consumers have lost control over how personal information is collected and used by companies.

1	2	3	4
Strongly agree	Somewhat agree	Somewhat disagree	Strongly disagree

Most businesses handle the personal information they collect about consumers in a proper and confidential way.

1	2	3	4
Strongly agree	Somewhat agree	Somewhat disagree	Strongly disagree

Existing laws and organisational practices provide a reasonable level of protection for consumer privacy today.

1	2	3	4
Strongly agree	Somewhat agree	Somewhat disagree	Strongly disagree

NEXT

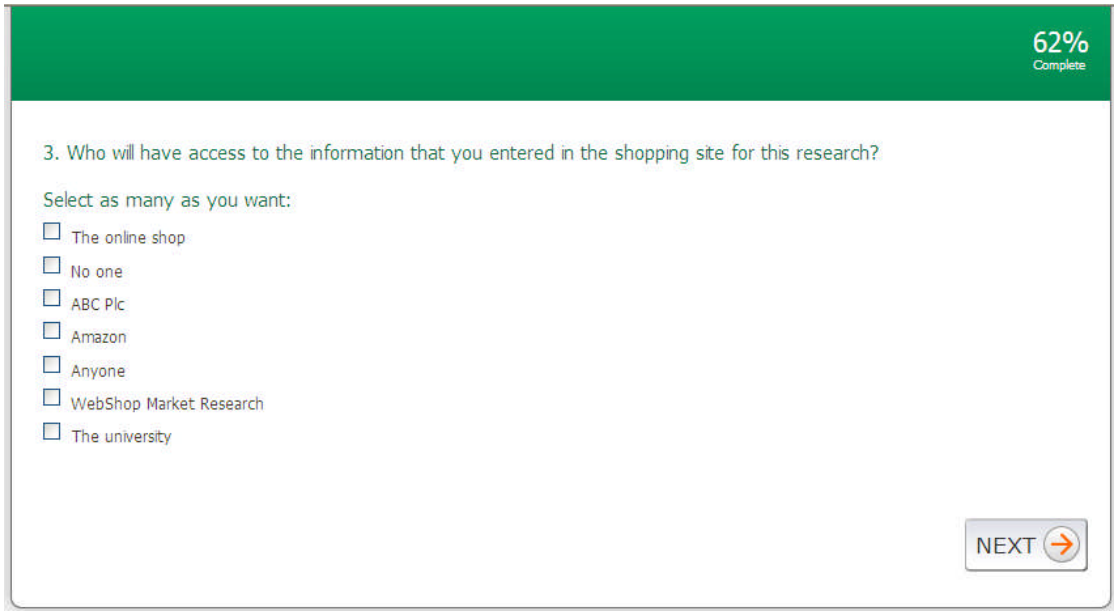
54%
Complete

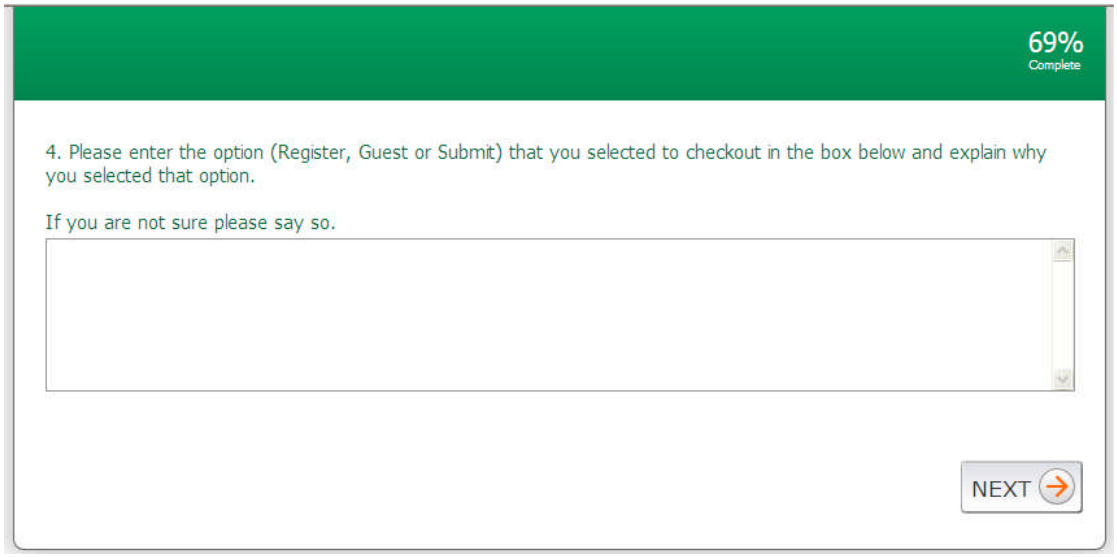
2. What private information was asked for in the shopping site of this research?

Select as many as you want:

- [ ] Profession
- [ ] Height
- [ ] Phone number
- [ ] Name
- [ ] Date of birth
- [ ] Favourite book
- [ ] Number of siblings
- [ ] Address
- [ ] Favourite movie
- [ ] Marital status
- [ ] Email address

NEXT


62%
Complete
3. Who will have access to the information that you entered in the shopping site for this research?
Select as many as you want:
The online shop
No one
ABC Plc
Amazon
Anyone
WebShop Market Research
The university
NEXT


69%
Complete
4. Please enter the option (Register, Guest or Submit) that you selected to checkout in the box below and explain why you selected that option.
If you are not sure please say so.
NEXT

77%
Complete

5. How confident are you that you were able to set the level of privacy you required (in the shopping task)?

- 1 Least confident
- 2
- 3
- 4
- 5
- 6
- 7 Most Confident

NEXT

85%
Complete

6. How easy was it to find privacy features (in the shopping task)?

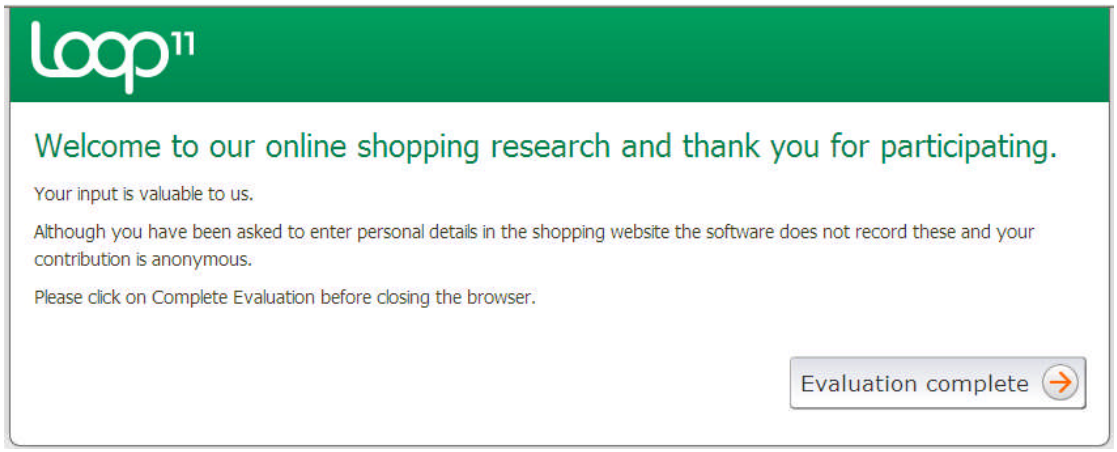
- 1 Difficult
- 2
- 3
- 4
- 5
- 6
- 7 Easy

NEXT

92%
Complete

7. Can you describe any online privacy issues that you are aware of (i.e.that you or someone you know suffered, or that you have heard about)?

NEXT


Welcome to our online shopping research and thank you for participating.
Your input is valuable to us.
Although you have been asked to enter personal details in the shopping website the software does not record these and your contribution is anonymous.
Please click on Complete Evaluation before closing the browser.
Evaluation complete

Appendix G

Testing the assumptions of the ANOVA

Normality of data

The distribution of the individual observations was roughly normal as shown in the below.

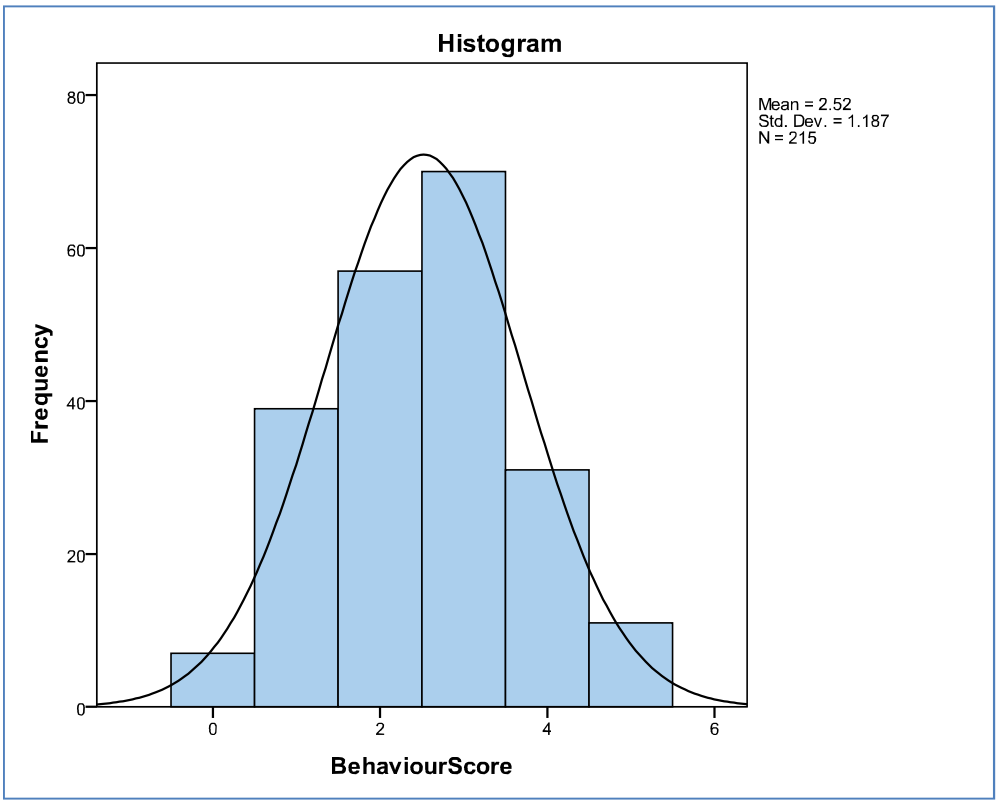


Figure 36: Histogram of behaviour score

Homogeneity of variance

For the privacy behaviour score for the different conditions, the variances were equal for conditions A, B, C and D: $F(3, 211) = .661$, $p>.01$ that is non-significant. This is

shown in the table 11 below. Homogeneity of variance was confirmed by the variances in table 41.

Table 55: Test of homogeneity of Variance

		Levene Statistic	df1	df2	Sig.
BehaviourScore	Based on Mean	.661	3	211	.577
	Based on Median	.495	3	211	.686
	Based on Median and with adjusted df	.495	3	209.949	.686
	Based on trimmed mean	.571	3	211	.635