# USER BEHAVIOUR IN PERSONAL DATA DISCLOSURE

MIGUEL MALHEIROS
UNIVERSITY COLLEGE LONDON

PHD THESIS
2013

# DECLARATION

I, Miguel Malheiros confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the thesis.

# ABSTRACT

Organisations see the collection and use of data about their customers, citizens or employees as necessary to enable value-adding activities such as personalised service or targeted advertising. At the same time, the increased efficiency and cost-effectiveness of information systems have removed most economic disincentives for widespread collection of personal data. HCI privacy research has mainly focused on identifying features of information systems or organisational practices that lead to privacy invasions and making recommendations on how to address them. This approach fails to consider that the organisations deploying these systems may have a vested interest in potentially privacy invasive features. This thesis approaches the problem from a utilitarian perspective and posits that organisational data practices construed as unfair or invasive by individuals can lead them to engage in privacy protection behaviours that have a negative impact on the organisation's data quality.

The main limitations of past privacy research include (1) overreliance on self-reported data; (2) difficulty in explaining the dissonance between privacy attitudes and privacy practice; (3) excessive focus on specific contexts and resulting lack of generalisation.

This thesis addressed these limitations by proposing a context-neutral model for personal data disclosure behaviour that identifies factors that influence individuals' perception of data requests from organisations and links those perceptions to actual disclosure decisions. This model synthesises findings from a series of interviews, questionnaires, and experiments on privacy perceptions of (1) loan application forms; (2) serious-games; (3) the UK census of 2011; and (4) targeted advertising, as well as existing research.

Results in this thesis show that individuals' decision to comply or not with data collection efforts of organisations depends largely on the same factors regardless of the context. In particular, a validation field experiment on online disclosure with 320 participants showed that perceptions of unfair data requests or expected use of the data lead to lower response rates and increased falsification of answers. Both these outcomes negatively impact organisations' data quality and ability to make informed decisions suggesting that more privacy conscious data collection procedures may lead to increased utility for both organisations and individuals.

# ACKNOWLEDGEMENTS

Completing this thesis would never have been possible without the help of several people.

I am deeply grateful to my supervisor, Prof. Angela Sasse, for her guidance and enthusiasm in driving my research to be as good as possible and for always pushing me to improve as a researcher.

I would like to thank my second supervisor, Prof. John Shawe-Taylor, my transfer viva examiner, Dr. Chris Clack, and my viva examiners, Dr. Emiliano De Cristofaro and Dr. Edgar Whitley, for their challenging questions, recommendations, and valuable insights which were crucial in shaping this thesis.

I want to express my gratitude to my research group, in particular to Dr. Sacha Brostoff and Dr. Charlene Jennett for their invaluable teachings and help and without whom I would never have been able to complete my PhD. Special thanks to Dr. Sören Preibusch for the stimulating discussions we had and for his insightful suggestions on experimental design.

I would like to acknowledge the financial support of the Fundação para a Ciência e a Tecnologia (Portuguese Foundation for Science and Technology) that made my PhD possible.

Last, but not least, I wish to thank my family, girlfriend, and friends for always making me laugh and encouraging me to do a good job.

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# Chapter 1: INTRODUCTION

The development and proliferation of computerised information systems in modern societies have increased the ability of organisations to collect, store, process and transfer large quantities of data in an efficient way. As a result, more personal data is being collected by public and commercial organisations with the stated aims of reducing costs, improving service quality, or predicting behaviour in order to manage risk.

The data that organisations store about their customers, citizens or employees is seen as a source of competitive advantage, but most organisations lack a formal assessment of the value they are realising from this data: they don't know which benefits are made possible or which costs they are incurring by having specific data. Without a detailed cost-benefit analysis of data ownership, there is risk of blindly hoarding data in a manner that can undermine, rather than further, organisational goals. In addition to the direct costs associated with maintaining data, such as storage, cleaning, and migration, there could be costs associated with negative perception of an organisation's data practices. Individuals value their personal data, and even though they may be willing to disclose it in exchange for benefits, they may perceive the collection and use of specific personal data items as invasive, and react adversely.

When individuals are faced with a request for personal data, they assess the costs and benefits of complying with the request. If the perceived benefits outweigh the perceived costs, they will disclose the data (Adams & Sasse, 2001). If individuals choose to disclose personal data and later perceive that an invasion of privacy took place (e.g.: data being used for a purpose different than for what it was collected), their trust in the organisation responsible will decrease and the next time they deal with a similar data request they will perceive it more negatively, potentially rejecting it (Adams & Sasse, 2001). If, on the other hand, the perceived costs are too high, then individuals will avoid disclosing data, such as when too many data items are requested (Hui et al., 2007), questions are difficult to answer, or seem unnecessary. Responses used to cope with requests perceived as too costly compared to the benefits include withholding (Metzger, 2007) and falsifying data (Horne et al., 2007).

An individual rejecting a service represents a lost opportunity for the organisation providing that service, as well as a potential reputation cost. The withholding and falsification of data can affect the quality of data held by the organisation, leading to incorrect assessments of individuals and sub-optimal or wrong business or public policy decisions (Horne et al., 2007). If an organisation's information systems have low-quality data as input (and have no way to detect this), they will get low-quality results – "garbage in, garbage out".

To date, it has been assumed that the more personal data an organisation collects the better. However, excessive data collection can not only have the immediate effect of alienating the individuals whose data is being requested, but also potentially cause the degradation of an organisation's data quality. If a more balanced and transparent data relationship is achieved between data subjects and data receivers (or data controllers), where targeted high value data collection is privileged over large indiscriminate data collection, individuals will react more positively to personal data requests while organisations will be able to obtain higher quality data, adding more value to their internal business processes.

## 1.1 Research Problem

Privacy research in computer science has mainly been undertaken in the fields of human-computer interaction (HCI) and information security with the aim of developing mechanisms that allow individuals to have better awareness and control over the flow of their personal data. HCI research has focused on understanding users' perceptions of privacy when interacting with information systems and finding new ways to provide them with feedback on the personal data practices of these systems and the organisations that own them. Information security research has focused on enabling users to protect their personal data through techniques such as encryption, access control, or anonymisation.

Regardless of the merits of supporting transparency and control for users, privacy research in computer science has not positioned organisational data practices in a value-oriented space. Organisations collect users' personal data to leverage their operations and - until proven that invasive practices are counter-productive to their goals - they will continue to do so. Thus, the research presented in this thesis interprets the data practices of organisations not as attacks against individual privacy, but as value-driven actions that should include negative reactions of individuals in their own cost-benefit assessments.

Some privacy research from the fields of marketing and behavioural economics has taken this approach. That research agrees that individuals make trade-offs when it comes to their personal data. If they perceive that the benefits of a service or product that requires their personal data to be higher than the costs then they will volunteer their data (Milne & Gordon, 1993; Adams & Sasse, 2001; Dinev & Hart, 2006; Grossklags & Acquisti, 2007). Past research in this field has tried to pinpoint what benefits must be offered for individuals to disclose different items of personal data (Hann et al. 2002a; 2002b; Hui et al. 2007; Cvrcek et al., 2006; Kourti, 2009) and, like in the field of HCI, has looked at how individuals' perceptions of data requests are formed (e.g.: Culnan, 1993) and how they affect willingness to disclose personal data (Dinev & Hart, 2006) and actual disclosure (Metzger, 2007; Horne, 2007).

This thesis is positioned in this space and is focused on mapping out the factors that individuals consider when an organisation asks to collect their personal data – e.g. perceived fairness of the data request – and investigating the relationship between these factors and truthful disclosure or privacy protection behaviours. Privacy protection behaviours like falsifying or omitting answers to data decrease the quality of the data provided and impair the data receiver's ability to generate value from that data. This research, tries to link data collection practices to its respective data quality impact by means of understanding how individuals react to them.

Past privacy research has mainly focussed on specific contexts, such as marketing and e-commerce, and has rarely tried to generalise their findings due to the extremely contextual nature of privacy. While this thesis acknowledges this, an attempt is made here to determine whether the factors that users consider when asked to disclose their personal data are the same in different contexts. The result is a proposed context-neutral model for individual disclosure behaviour.

## 1.2 Scope of Thesis

The focus of the research described here is to understand how individuals perceive organisational requests for their personal data and how those perceptions affect their willingness to comply with those requests. It is positioned close to the field of privacy calculus (see, for example, Dinev & Hart, 2006) in that it acknowledges that individuals may wish to pay a privacy cost so that they may realise some other benefit – e.g. in the form of a service such as a loan – and attempts to determine what leads individuals to accept (or refuse) to pay that price. It differs from other research in the field in that it focuses less on determining the costs and benefits of disclosure and instead tries to understand why a specific transaction is perceived as costly or beneficial and how that affects the individual's final decision.

Therefore, a quantification of the value of privacy (such as in Hann et al., 2002a; Cvrcek et al., 2006; or Preibusch et al., 2013) is outside the scope of this thesis. This research makes no attempt to link the identified perception factors to quantified costs and benefits. While it is assumed that individuals consider all these factors when determining the utility of complying with the data request, value assessments are treated as a black box from which a decision emerges. Thus, the methodological issue of eliciting value considerations from participants is avoided. The approach taken here is similar to that of Holbrook's (1999) when mapping the dimensions of consumer value – i.e. the features that consumers consider when assessing products and services – in a qualitative way.

Different types of contexts of interaction (individual-organisation interactions) were covered in this research. First, interactions where a customer interacts with a service provider and is asked to explicitly disclose personal data so that the transaction is complete. Interactions like these are investigated in the Applying for Credit (Chapter 3) and Advertising studies (Chapter 4). In former, there is a clearer trade-off between the costs of disclosure and the benefit obtained. In the latter, the potential for profiling and cross-site advertising make the costs less clear. In the second type of interactions studied, citizens are asked by their government to disclose personal data to facilitate the administration of public affairs as in the case of the UK Census (Chapter 6). In this situation the immediate benefits for the citizen may not be clear and, instead, there is only a promise of future social benefits. The costs of not complying with the data request, however, are obvious - e.g. £1000 fine for not completing the UK census. Finally, the monitoring of employees by their employers is investigated in the Serious Games studies (Chapter 5). In this scenario, an employee is required or asked to interact with an information system of her/his employer to fulfil some organisational purpose. There may be immediate and tangible benefits for the employee resulting from agreeing to this type of monitoring, such as constructive feedback. However, withdrawing their consent to be monitored may not be a viable option since the employee may feel coerced by the employer. Outside the scope of this thesis are, notably, interactions with a health provider requiring the disclosure of personal data in order to obtain healthcare. Healthcare privacy is a topic which has been extensively studied in the literature.

The focus of this thesis was on individuals' perceptions of explicit collection of their personal data, such as in cases where individuals are asked to disclose their data by filling in an application or registration forms and can meaningfully reject to disclose their data (Chapter 3, Chapter 6, and Chapter 9). On the other hand, it was also investigated how individuals perceived interactions where an information system tracks their behaviour where data collection is implicit (Chapter 5) and can be passed in an obscure way from one context to another (Chapter 4).

While regulatory bodies have precise definitions for what constitutes personal data (see Section 2.2.3), no distinction is made in this thesis between items relating to an individual, but that are not officially considered personal, and those that are. For the purpose of the research described here any data item that an individual perceives as personal is personal data. Moreover, the focus of this thesis is on the factors that affect individuals' perceptions of requests for personal data items and not on the data items themselves.

## 1.3 Contributions

This thesis makes several theoretical and empirical contributions to the understanding of individuals' perceptions and behaviour regarding organisational personal data practices in general and requests for personal data in particular.

### 1.3.1 Theoretical Contribution

#### 1.3.1.1 A context-neutral model for individual disclosure behaviour

This model identifies the factors that influence how individuals perceive data requests from organisations, and how those perceptions can affect their response to the requests (see Figure 1.1). Individuals asked to disclose their personal data evaluate the request according to these factors, and depending on this evaluation decide whether to comply with the request, falsify, or omit their answer.

The model is based on the findings from the studies conducted in this thesis, which looked at different types of relationships between individuals and organisations where personal data is collected, and on existing privacy research. It builds on existing privacy research by including non-privacy factors that have an influence on disclosure behaviour, such as effort of answering. The model is context-neutral because the same factors emerged in studies focusing on different situations where organisations ask individuals for their data. As a result, this thesis proposes that an individual will react differently to data collection practices happening in different contexts, but will consider the same group of factors.

The model is relevant for any organisation that collects and uses personal data. It can be used to understand the potential impact of data collection efforts on the data subjects and how their potential responses can affect the organisation's data quality. The data collection effort can then be adjusted to minimise negative responses and maximise the value of the data for the organisation.

The model is relevant for researchers as it can be used as a base for future studies. New research can focus on augmenting the model with additional factors, validating the impact of these factors in new contexts of interaction, or bounding the impact of the factors on the actual response for specific individual-organisation relationships.

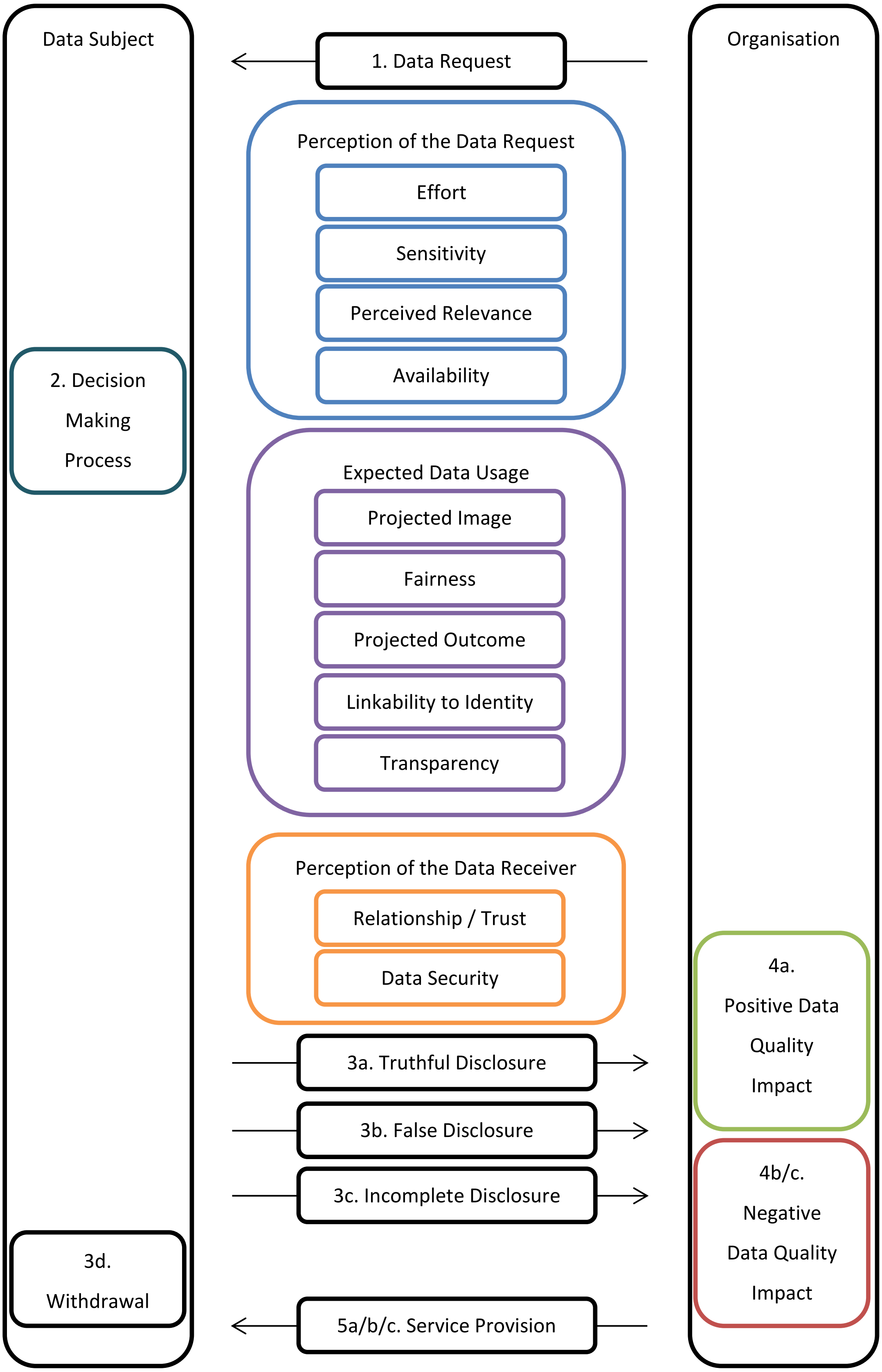


**Figure 1.1: A context-neutral model for individual disclosure behaviour**

### *1.3.2 Methodological Contribution*

#### 1.3.2.1 Estimating likelihood of privacy protection behaviours

This thesis addresses methodological limitations in past research by observing actual disclosure behaviour of individuals under deception in the field. Factors related to the perception of personal data requests are linked to actual disclosure decisions, including the decision to omit or falsify data. It is shown that, by regressing answer and falsification rates of questions on self-reported perception factors, such as question fairness or sensitivity, it is possible to approximate how data quality degrades or improves when perception of the question varies. This method can be used by organisations to determine whether it is valuable or counter-productive for them to collect specific data items. It can be repeated for specific organisational contexts and extended with additional factors.

### *1.3.3 Empirical Contributions*

#### 1.3.3.1 Research findings on loan applicants' perceptions of personal data collection and use by lenders

The findings identify issues with the lack of transparency of the risk assessment process and the collection, use and sharing of certain data items by lenders. These findings have implications for industry regulators who have an interest in minimising feelings of privacy invasions and discomfort of financial services customers. They also are of interest to lenders who can use these findings to improve customer relations and potentially create new products, which address the concerns identified.

#### 1.3.3.2 Research findings on potential privacy issues of serious-games system deployed in organisational contexts

The author's findings suggest privacy issues may arise when deploying serious-games based competence development systems in organisational settings with employees having several concerns regarding the collection and use of game-generated data. Findings are relevant for game designers as they suggest mechanisms that can be employed to minimise privacy risks. They are also useful for large organisations that use technology-enhanced competence development systems since several practices that were considered unacceptable by prospective user are identified.

#### 1.3.3.3 Research findings on citizens' perceptions of government data collection and use

The findings can help government organisations understand how their data practices are perceived and how they impact individuals. They can be used to maximise response rates and data quality as well as improve communications with citizens who do not feel their needs are addressed by government organisations.

#### 1.3.3.4 Research findings on individuals' perceptions of rich-media personalised advertising

These findings identify potential privacy issues with personalised ads. Results are relevant for advertising professionals as they suggest that the gains in attention provided by increased personalisation can be offset by users feeling uncomfortable with their data being used for advertisement purposes. Findings can also support future research into how to design ads that are both acceptable are noticeable.

## 1.4 Publications Relating to this Thesis

**Paper Title:** Malheiros, M., Preibusch, S. & Sasse, M.A. (2013) "Fairly Truthful": The Impact of Perceived Effort, Fairness, Relevance, and Sensitivity on Personal Data Disclosure. In M. Huth et al., eds. *Trust and Trustworthy Computing*. Lecture Notes in Computer Science. Springer Berlin Heidelberg, pp. 250–266.

**Author's Contribution:** This paper presents a study conducted in collaboration with Dr. Sören Preibusch from Microsoft Research Cambridge. The study attempted to both validate part of the disclosure model presented in this thesis and answer some of Dr. Preibusch's research questions. Each researcher designed the part of the study that addressed his research goal. Only the author's part is reported in this thesis. Data was collected by Dr. Preibusch and analysed by the author. The paper was written by the author, Dr. Preibusch, and Prof. Sasse.

**Relation to Thesis:** Chapter 9

**Paper Title:** Malheiros, M., Brostoff, S., Jennett, C. & Sasse, M.A. (2012). Would You Sell Your Mother's Data? Personal Data Disclosure in a Simulated Credit Card Application. 11th Annual Workshop on the Economic of Information Security (WEIS 2012), Berlin, Germany, June 25-26, 2012

**Author's Contribution:** This paper presents a study designed by Dr. Sacha Brostoff, Dr. Charlene Jennett, and the author. The author designed the website used in the experimental setup. The experiment was conducted by undergraduate UCL Psychology students Madalina

Vasilache, Diana Franculescu and Jessica Colson. All results were analysed by the author. The paper was written by the author, Dr. Brostoff, Dr. Jennett, and Prof. Sasse

**Relation to Thesis:** Chapter 4, Section 4.7

**Paper Title:** Malheiros, M., Jennett, C., Patel, S., Brostoff, S., Sasse, M. A. (2012). Too close for comfort: A study of the effectiveness and acceptability of rich-media personalized advertising. Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems. ( pp.579-588). New York, NY, USA: ACM

**Author's Contribution:** This paper presents a study designed by the author and UCL MSc student Snehalee Patel. Data was collected by Snehalee Patel. Eye-tracking data was analysed by Dr. Charlene Jennett. Thematic analysis of interview transcripts was done by the author. The paper was written by the author, Dr. Jennett, Dr. Brostoff, and Prof. Sasse.

**Relation to Thesis:** Chapter 7, Section 7.2

**Paper Title:** Malheiros, M., Jennett, C., Seager, W. & Sasse, M.A. (2011) Trusting to Learn: Trust and Privacy Issues in Serious Games. In J. M. McCune et al., eds. *Trust and Trustworthy Computing*. Lecture Notes in Computer Science. Springer Berlin Heidelberg, pp. 116-130

**Author's Contribution:** This paper presents two studies. The first was designed and carried out by Dr. Seager and author. The author did the data analysis. The second was designed and carried out by Dr. Jennett and the author. Dr. Jennett analysed the data related to trust perceptions and the author analysed the data related to privacy perceptions. The paper was written by the author, Dr. Jennett, and Prof. Sasse.

**Relation to Thesis:** Chapter 5, Sections 5.3 and 5.4

**Paper Title:** Jennett, C., Brostoff, S., Malheiros, M., Sasse, M. A. (2012). Adding insult to injury: Consumer experiences of being denied credit. International Journal of Consumer Studies 36(5), 549-555

**Author's Contribution:** The study presented in this paper was planned by Dr. Sacha Brostoff, Dr. Charlene Jennett, and the author. The author implemented the corresponding online questionnaire. Data analysis was done by the three researchers. Results were re-framed or re-analysed by the author for the purpose of this thesis. Qualitative answers were re-coded by the author in light of the research goals of this thesis. The paper was written by Dr. Jennett, Dr. Brostoff, the author, and Prof. Sasse.

**Relation to Thesis:** Chapter 4, Section 4.6

**Paper Title:** Jennett, C., Malheiros, M., Brostoff, S. & Sasse, M. A. (2012). Privacy for loan applicants versus predictive power: Is it possible to bridge the gap? In S. Gutwirth et al. (Eds.) *European Data Protection: In Good Health?* pp. 35-52. Springer Press.

**Author's Contribution:** The studies that are described were planned by Dr. Sacha Brostoff, Dr. Charlene Jennett, and the author. The author implemented the corresponding online questionnaire. Data analysis was done by the three researchers. Results were re-framed or re-analysed by the author for the purpose of this thesis. The paper was written by Dr. Jennett, the author, Dr. Brostoff, and Prof. Sasse.

**Relation to Thesis:** Chapter 4, Sections 4.4 and 4.6

**Paper Title:** Jennett, C., Brostoff, S., Malheiros, M., Sasse, M. A. (2010). Investigating loan applicants' perceptions of alternative data items and the effect of incentives on disclosure. *Privacy and Usability Methods Pow-wow (PUMP) 2010: Proceedings*. British Computer Society.

**Author's Contribution:** This paper describes the planning of two studies presented in this thesis. Planning of the studies and writing of this paper was carried out by Dr. Jennett, Dr. Brostoff, the author, and Prof. Sasse.

**Relation to Thesis:** Chapter 4, Section 4.5 and 4.7

## 1.5 Overview of Studies in this Thesis

Table 1.1 provides an overview of all the studies carried out in this thesis.

|  | Applying for Credit |  |  |  |  | Serious Games |  |  | UK Census 2011 |  | Advertising | Validation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
|  | Study 1 | Study 2 | Study 3 | Study 4 | Study 5 | Study 1 | Study 2 | Study 3 | Study 1 | Study 2 | Study 1 | Study 1 |
| **Section** | 4.3 | 4.4 | 4.5 | 4.6 | 4.7 | 5.2 | 5.3 | 5.4 | 6.2 | 6.3 | 7.2 | Chapter 9 |
| **Topic** | Personal data in risk assessment | Loan applications data requests | Loan applications alternative data requests | Collection and use of personal data by lenders | Loan applications alternative data requests and disclosure behaviour | Privacy risks in a serious-games platform | Collection and use of data by a serious-games platform | Collection and use of data by a serious-games platform | Census data requests | Census data requests and privacy protection behaviours | Rich-media personalised advertising | Impact of perceived effort, fairness, relevance, and sensitivity on personal data disclosure |
| **Method** | Semi-structured expert interviews | Online survey | Online survey | Online survey | Lab experiment | Group interview (Developer workshop) | Focus Groups | Semi-structured interviews | Semi-structured interviews | Online survey | Lab experiment | Field experiment |
| **N** | 10 | 283 | 285 | 298 | 48 | N/A | 8 | 32 | 11 | 174 | 30 | 279 |
| **Date** | Jun 2009 – Aug2010 | Aug – Sept 2010 | Aug – Sept 2010 | Aug – Sept 2010 | Mar 2011 | Oct 2009 | Feb 2010 | Jun – Nov 2010 | Mar - Apr 2011 | Apr - May 2011 | Jul – Sept 2011 | Sept 2012 – Apr 2013 |

**Table 1.1: Overview of studies conducted for this thesis**

# Chapter 2: Literature Review

This chapter reviews the literature on privacy and disclosure of personal data relevant for this thesis. It starts with a discussion of the different factors that have been linked to privacy perceptions and decision-making; why privacy behaviour sometimes appears to be inconsistent with privacy attitudes; how individuals make trade-offs with their personal data; and how they sometimes engage in privacy protection behaviours.

Second, an historical account of the evolution of the concept of privacy is given, from its first appearance in the discussion of the differences between private and public life to the more modern conceptualisations of privacy as intimacy. This is followed by a summary of the ways different fields of science approach the study of privacy and a breakdown of the different types of privacy and privacy invasions. The key concepts of data, information, and personal data are then clarified.

Third, the study of privacy in computer science is discussed. In particular, privacy sensitive design of information systems is discussed focusing on findings in the human-computer interaction and the security fields. The concepts of data mining and data quality, both highly relevant for the debate on the value of data, are presented.

Finally, the issues with the regulatory approach to solving privacy invasions are discussed. One such issue being the focus of privacy legislation in clear-cut definitions of what is and is not private, and another being the difficulty in identifying privacy invasions when so much personal data collection, use, and transfers goes undetected.

## 2.1 Disclosure Behaviour

To provide a service, most organisations require customers to either voluntarily disclose items of personal data or accept their collection by other (usually automated) means. Customers assess the social and economic benefits of complying with the data practice and weigh it against the privacy cost of the disclosure. If they perceive the benefits of this exchange are bigger than its costs than they will go ahead with it; if not, then they will refuse it. This assessment is called *"privacy calculus"* (Laufer and Wolfe, 1977; Milne and Gordon, 1993; Culnan, 1993; Culnan and Armstrong, 1999; Dinev and Hart, 2006) – also privacy decision-making or privacy behaviour.

Research on the *privacy calculus* has attempted to determine (1) how individuals assess the costs and benefits of disclosure and how it affects their willingness to disclose personal data, and (2) for which types (and amount) of benefits individuals are willing to disclose their personal data.

### 2.1.1 *Factors Linked to Privacy Attitudes and Behaviour*

In this section, factors that have been linked to privacy attitudes and behaviour are discussed, both the ones that have been mentioned in privacy calculus literature, as well as the ones identified in HCI research.

#### 2.1.1.1 Sensitivity

Individuals evaluate the sensitivity of the information they're broadcasting according to a "*scale of sensitivity*" and not in a binary - sensitive vs. non-sensitive – way (Adams, 2001). The sensitivity depends on how "*personally defining*" the information is deemed to be and how the user predicts others will interpret the information. Thus, different types of personal data have varying degrees of sensitivity, which means individuals are more comfortable disclosing some items of personal data than others (Tolchinsky et al., 1981; Woodman et al., 1982; Ackerman et al., 1999). Items that are typically seen as more sensitive include: personal identifiers such as social security number (Metzger, 2007), financial data (Phelps et al., 2000), and medical data (Ackerman et al., 1999). The same data item can also be seen as more or less sensitive depending on the context where it is observed. For example, data items that are transferred outside their context of collection may become more sensitive because they lose contextual cues, increasing the chances that they are misinterpreted (Adams and Sasse, 2001; Nissenbaum, 2004). Organisational practices involving more sensitive items of personal data have been associated with feelings of discomfort (Ackerman et al., 1999) and privacy invasion (Tolchinsky et al., 1981; Woodman et al., 1982). Perceived sensitivity of a data item has been linked with behavioural intention (Malhotra et al., 2004) and disclosure behaviour: in a study where participants were asked to fill in an online form in exchange for a free CD, Metzger (2007) observed that disclosure and falsification rates of a data item were positively and significantly correlated with the self-reported sensitivity of that item.

#### 2.1.1.2 Relevance

A request for a personal data item is perceived, by the data subject, as relevant or irrelevant depending on the context in which it happens. A doctor asking a patient for the history of cancer in her family is seen as a relevant request; the same request coming from a store clerk in the context of a loyalty card application would be seen as irrelevant - as well as unacceptable. Relevance judgements are based on what individuals perceive to be the legitimate data needs of the organisation asking for the data (Hine and Eve, 1998). Thus, what the organisation collecting the data presumes to be relevant and the individual's perception may differ. If the individual does not perceive a data item to be necessary for the communicated purpose of the current transaction it will see it as irrelevant. Data practices involving items of personal data perceived as irrelevant are considered less acceptable (Woodman et al., 1982), more invasive (Culnan, 1993), and as having a higher associated privacy cost (Annacker et al., 2001). However, perceived relevance of a data request has never been linked to disclosure behaviour.

#### 2.1.1.3 Fairness

The concept of fairness, in the procedural sense of Fair Information Practice Principles (FIPs; see US Secretary's Advisory Committee, 1973), has been linked to disclosure attitudes (Culnan and Armstrong, 1999). In a re-analysis of responses to the 1994 Harris Survey on Interactive Services, Consumers and Privacy, Culnan and Armstrong observed that, when respondents were explicitly told that fair procedures would be employed in the management of their data, their level of privacy concern did not affect willingness to be profiled for advertising purposes. Unfortunately, the study did not investigate whether the promise of fair procedures increased willingness to be profiled.

Research on the interplay between fairness perceptions and privacy behaviour should look beyond legally rooted interpretations of fairness to individual perceptions of fairness. Individuals' definitions of what constitutes fair uses of their personal data may not necessarily match the principles set out in data protection law. For this reason, procedurally fair data uses may still be interpreted as invasive (Raab and Bennett, 1998). Milne and Gordon (1993) propose interpreting exchanges of personal data for services as social contracts. The contracts are "social" in the sense that they are regulated, not only by legal norms, but also by implicit norms derived from what is socially acceptable and the expectations of the individual disclosing the data.

Milne and Gordon's framing of personal data exchanges was done in the context of direct mail marketing, which had unclear regulation from the perspective of the consumer. Nowadays, most interactions requiring customers' personal data are governed by legal statements such as terms of service or privacy policies that are binding on the organisations collecting the data. Still, these are often too long (McDonald and Cranor, 2008) or difficult to understand (Milne and Culnan, 2004) for the average customer. In that sense, one can say that, from the point of view of the data subjects, these interactions continue to be interpreted as social contracts – i.e. individuals' expectations of what can be done with their personal data depend on what they consider socially acceptable or fair. Therefore, a more complete definition of fairness in the processing of personal data can be: the fulfilment of the social contract. Unfair data practices are thus those that violate the social contract – i.e. the expectations of the individual - even if they do not violate the legal one.

### 2.1.1.4 Data Receiver

Attitudes towards personal data practices vary with the receiver of the data (Stone et al., 1983). Usually, individuals are more comfortable disclosing personal data to organisations or individuals that they trust and with whom they have an existing relationship (Ackerman et al., 1999) such as an employer (Tolchinsky et al., 1981; Woodman et al., 1982). However, in some cases, such as when data portrays the individual in a bad light, sharing with a close recipient can be perceived as more damaging than sharing with a stranger (Adams, 2001). In 2007, Kevin Colvin, an intern at Anglo Irish Bank, told his boss he had to miss work due to a "family emergency" (Williams, 2007). Kevin later shared a photo of himself at a party dressed as a fairy, on Facebook. His boss saw the picture and shared it in with the whole office in an email reply to Kevin. The photo would have been harmless if seen by strangers to Kevin, but because his employer saw it it became extremely sensitive.

While trust may increase disclosure, disclosure of personal data can also help build up trust between individuals (Joinson & Paine, 2007). Disclosure makes one vulnerable to the data receiver and accepting this vulnerability is a trusting action (Riegelsberger, 2007). Disclosure and trust thus have a mutually reinforcing relation that is at the basis of the *intimacy* definitions of privacy (Inness, 1992; Fried, 1967): friendship and love relationships are developed by successive surrenders of privacy. Adams (2001) points out that excessive focus on trust as a factor of privacy perceptions may hide the fact that trusted systems and trusted data receivers may still invade individuals' privacy without their knowledge; thus, the fact that the individual trusts the receiver does not prevent *per se* unacceptable uses of their personal data.

### 2.1.1.5 Data Usage

Individuals' attitudes towards disclosure of personal data depend on the communicated purpose of the data collection and how they think their data is going to be *used* (Ackerman et al., 1999; Phelps et al., 2000; Adams & Sasse, 2001). Some uses of personal data are seen as more acceptable than others. If individuals think that the data being disclosed in the current interaction "*will be used to draw reliable and valid inferences about them*" then they will consider it less privacy invasive (Culnan, 1993). Data being disclosed in one context that is then passed on to a third-party or used for a different purpose than the one originally communicated is usually seen as a privacy risk (secondary data use). Organisations that assume that personal data disclosed for the purposes of providing a service can be used for direct marketing, for example, are ignoring that sensitivity of data varies when usage contexts change (Adams & Sasse, 2001).

Individuals will also assess whether a disclosure might result in harmful consequences for them (Tolchinsky et al., 1981; Phelps et al., 2000). Examples of harmful consequences include reputational impact (e.g. disclosing social activity makes one look bad in job interview) or being unable to achieve a goal (e.g. disclosing income level prevents individual from obtaining credit). It should be noted that when an individual discloses personal data to an organization s/he loses control over how the data will be used, making it difficult to foresee negative consequences. The data is stored by the data receiver, who can edit it, link it with other data, or disseminate it at a later date. All of which can cause the data to lose contextual cues increasing the likelihood of privacy invasions (Adams, 2001; Nissenbaum, 2004). One example of hidden data usage that can impact individuals' life is the use of census data in marketing products used for geo-demographic profiling (e.g. Mosaic UK; Experian, 2013) which can result in social sorting, where individuals are offered services under harsher conditions (e.g. high insurance premiums or interest loans) or simply denied services because of the way they have been profiled (Lyon, 2003).

In the 2001 Culnan-Milne Survey on Consumers & Online Privacy Notices, 64% of participants said they had refused to disclose data to a website because they did not know how it would be used (Culnan & Milne, 2001). Making individuals understand how their personal data is used by organisations or information systems is an important factor in minimising perceptions of privacy invasion (Lederer et al., 2004). However, effectively communicating how data is used is not a trivial task. For example, individuals rarely read privacy policies (Kobsa & Teltzrow, 2004) and when they do most policies require too much time and effort to understand (Sherman, 2008). Providing a reason for each data request seems to be more effective: in a between-participants experiment on disclosure in web forms, participants were significantly more likely to answer questions when shown individual justifications for each one, than when provided with a link for a general privacy policy (Kobsa & Teltzrow, 2004).

### 2.1.1.6 Effort

The effort required to answer data requests has an impact on the likelihood of compliance. If a request is perceived as difficult to answer by individuals they will be less willing to provide it (Annacker et al., 2001). Difficult data requests include questions that require memory effort, looking up information in documents, or creating new answers (e.g. "Tell us what you think about X") (Jarrett & Gaffney, 2009). Effort also depends on how many data items are requested. Quantity of required data has been linked to perceived value of providing the data (Miltgen, 2007) and actual disclosure likelihood (Hui et al., 2007).

#### 2.1.1.7 Contextual Factors

Disclosure behaviour is influenced by the context in which the interaction takes place. The social, organisational and cultural conditions in which the interaction takes place affect privacy perceptions because they determine the communication and behavioural norms of the situation (Adams, 2001; Stone and Stone, 1990 cited in Millberg et al. 2000). Moreover, the technology environment, the individual's past experiences, knowledge and preconceptions of that technology, and the level of interaction she will have with it also have an influence on her perceptions (Adams, 2001; Hine and Eve, 1998; Stone and Stone, 1990).

#### 2.1.1.8 Privacy Concern

Researchers have developed several different measures of privacy concern. One of the first and most used is Westin's privacy segmentation (Harris and Associates Inc. & Westin, 1998). This scale consists of three privacy concern statements which participants are asked to rate with regards to their level of agreement (1 = strongly disagree and 4 = strongly agree):

- "Consumers have lost all control over how personal information is collected and used by companies"
- "Most businesses handle the personal information they collect about consumers in a proper and confidential way"
- "Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today"

Based on their answers respondents to Westin's privacy segmentation are assigned to one of three groups: (1) privacy fundamentalists, who agree with the first statement and disagree with the other two; (2) privacy unconcerned, who disagree with the first statement and agree with the other two; or (3) privacy pragmatists, who comprise everyone else. While widely employed, possibly due to its shortness, there is little evidence that Westin's scale is a good predictor of actual behaviour (Consolvo et al., 2005; Malheiros & Preibusch, 2013).

Smith et al. (1996) developed a 15-item scale aimed at measuring individuals' concerns regarding organisational personal data practices, the Concern for Information Privacy Scale (CFIP). The items load on four factors: concern with (1) collection; (2) errors; (3) unauthorised secondary use; and (4) improper access. Stewart & Segars (2002) confirmed that each dimension (factor) of the scale is indeed reliable and distinct, but suggest representing CFIP as a higher-order factor structure instead of the four first-order factors in the original scale, i.e. CFIP is not the four factors, but influences the four factors.

Since CFIP was focused on offline consumers and it was assumed that internet users' concerns differed from them, Malhotra et al (2004) develop the Internet Users' Information Privacy Concerns (IUIPC), a second-order model. IUIPC has three dimensions: users' (1) concern with collection of personal data; (2) control over that collection; and (3) awareness of how the collected data is used. IUIPC had a negative impact on behavioural intention (through the factors *trusting beliefs* and *risk beliefs*, but no research was done linking it to actual disclosure behaviour.

Buchanan et al. (2007) attempted to develop a multi-dimensional privacy concern scale but find their 16 items load only on one factor, which they call *privacy concern*. They developed two more scales, one for *general privacy caution* and another for *technical protection*. They found that both Westin's privacy scale and IUIPC were significantly and positively correlated with their privacy concern measure.

While these measures exhibit good internal validity, they have not been linked to actual privacy behaviour. Instead, only their relationship to self-reported behavioural intentions was investigated. In the context of privacy research this constitutes a major limitation of privacy scales, because privacy concern is often inflated comparing to actual behaviour. This discrepancy, known as the *privacy paradox*, is discussed in the next section.

### *2.1.2 The Privacy Paradox: Stated Concern versus Actual Behaviour*

One of the main research problems in privacy research is to explain why individuals' stated privacy concerns differ from their disclosure behaviour. In its 1998 report to US Congress on online privacy, the Federal Trade Commission (1998) states that many consumers were still reluctant to participate in the online market. Citing a study by Louis Harris & Associates and Dr. Alan F. Westin (1997 in Federal Trade Commission, 1998), the FTC argues that "a substantial number of online consumers would rather forego information or products available through the Web than provide a Web site personal information without knowing what the site's information practices are". In a Business Week and Harris (1998) survey of the same year, respondents chose privacy as the number one factor affecting how much they use the internet. A survey conducted by the Pew Internet and American Life Project (2000) discovered that 86% of American internet users are in favour of policies that make companies ask people for permission before using their personal data and 54% think being tracked by websites is harmful because it is a privacy violation. Moreover, 84% of the users state they are concerned with businesses and strangers getting their – or their families - personal information. Similarly, a Jupiter Research (2002) study concluded that 70% of US internet users are concerned that their privacy is at risk on the internet.

The overwhelming number of respondents to these surveys that said they were concerned with privacy and the collection of personal data seemed to indicate that a severe consumer backlash against internet use and e-commerce was in order. However, between 1998 and 2001, not only did e-commerce keep growing, it grew at a faster pace than predicted by privacy surveys (Harper and Singleton, 2001) and it kept on growing (comScore, 2008).

In an study that involved asking participants about their privacy notions and then watching their interaction with an e-commerce website, Berendt and Spiekermann, (2005) observed that subjects who had expressed concerns regarding their privacy online seemed to forget them when interacting with the website bot that asked them both product related and personal questions (non product-related). Unfortunately, the effect of using an anthropomorphic bot in the interaction and the fact that it may have lead participants be more comfortable with disclosing personal data was not investigated.

Harper and Singleton (2001) argue that this discrepancy is due to the flawed (or manipulative) design of some privacy surveys. Common errors, according to the authors, include starting with provocative questions, asking questions in a biased way ("push polling") and mixing privacy with issues such as spam and credit card fraud. In addition, surveys suffer from the "talk is cheap" problem, i.e., consumers asking for better regulation often do not consider the costs that would be associated with it. Moreover, in unprompted surveys, privacy does not come up as a top concern.

Similarly, in a 2009 London School of Economics (LSE) study (Kourti, 2009), student participants were rewarded with chocolate bars in exchange for answering personal questions. The majority of participants disclosed a valid LSE username (91%), address (90%) and phone number (67%). A few people further revealed their date of birth and LSE password. It should be noted that the inquiry took place at a university fair and that the researchers never identified themselves. This experiment shows that some individuals are willing to trade sensitive data for small immediate rewards like confectionary items, seemingly undervaluing the privacy risks involved.

### *2.1.3 Psychological Biases in Privacy Decision Making*

Acquisti (2004) explains the underestimation of privacy risks by suggesting that privacy decision-making does not follow a rational behaviour model. Even individuals who are privacy conscious and want to protect themselves may be unable to do so due to having: (1)

incomplete information; (2) bounded rationality; and (3) psychological distortions. Individuals do not usually possess enough information to estimate the risk resulting from a disclosure – i.e. the probability of suffering a privacy invasion and the magnitude of its impact on their lives. They are also unaware of the protective measures – legal and technological – that they can employ to decrease that risk. Even if they were aware of these facts, it would be very complex for an individual to calculate the costs and benefits of each disclosure decision and compare the utilities of each one to determine a course of action. Humans have limited processing power and time. Finally, assuming that individuals had enough information and rational capability to estimate the utility of each decision, psychological distortions can still lead them away from an optimal decision. These include: (1) *hyperbolic discounting,* i.e. underestimating the probability of future risks; (2) opting for immediate gratification when they should look to protect themselves; (3) having optimism bias, i.e. assuming their own risk is smaller than other people's; and (4) difficulty in dealing with cumulative risks, such as the successive increase in the likelihood of suffering a privacy invasion that comes with each individual disclosure.

Aspects related to how data requests are framed can also influence disclosure behaviour. Acquisti et al (2012) replicate two effects that play on the comparative nature of decision-making: (1) herding; and (2) anchoring. In a series of studies, they found that individuals were more likely to disclose sensitive data if they were told that other people have made the same disclosure. They also found that the order in which questions are asked can influence the likelihood of an individual answering them. Individuals will "anchor" their perceived sensitivity of the questions on the first question they read. Thus, when questions are asked in decreasing order of sensitivity disclosure is higher.

Syverson (2003) disagrees that individuals are irrational in privacy decision-making. For the author, the probability that disclosing personal details will result in serious negative consequences – such as identity theft – is so low that going ahead with the disclosure in exchange for small rewards is the rational decision. One should also consider that not only immediate benefits contribute to individuals disclosing personal details. Individuals are willing to exchange personal data related to specific products or services if they perceive that it will contribute to a better service and product quality in the future (Annacker et al., 2001); thus, their decision-making is not always myopic.

### 2.1.4 Privacy Trade-Offs

Even when users perceive that an interaction can have implications for their privacy, they may still be willing to accept it if they consider its benefits outweigh the privacy risks (Laufer and

Wolfe, 1977; Milne and Gordon, 1993; Culnan, 1993; Culnan and Armstrong, 1999; Adams, 2001; Dinev and Hart, 2006). As mentioned above, when consumers are asked to exchange personal data for a service or product they are entering into a social contract. If the benefits from this social contract are larger than the costs resulting from loss of privacy they will agree to it (Milne and Gordon, 1993).

Previous studies have found mixed support for the claim that individuals are willing to pay for privacy. Hann et al. (2002a; 2002b) estimated that U.S. individuals would be willing to pay between 30 and 45 USD to prevent errors, improper access, and secondary use of their personal data by a website in one of three industries: financial, healthcare, and travel. While commendable for "putting a value" on privacy this research is limited for being based participant rankings of options and not actual financial commitments involving their own money. Moreover, it is likely that willingness to pay, and how much to pay, for privacy will be highly depended on contextual factors like brand perception, which go beyond the industry.

Beresford et al. (2010) designed a field experiment where participants were asked to buy a DVD from one of two online stores identical in everything except the fact that one asked for more sensitive data during the purchase. In the treatment where the DVD was 1 EUR more expensive at the privacy sensitive store, participants preferred the cheaper store. In the treatment where DVDs were the same price, participants bought equally from the two stores.

Less ambiguously, past research shows that individuals are willing to disclose personal data in exchange for economic benefits. Hui et al. (2007) found that monetary rewards had a positive effect on disclosure, while Kourti (2009) found evidence that individuals will exchange personal data for other types of rewards, such as chocolate. Cvrcek, D. et al (2006) asked participants to bid how much they would have to be paid to disclose their location data for commercial or academic uses. Using participants from five different countries, they found that the median bid for commercial use of data was roughly double the median bid for academic use of data, which was around 30 EUR.

These studies suggest individuals are more willing to sell their personal data than to pay for privacy. In fact, this was exactly what Grossklags & Acquisti (2007) found in a study comparing willingness to sell and willingness to protect personal data: participants showed a clear preference for selling their data over protecting it.

### *2.1.5 Privacy Protection Behaviours*

In the case that individuals do not perceive the benefits of a disclosure to outweigh the costs there is a chance they will engage in privacy protection behaviours by either withholding

(Sheehan & Hoy, 1999; Culnan & Milne, 2001; Metzger, 2007) or falsifying their answers (Culnan & Milne, 2001; Lwin & Williams, 2003; Horne et al., 2007; Metzger, 2007). These can be interpreted as attempts to minimise the costs of disclosure while still obtaining the reward. While some factors have been linked to privacy protection behaviours, namely sensitivity and effort, it is not clear how likely individuals are to engage in them. This thesis investigates the relationship between other perceptual factors and privacy protection behaviours and the likelihood of individuals actually lying or omitting personal data.

### *2.1.6 Property rights over personal information*

Posner (1978, 1981) argues that, since personal information disclosure is costly for the person it relates to and valuable to others, people having property rights over it and being allowed to sell these rights would lead to exchanges that would maximize the information's value for society. However, depending on the nature and origin of the information and transaction costs, there could be exceptions for this attribution of property rights. For example, for a magazine that wants to sell its subscriber list to another company the cost of obtaining consent is higher than the value of the list. As the value of the list is higher for the company buying it than the value of being protected from direct marketing is for the subscriber, Posner argues that property rights should be attributed to the magazine.

This is a purely utilitarian view, where the option that maximizes value for society is considered optimal. The author would argue that it is difficult to make any comparison at all. Although companies know the exact value of a subscribers list, measuring how different individuals value "not being bothered by direct marketers" is a much more difficult task. Moreover, it has been suggested that it is not the actual marketing that bothers people, but not knowing how companies got their names and addresses (Culnan, 1993).

The problem of framing privacy issues (or control over personal information issues) in an "individual preference versus society's interest" way is that it misses out on fundamental aspects of privacy by ignoring its social value (Solove, 2008). If individual privacy loses every time it is pitted against society's interests then an environment is created where privacy can always be invaded as long as it is done in the name of a "higher" societal value, such as security. This contributes to the surfacing of "chilling effects", where citizens, believing to be under constant surveillance start to self-censor their behaviour for fear of looking suspicious in the eyes of the observers. These effects would adversely impact creativity, free speech, freedom and the quality of democracy. Because of this, Solove (2008) defends that privacy should not be seen as an individual value but as a societal good, in a sense applying Kant's categorical imperative in that if privacy losing against other interests becomes universal law, then the overarching consequences will be negative.

## 2.2 Perspectives on Privacy

The concept of privacy first emerged from the discussion of the public life / private life dichotomy, albeit not addressed directly. In Politics, Aristotle (1999), while speaking of the state, describes the oikos (home, household) as the domain of the private life and family relationships and sets it in opposition to the polis (community or state), the realm of political discussion and public affairs. In the 17th century, John Locke (1823), in Two Treatises of Government, also makes a distinction between the private and public realm by way of the discussion of the differences between paternal and political power (Kelly, 2002). He further states the limits of the power of politic authority over family matters, a point of argument which is reinforced in A Third Letter for Toleration (John Locke, 1988 cited in Kelly, 2002), where he makes an argument for the autonomy and freedom of interference, either from the government or others, in private affairs. This is a view shared by John Stuart Mill (1859), whose claim that “over himself, over his own body and mind, the individual is sovereign” also hints at a private realm of the individual, which only he has power over.

With the invention and increasing use of portable photographic cameras, and the widespread dissemination of photographs by means of newspapers, at the end of the nineteenth century came the first modern argument in favour of a right to privacy. Privacy was equated with “the right to be let alone” and sustained by the principle of “inviolate personality”(Warren and Brandeis, 1890). Privacy can therefore be understood as the state of other people being unable to access some part of ourselves, such as information about ourselves or our behaviour (Clarke, 1997; Smith, 1993; Reiman, 1995; Gavison, 1979; Posner, 1978; 1981). Clarke (1997) defines it as “the interest that individuals have in sustaining a 'personal space’, free from interference by other people and organisations.” Gavison (1979) adds that, in order for an individual to enjoy perfect privacy, three things must happen: 1) no one has information about the individual; 2) no one pays the individual any attention; and 3) no one has physical access to the individual.

Historically, there was an evolution from a perception of privacy and the private space as something closely related to the family space, which is in contrast to the political sphere and in potential conflict with political power to an individual claim to be able to keep certain things outside the accessibility of everyone else, including not only political authority but also business organisations and even members of our families. This personal space, however, is never fully defined which makes this type of definitions vague and consequently difficult to apply to real world problems (Solove, 2008).

Privacy is also commonly interpreted as having control over who has access to (1) your personal information (Culnan, 1993; Westin, 2003); (2) “knowledge about oneself” (Fried, 1967); (3) “the ways that information about [you] is collected, verified, and passed on to other organisations” (Kling, 1996); (4) or “an aspect of the identity one projects to the world” (Agre and Rotenberg, 1998), among other similar definitions. The difference between definitions of privacy as control and definitions of privacy as deprivation of access are better illustrated by an example given by Fried (1967). Consider a person stranded in a desert island. No one has access to her, but not as a result of her exercising any type of control. Thus, according to control definitions, she has not privacy. This goes against the common sense understanding of privacy and, for this reason, proponents of the deprivation of access definitions, such as Reiman (1996) reject control as a necessary condition for privacy.

An additional theme in the concept of privacy is intimacy. Inness (1992) defines privacy as “the state of the agent having control over a realm of intimacy”, and argues that “privacy’s contents cover intimate information, access and decisions”. Insofar as it concerns control, this definition is similar to the ones mentioned before. However, the author only includes information which is intimate in the realm of privacy. Fried (1967) similarly affirms that privacy “creates the moral capital which we spend in friendship and love.” The main problem with interweaving the concepts of privacy and intimacy is that many non-intimate pieces of information, such as your address or phone number, can lead to privacy invasions. DeCew (1997 cited in Solove, 2008) gives the additional example of financial records, which are private despite not being intimate.

Normative discourse on privacy focuses on whether privacy should be considered a fundamental human right and what its benefits and costs for society are. One view is that privacy is a necessary condition for democracy and individual freedom. Privacy is seen as important because it allows for a personal inviolable space where thoughts, ideas and emotions can take form and where creativity and imagination strive. It allows for self-development, self-affirmation and experimentation away from society’s judgement. It protects every individual from what Mill (1859) called the “tyranny of the majority”. It contributes for the development of intimacy and personal relationships. Privacy is seen as vital because it allows private and critical political and ideological discussion and thought to take place without oppression from the state. The opposite view is that privacy can be costly to society and should not be protected, at least in some cases. For example, Posner (1978, 1981) sees privacy as concealment of information and argues that the less information is available in the marketplace the less efficient it will be. He argues that people should not be allowed to withhold unflattering information about themselves since that information could have value for other people. Posner compares an individual keeping secrets about himself from a potential employer with a vendor concealing defects on her products. Privacy in conjugal life has also been criticised from a feminist perspective because it can contribute to keeping spousal abuse hidden and women oppressed (Solove, 2008).

With regards to the definition of privacy, this thesis is firmly positioned in the field of privacy as control. This is in accordance with privacy research in computer science, which sees privacy as control over one's personal information (see Section 2.3). From a normative perspective, this thesis takes a utilitarian approach to the study of privacy. It argues that excessive collection, storage, use, and transfer of personal data can actually be counter-productive to an organisation because individuals may engage in privacy protection behaviours. It attempts to clarify how organisational data practices can be adjusted to better serve their customers' (or employees or citizens) interests while improving the quality of the data they collect, thus maximising utility.

### *2.2.1 A Multi-Disciplinary Concept*

Privacy presents itself as a complex and difficult to capture concept for which there is no single consensual definition. However, independently of the perspectives on privacy that different authors have, it is possible to find common privacy themes within the same scientific discipline. Table 2.1 summarises some of the different foci of enquiry in the study of privacy by field of science. Of particular relevance for this thesis is the research on privacy decision-making (and *privacy calculus)* that originated in the fields of social psychology (Laufer & Wolfe, 1977) and marketing (Milne and Gordon, 1993; Culnan, 1993; Dinev and Hart, 2006).

| Discipline | Themes | Examples |
|---|---|---|
| Law | - Definition of privacy<br>- Value of privacy<br>o Independent normative value<br>o Balancing privacy against other interests<br>o Individual vs. societal interests<br>- Legal protection of privacy | Warren and Brandeis, 1890; Gavison, 1979; Solove, 2008; Inness, 1992; Posner, 1978; Fried, 1967. |
| Political Science | - Data protection policy<br>- Social impact of collection and use of personal data<br>o Social distribution of this impact | Raab and Bennett, 1996; 1998; Westin 2003; |
| Computer Science | - Development of tools to control flow of personal data<br>- Feedback on systems' and web sites' data practices<br>- Data protection<br>- User models of privacy | Ackerman and Mainwaring, 2005; Cranor et al., 2006; Lederer et al., 2004; Adams, 2001 |
| Sociology/<br>Social Psychology | - Social constructions of privacy<br>- Social impact of collection and use of personal data | Hine and Eve, 1998; Laufer and Wolfe, 1977 |
| Economics | - Value of personal information<br>- Market for personal information<br>- Privacy individual decision making process | Posner, 1978; Acquisti, 2004; Syverson, 2003 |
| Philosophy | - How privacy works<br>o Control vs. limited access<br>- Content (scope) of privacy<br>o Individual, decisions and information<br>- Value of privacy | Inness, 1992; Ullmann-Margalit, 2009 |
| Marketing | - Trade-offs: personal information for benefits<br>- Marketers data practices<br>- Consumer privacy<br>- Data quality | Nowak and Phelps, 1997, Milne and Gordon, 1993; Phelps et al., 2000; Culnan, 1993 |
| Management | - Self-regulation vs. government intervention approach to privacy<br>- Organisational information privacy practices<br>- Organisational notions of privacy<br>- Workplace privacy | Milberg et al., 2000;<br>Smith, 1993; Smith et al., 1996;<br>Stone et al., 1983;<br>Tolchinsky, 1981. |

**Table 2.1: Approaches to privacy research from different disciplines**

### *2.2.2 Multi-Dimensionality of Privacy*

Attempts to find unifying definitions of privacy end up being too vague to tackle real world issues. In order to address these limitations, some authors have broken down the privacy concept into components better adjusted to specific situations. One way to do this is to categorise privacy according to its object: e.g. body, behaviour, communications or information (Clarke, 1997; 2006; Davies, n.d.) – see Table 2.2.

| Clarke | Davies; Privacy International | Description | Invasion Examples |
|---|---|---|---|
| Privacy of Personal Data | Information Privacy | Individuals' right to control the way their personal data is available and used by others | Bank selling someone's credit record to a marketing company without his or her knowledge |
| Privacy of the Person | Bodily Privacy | Individuals' freedom from interference with their own body by others | Medical treatments against the individual's will; compulsory blood or DNA sampling |
| Privacy of Personal Communications | Communications Privacy | Individuals' claim that their communications should not be monitored by others | Wiretapping; third party email access |
| Privacy of Personal Behaviour | Territorial Privacy | Individuals' right to a private space | Intrusion into a inherently private space such as a toilet; excessive scrutiny while in a public space such as a street |

**Table 2.2: Dimensions of privacy**

Solove (2008) proposes a different way to look at privacy invasions. This author creates a privacy issues taxonomy structured around the information life cycle (Figure 2.1). This data or information life cycle comprises a collection phase, a processing (or usage phase), and a dissemination (or transfer phase). Information or data privacy concerns and invasions are intrinsically related to this cycle and vary according to the phase they occur (Solove, 2008; Culnan, 1993; Stone, 1983). This taxonomy also includes two additional privacy harms not related to the information cycle: (physical) intrusion and decisional interference (not in the figure).

This constitutes a pragmatic deconstruction of the privacy concept, which also aims to help address specific real world situations. However, this applicability comes at the expense of a more detailed (and colourful) explanation of the harmful consequences of these privacy violations for the individual (Bartow, 2006 in Solove, 2007, p.768; Schneier, 2009). In a study trying to identify the various dimensions of individuals' concerns with regards to information privacy present in the literature, Smith et al. (1996) singled out collection, unauthorized secondary use, errors and improper access as the most relevant (all of which are included in this taxonomy, albeit with different names).

**Figure 2.1: Solove's (2008) privacy issues taxonomy (adapted)**

Parallels can be drawn between these two different ways of breaking down privacy. Clarke (1997) argues that personal data privacy and personal communications privacy have become closely related. He calls the combined concept *information privacy*. In fact, those two dimensions are related to Solove’s information collection, processing and dissemination activities; while Solove’s intrusion privacy harm (not included in the figure) is related to the bodily and territorial privacy dimensions of Clarke and Davies. It should also be considered that even non-informational aspects of a person’s life - such as the body or behaviour of an individual - can become data and information when they are captured or recorded, such as a video recording or digital copy of DNA sample.

The conversion of non-informational elements of an individual’s life into information can have a serious impact on that individual’s privacy. First, despite being impossible to fully capture reality in the form of data fields, organisations will make decisions based on them that will have real life implications for the people the data concerns. Second, data can be easily stored and transmitted quickly getting out of reach – and awareness - of the individual. Finally, data can be used, either by itself or in an aggregated form, to draw inferences about a person that would have been difficult to draw otherwise. These factors can influence the way individuals perceive the value of disclosing certain items of personal data and how willing they are to disclose it to specific organisations.

### *2.2.3 Personal and Sensitive Data*

Due to the subjective and contextual nature of personal data, there is often a discrepancy between regulatory bodies' definitions and individuals' perceptions' of what and when data items are personal. The UK Data Protection Act of 1998 (UK Data Protection Act, 1998) states that personal data is "*data which relate to a living individual who can be identified from those data*", such as the individual's name, address or date of birth. Personal data elements which are considered sensitive are enumerated and include racial or ethnic origin, political opinions and religious beliefs. This pragmatic view makes it possible to work with the concept of personal data and create and apply laws that protect individuals from privacy violations. However, it focuses exclusively on the data itself and not on how the data is perceived by different individuals in different contexts. According to Adams (2001), it is important to consider how individuals perceive data and not rely solely on clear cut definitions of personal data that focus on personal identifiable items in order to avoid privacy invasions.

## 2.3 Privacy and Technology

> *"Technology boosts our privacy in the present, but it threatens the privacy of our past."*
>
> *(O'Hara & Shadbolt, 2008).*

Information technology has a dual role with regard to privacy. It has facilitate widespread collection and processing of personal data hugely increasing both the probability and the impact of privacy invasions. Commercial and government databases store huge amounts of personal data and transaction logs from which profiles and patterns of behaviour can be inferred with the help of data mining algorithms and decisions based on these profiles have real impact on individuals' lives. At the same time, information systems allow individuals to interact anonymously and even completely avoid visual and physical contact if they so wish, while cryptographic algorithms help keep personal data secure. Some technologies, called privacy enhancing technologies (PETs) are developed specifically with the goal of supporting transparency and control over personal data. Still, the design of privacy sensitive systems is not trivial and offers many challenges.

### 2.3.1 DESIGNING FOR PRIVACY

In computer science, privacy is equated with an individual having control over the flow of her personal data. This definition has a natural affinity with the fields of HCI and security (Ackerman & Mainwaring, 2005); thus, most privacy related work in computer science has been done in these two fields. HCI has focused on creating mechanisms that provide feedback to the user on the actual or potential flow of her personal data when interacting with an information system or organisation. The security field has focused on giving the user tools that allow her to protect data she deems personal by means of encryption and access control or avoid surveillance – or at least mitigate its effects – by means of anonymisation. Despite the work done in the HCI and security fields, the difficulty in operationalising the concept of privacy has caused many information systems to have serious privacy flaws.

Most attempts that have been made at developing tools that enable an individual to manage the disclosure of her personal data end up being too complex or cumbersome for the average user. Ackerman (2000 cited in Ackerman & Mainwaring, 2005, p.390) argues that there is a "*gap between what we know we must do socially and what we know how to do technically*" - the "*social-technical gap*". This gap may be due to the difficulty in codifying privacy's operational concepts, such as "control" and "personal data" in a standard way. In fact, it is argued that privacy cannot be understood in a "standard" way due to its extremely contextual nature (Ackerman & Mainwaring, 2005; Acquisti, 2004; Adams, 2001; Hine & Eve, 1998). This context dependency means that people have difficulty reasoning about privacy in the abstract. Unless confronted with very specific examples they are unable to predict how they would (not) want their information to be disclosed in a hypothetical situation (Lederer et al.,2004; Cranor, 2005). This makes it very difficult to understand people's privacy needs and attitudes a priori and consequently eliciting privacy requirements.

These limitations have contributed to some common privacy design issues. One such issue is the lack of clarity regarding the potential and actual information flows of technologies, i.e., it should be explicitly stated what information is and will be collected, who has and will have access to it, for how long, for what purposes, etc. (Lederer et al., 2004; Friedman, Lin and Miller, 2005). Another important aspect is that although users value privacy it is not their main concern when using a technology (Karat, Brodie and Karat, 2005). This means that whatever mechanism is used to enforce privacy it should blend in with the normal usage of the system. Privacy should be a natural result of the user's interaction with the system and should not require too much configuration (Lederer et al., 2004). Moreover, users should have a high-level mechanism to control participation and information flow as well as the opportunity to withdraw approval at any time (Lederer et al., 2004; Friedman, Lin and Miller, 2005). An additional dilemma of privacy tools is that if they are being effective in protecting user's privacy nothing seems to happen. Brunk (2005) suggests a logging mechanism that reassures users that the tool is working properly and protecting their personal data in order to contravene this problem. However, this author would argue that feedback mechanisms have to be pondered carefully since they can have a negative impact on usability. Privacy protection mechanisms should not disrupt a user's *main task* (Friedman et al., 2005) – the operations performed to achieve a specific goal (Hackos and Redish, 1998). The cost for failing to comply with these or other users' privacy requirements can be rejection of the technology (Karat, Brodie and Karat, 2005; Adams and Sasse, 2001; Adams, 2001).

In order to evaluate the universe of privacy tools available, Brunk (2005) created a framework - based on Schneier's Security Processes Framework (2002, cited in Brunk, 2005) - covering awareness, detection, prevention, response and recovery. This approach describes privacy as a process where each stage gives more feedback and control to the user, meaning that the more categories covered by a privacy solution the better it is. This framework results from a comprehensive compilation and analysis of different privacy features that several privacy software tools offer. Although attempting to take a user-centred approach to the privacy protection problem the author's analysis does not factor in *user experience* – thoughts, emotions, perceptions that a user has while interacting with something (Tullis and Albert, 2008). This is an important issue, because the same factors that shape the user experience will affect the way the user perceives her privacy (Adams, 2001) when interacting with a tool. In fact, this author would argue that privacy perceptions are an integral part of the user experience.

#### 2.3.1.1 The example of P3P

The Platform for Privacy Preferences (P3P) (Cranor, 2006) is one of the most well known privacy enhancing technologies (PETs). P3P is a W3C specification for writing privacy policies in a machine and human readable format using XML. The goal is to allow websites to communicate their privacy practices in a standard way and transfer the burden of reading and evaluating privacy policies from the user to agents installed in the user's browser. The user configures his privacy preferences in the agent, which compares them with each visited website's policies and either informs the user of the result of this evaluation or make a decision regarding access to the website – possibly blocking it. A P3P policy covers the whole information cycle, i.e., data collection, data usage and data transfer practices and includes components for describing the purpose of the data collection, types of data collected, whether users can opt-out or opt-in of specific data uses and who the data is shared with. However, P3P has been criticised for failing to establish privacy standards and instead focusing on mediating privacy negotiations which will harm those who cannot "*purchase*" enough privacy (Electronic Privacy Information Centre, 2000). If there is already a discrepancy of power between the parties negotiating – company and client – a negotiating tool will not increase the privacy protection of the user and can actually make it easier for the user to part with data he deems personal. In addition, the configuration of P3P tools can be too difficult for the average user. Moreover, P3P in no way enforces the policies that websites state meaning that users will have to trust websites to do what they say they do with their personal data (Electronic Privacy Information Center, 2000). Finally, the adoption rate of the P3P standard by websites is very small: "*10% of the sites returned in the top-20 results of typical searches*" (Cranor et al., 2008). This can be explained in part by the fact that those who have to do the effort to implement P3P - the websites – do not have strong incentives to do so. When those that have to bear the costs of a technology are not the ones benefitting from its use the technology can be rejected (Grudin, 1994 in: Iachello and Hong, 2007).

### *2.3.2 Data mining*

Data mining allows additional layers of meaning to be inferred from data collections. It supports the transformation of data into information and *knowledge*. Knowledge consists of information aggregated in such a way as to be useful and allow predictions to be made regarding future events (Bellinger et al., 2004). Going back to the bank account example above, linking all the data concerning an individual in order to build a customer profile would be considered creating information. Using these profiles to extract rules that predict the likelihood of a customer defaulting on a loan would be considered knowledge creation according to this definition.

Depending on what one wants to find out from the data, different data mining algorithms can be used. Tasks that can be carried out by these algorithms include, among others (Hormozi and Giles, 2004):

- *Clustering*. Clustering consists in grouping data into clusters so that each clusters contains similar elements according to some criteria. Clustering can be used by businesses for market segmentation, i.e., to understand the different types of customers they have.
- *Predictive modelling*. Predictive modelling is used for predicting the value of an attribute based on the value of another attribute. It can be used for credit approval (who is more likely to default) or for anticipating which customers will leave for instance.
- *Link analysis*. Link analysis tries to reveal connections between data records. It can be used by retailers to find out which products are normally bought together (market

basket analysis) or to analyse the purchasing pattern of the same customer over a long period of time (if they use a loyalty card for instance).

- *Deviation detection*. Deviation detection consists in identifying outliers such as records that do not fit into any cluster for example. Credit card fraud detection and quality control are two areas where deviation detection is used.

Because it formalises knowledge in probabilistic models based on large quantities of aggregated data, data mining can create privacy risks for individuals. First of all, an individual voluntarily providing personal data may not be able to foresee the conclusions that can be drawn from that data through its aggregation with other data – hers or other individuals' - and the use of data mining techniques. Second, organisations may rely on the knowledge extracted by data mining to automate decision making. If probabilistic models are applied in a deterministic way and without human supervision they have the potential to unfairly exclude individuals from certain services. These two issues are related in that they both result from an individual's personal data being fitted against a model which is based on other individuals' personal data. Although these models assign probabilities to events and personal characteristics (e.g.: probability of an individual defaulting on a loan; probability of a customer buying milk after buying cereal) they ultimately result in a deterministic decision from the individual's point of view. The use of postal codes for assessment of credit worthiness by financial institutions is an example of these issues. If a new customer lives in a neighbourhood associated with loan defaults, she can have difficulty getting a loan simply by disclosing her address, even if she is in a sound financial position.

The need to address some privacy issues has caused the development of privacy preserving data mining techniques (Clifton & Marks, 1996; Agrawal & Srikant, 2000; Verykios et al., 2004). These techniques have the goal of balancing privacy with inferring power and should ideally preserve individuals' privacy (or organisations') with minimum impact on the data mining algorithms predictive power. Solutions include query restriction techniques (e.g.: restricting the size of a query result or keeping an audit trail of answered queries) and data perturbation techniques (e.g.: blocking data, adding noise or swapping values of individual records). (Agrawal & Srikant, 2000; Verykios et al., 2004). However the amount of privacy protection offered is limited by the algorithm being used (Verykios et al., 2004).

### *2.3.3 Data quality*

With the evolution of data mining algorithms and their profiling and predictive capabilities, the potential value of raw data has increased, and with it the incentive to collect as much of it for as long as possible. The rational for the increased data collection is that even if the data is not useful right now it may be so in the future. However, in addition to its privacy implications, extensive personal data collection and use may affect the quality of the data.

Data quality is defined as data which is fit for use by data consumers with fitness usually being evaluated according several dimensions which include accuracy, timeliness, completeness, consistency, reliability, relevance and precision (Strong, Lee & Wang, 1997; Rudra & Yeo, 1999; Xu et al., 2002).

Organisations usually have heterogeneous data structures, with different departments working with different database systems. These departments may share data with each other, and also with external organisations. This contributes for the existence of several versions of the same data records which sometimes are inconsistent across the systems negatively affecting data reliability (Rudra & Yeo, 1999). It is likely that the more extensive the data collection, the more serious this problem becomes. In addition, the practice of keeping data for long periods of time will cause it to be progressively more outdated negatively affecting its accuracy and reliability.

If data subjects perceive that a data request is not relevant for the interaction in question, they are more likely to feel that their privacy is being invaded (Culnan, 1993). Also, if too many data items are requested that will negatively affect disclosure rates (Hui et al., 2007). Moreover, when individuals do not perceive the benefits of a disclosure to outweigh the costs they can engage in privacy protection behaviours by either refusing to answer or disclosing false answers (Horne et al., 2007). These reactions adversely affect the receiving organisation's data quality (Horne et al., 2007). In fact, data never being fully captured has been identified as one of the main causes of companies' data quality issues (Rudra & Yeo, 1999).

The quality of the data of an organisation is important because it influences how well its business and decision-making processes run. Poor data quality impacts the effectiveness and efficiency of these processes causing customer dissatisfaction, increasing costs and impairing strategic manoeuvrability (Redman, 1998). Poor data quality is estimated to cost businesses hundreds of millions of dollars in the U.S. alone (Batini & Scannapieco, 2006).

It seems likely that more balanced personal data collection policies and processes, where less items and more relevant data are collected on individuals, would actually increase the value of that data for organisations. If individuals are able to understand why the data is being collected and the benefits they will get from that disclosure they will probably be more accurate and truthful in their answers; hence, they will not engage in privacy protection behaviours, which would decrease the reliability of the data.

### *2.3.4 Data and Information*

A distinction needs to be made between the concepts of data and information. Data is commonly defined as raw facts that describe objects' and events' properties (Ackoff and Rovin, 2003). These facts have little value until they are transformed into information and used for a specific purpose. Data is transformed into information through interpretation, i.e., the attribution of meaning to data items by finding relationships between them (Ackoff in: Bellinger et al., 2004). For example, an account number residing in a bank's information system has, by itself, little usefulness, but if it is associated to other facts and events such as a name, a balance, cash withdrawals, deposits, etc. then it can be used by the bank to decide whether to grant a  loan to the customer these data relate to. This collection of facts and their relationships constitutes information.

There are several factors that prevent interpretation from being a simple process. In the first place, interpretation is influenced by how one plans to use the resulting information. In other words, the purpose shapes the interpretation which in turn shapes the information (Kent, 2000). Furthermore, the data being interpreted is often not a perfect reflection of reality. First of all, because there is an inherent discrepancy between reality and representation of reality (Kent, 2000). Second, because data quality naturally degrades with time (see section 3.3). These imperfections of data, and the process through which data is transformed into information, mean that conclusions drawn from personal data have to be carefully weighed before being used to make decisions that have real implications for individuals.

## 2.4 Regulatory Approach to Privacy Protection

> *"Laws are always reactive and therefore they lag behind the problems they purport to solve"*
>
> *(Stone, 1975 in: Smith, 1993)*

With the evolution of personal data management from paper-based to computer-based, the risks to individuals' privacy increased. First, as personal data became easier to collect, store, process, and transmit, more people had access to it. Second, the control people had over their personal data and information on its collection and processing decreased. As an answer to these increasingly relevant issues, the UK government appointed Sir Kenneth Younger to lead a committee on privacy in 1972 (Smith, 1994). While this report was largely inconclusive with regard to what the concept of privacy encompassed (Dworkin, 1973) it predicted that computers would constitute a privacy threat in the future. In 1976, Sir Norman Lindop was asked by the government to lead a committee on data protection. In 1978, in the resulting report, Lindop recommended the establishment of a Data Protection Authority, which would be in charge of the creation of codes of practice for different industries, but the recommendation was not enacted (Cooper et al., 1988). After 1978, international pressure for the UK to adopt privacy legislation grew as international flow of data increased and, in 1981, the UK signed the Council of Europe Data Protection Convention, which secure individuals' right to privacy over the automatic processing of their personal data (Cooper et al., 1988). To pass into law what had been agreed in the convention, the UK passed the Data Protection Act of 1984, which gave individuals the right to: (1) claim compensation in case of misuse of their personal data; (2) have a copy of their personal data; and (3) correct or erase erroneous data about them (Smith, 1994). The Data Protection Act was updated in 1998 (UK Data Protection Act, 1998) in an attempt to harmonise legislation across Europe, following the European Data Protection Directive of 1995 (European Commission, 1995).

The following sections discuss the two main criticisms made to the regulatory approach to privacy protection: the first is that its perspective is too much focused on strict definitions of what data items are sensitive or not; the second is that it requires individuals to notice when their privacy is invaded.

### 2.4.1 Data-centric view

The UK Data Protection Act of 1998 (UK Data Protection Act, 1998) has the stated goal of providing "*a framework to ensure that personal information is handled properly*" while the European Data Protection Directive of 1995 aims at removing the obstacles to the free movement of personal data while ensuring its protection (European Commission, 1995). They focus on defining what data items are considered personal or sensitive and which types of protections and provisions have to be in place in order to collect, process and transfer this data.

This data-centric approach to privacy and personal data protection (Raab and Bennett, 1998) has some drawbacks. First, it fails to consider the variations between individual perspectives and assumes static global definitions for complex concepts, such as personal data. Yet, how a data item is perceived varies from person to person. The *sensitivity* of the data depends on the context and how "*personally defining*" the data is perceived to be by the individual (Adams, 2001). This means that what constitutes a privacy invasion for one person may be an advantageous trade-off for another (Raab and Bennett, 1996). Second, it considers that all data is either public or private. However, the sensitivity of data is not a binary – private vs. public – decision; it varies along a continuum (Adams, 2001). Finally, the data centred perspective fails to address the fact that different populations are exposed to different types of risks. In the privacy legislation and policy, these nuances are not considered and individuals are simply abstracted as "*data subjects*" (Raab and Bennett, 1998; Adams, 2001). On the other hand, it should be noted that too much vagueness in the definition of privacy related concepts can also have adverse effects. Solove (2008) argues that the difficulty (or impossibility) in finding a single global definition for privacy has rendered US privacy law ineffective.

A related criticism of privacy regulation is the lack of input from citizens and customers in its development. This contributes not only to the issues described above, but also to a "*due process*" approach to identifying and solving privacy issues which does not address specific problems (Raab and Bennett, 1998). Solove (2008) attempts to address this issue by developing a privacy issues taxonomy where he enumerates several types of situations that people have shown to experience as privacy invasions in the past (see Figure 2.1).

### *2.4.2 Identifying privacy invasions*

The regulatory approach in the UK expects people to notice when their data is misused, and to formally complain. Privacy is protected through "*self-help*" (Raab and Bennett, 1996). However, individuals are often not aware that their data is being collected or processed which makes it very difficult for them to detect any privacy invasions. Contributing to this is the fact that companies are not obliged to report data losses or security breaches and they usually do not because of the impact it has on their reputation.

This issue is not exclusive to the UK. In a 1993 study, Smith (1993) described information policy development within US corporations as a cyclical process, where unofficial data usage practices are "*corrected*" or brought under internal regulation only when the organisations perceive an external threat, such as a media backlash or governmental scrutiny (see also Milberg et al., 2000). Even after policies are established, it is common to have a discrepancy between real practice and policy. This puts the burden of uncovering privacy violations on the "data subject", which also means that less educated and poorer populations will be more at risk since they will not know how to use the proper channels to investigate privacy violations or ask for redress. Stone (1975, cited in Smith, 1993) argues that, in order to successfully pressure business organisations:

- Consumers must be aware of an injury
- Consumers must know where to apply pressure
- Consumer must be in a position to apply that pressure
- The pressure must be capable of causing substantial change in the organisations

It should be noted that, even within the limits imposed by regulations, it is perfectly possible to develop massive personal data programs and systems (Raab and Bennett, 1998). The UK has currently millions of CCTV cameras which monitor the movements of its citizens 24 hours a day. The exact number is not known, but it is thought to be more than 4 million (Lewis, 2009). While many people consider it an invasion of their privacy, the system is legal and continues to grow.

## 2.5 Conclusions

This chapter starts by reviewing different factors that have been linked to privacy perceptions and behaviour. The perceived sensitivity of the data being requested, for example, has been linked, not only to privacy perceptions, but also to whether individuals disclose their personal data, and whether they lie or not when they do disclose it. However, most of the reviewed factors have only been associated with perceptions of privacy in general and, thus, it is not clear whether they affect disclosure decision-making. The research presented in this thesis attempts to link some of these factors to actual privacy behaviour (see Section 2.1.1).

The majority of past research on privacy factors has been conducted in the contexts of direct marketing and online interactions, such as e-commerce. Because privacy perceptions are interpreted as highly context dependent, attempts to make generalisations about how individuals think about it are rare. The research presented in this thesis goes beyond those classic interaction scenarios and explores privacy perceptions and disclosure behaviour in under-researched contexts (from a privacy perspective), such as: loan applications (Chapter 4:), serious games deployed in working environments (Chapter 5:); the UK census (Chapter 6:); while also looking at targeted advertising (Chapter 7:) and web forms (Chapter 9:). Surprisingly, many of the same privacy factors emerge in these different situations, suggesting that while privacy perceptions are contextual, maybe the decision-making process is not.

Individuals' self-reported concern with privacy issues does not always match their actual disclosure behaviour – i.e. study participants say they take privacy seriously, but then exchange personal data for small rewards. Some researchers attempt to explain this discrepancy by arguing privacy surveys have a biased design that prime participants to say they are concerned; others argue that the decision-making process itself of individuals is biased in such a way that, even if they want to protect their privacy, they cannot due to psychological distortions. A different explanation advanced is that the probability of personal data disclosure resulting in negative consequences is so low that adventurous disclosure behaviour is rational. The research in this thesis bypasses the *privacy paradox* problem, by not putting individual privacy concern at the centre of the decision-making process. Instead, it takes a qualitative approach to determining disclosure behaviour factors, which it then attempts to validate with actual observations of disclosure behaviour. This also avoids the methodological issue of measuring privacy concern.

When individuals perceive the costs of a disclosure to be higher than the benefits, they may engage in privacy protection behaviours, such as lying or omitting the data requested. Research on the likelihood of these behaviours or on the factors that lead to them is limited. This thesis attempts to link privacy perception factors to actual privacy protection behaviours and estimate how probable they are (Chapter 9:). This is important because it paves the way to link privacy perceptions to a quantified impact on data quality.

The multitude of privacy definitions and perspectives, make it difficult to address some real world privacy issues, not only from a legal point of view (see Section 2.4), but also when trying to design privacy sensitive systems (see Section 2.3.1). The lack of working, agreed upon definitions for privacy related concepts such as “control”, “transparency”, or “personal data” complicate the identification of privacy issues and gathering of privacy requirements. Privacy research also suffers from definitional issues and, in fact, has been criticised for mixing privacy with other problems, such as identity theft or spam (see Section 2.1.2). This complication is largely avoided in this research by focusing on how individual perceive data requests and how those perceptions shape their response. While privacy related concepts are expected to shape these perceptions and behaviour, this thesis is not limited to them. This research also rejects the data centric view that some data items are personal *a priori*. For the purposes of this thesis, only the individual’s perceptions of the data items matter.

In the next chapter (Chapter 3:) different quantitative and qualitative research methods commonly employed in privacy research are presented and their advantages and limitations discussed. The second part of the chapter justifies the choice of method for each study that is part of this thesis and describes how common limitations of privacy research were addressed.

# Chapter 3: METHODOLOGY

## 3.1 QUANTITATIVE AND QUALITATIVE RESEARCH

Quantitative research has its historical roots in the positivistic paradigm. The ultimate goal for positivists is the finding of universal laws to explain reality, through the identification of causal relations between things. They believe that knowledge can only be obtained through direct experience or observation and facts should be separated from values. According to this paradigm, science is almost exclusively based on quantitative data obtained through rigorous processes (Denzin and Lincoln, 1998; Robson, 2002). Post-positivism, however, acknowledges that the observer has an impact on that which is observed and that knowledge about reality is bounded by the researcher's limitations. Modern quantitative research is done under this paradigm (Robson, 2002). Quantitative research techniques include surveys and experiments.

Qualitative research was also initially carried out in line with the positivistic philosophy, albeit with more relaxed methods then quantitative research (Denzin and Lincoln, 1998). Modern qualitative inquiry, however, is strongly (but not exclusively) associated with constructivism, which sees reality as a social construction (Guba and Lincoln, 1998; Robson 2002). Qualitative researchers bring this social construction to their research by trying to capture multiple perspectives and emphasising the importance of the context in which data was collected and the influence of the relationship between researcher and object/subject of the research (Denzen and Lincoln, 1998; Robson 2002). Qualitative research techniques include interviews, focus groups and diary methods.

In the next sections different data collection and data analysis methods are discussed in the context of privacy research and in the context of the research presented in this thesis.

## 3.2 PRIVACY RESEARCH METHODOLOGY

### *3.2.1 SURVEYS*

Surveys "feel the pulse" of a specific population regarding a certain topic. Surveys have been used extensively in the study of privacy to explore:

- Individuals' concerns, attitudes and desire for regulation (FTC, 1998; Pew Internet and American Life Project, 2000; Jupiter Research, 2002);
- Individuals' attitudes towards data collection and use (e.g.: Adams, 2001, Berendt et al., 2005; Culnan, 1993);
- Factors that influence perceived value of personal data and willingness to disclose personal data (e.g.: Dinev and Hart, 2006; Horne et al., 2007; Lederer et al., 2003; Phelps et al., 2000);

- Privacy perceptions in organisations (Tolchinsky et al., 1981; Woodman et al., 1982; Millberg et al., 2000).

According to Robson (2002), surveys are defined by having a fixed and quantitative design; collecting small amounts of data from large numbers of people; and by being targeted at people who constitute a representative sample of some specific population. Advantages of surveys include the ability to question large numbers of people; its efficiency; statistical significance; simplicity; transparency and credible results (Iachello and Hong, 2007; Robson 2002). Robson (2002) however, argues that "*the reliability and validity of survey data depend to a considerable extent on the technical proficiency of those running the survey*". In fact, privacy surveys have been criticised for their flawed or manipulative design (Harper and Singleton, 2001), including:

- Starting off with provocative questions;
- Asking questions in a biased way;
- Mixing privacy with other issues such as spam and identity theft;
- Guiding participants' attention to risks they might otherwise not consider.

Another limitation of surveys is that they only measure attitudes and not behaviour; thus, their usefulness for public policy decisions or system design is limited (Robson, 2002; Iachello and Hong, 2007). In fact, studies comparing privacy attitudes and behaviour seem to indicate that privacy concerns in survey answers are exaggerated (Spiekermann et al., 2001). Surveys also commonly fail to consider that even people who are protective of their privacy may be willing to trade personal data for some kind of benefits (Adams, 2001). Finally, people who are more privacy sensitive are probably the ones more likely to refuse to answer questions (Paine, 2006), especially when asked by strangers, leading to a self-selection (exclusion) bias.

### *3.2.2 Interviews*

Interviews are usually conducted with a smaller group of people than surveys. Interviews are commonly categorized as structured, semi-structured or unstructured. In structured interviews the order and wording of the questions is fixed while in semi-structured interviews the order and wording of the questions can be changed and questions can be added or removed if the researcher deems it appropriate for a specific interviewee. Unstructured interviews are basically informal conversations about a defined but general topic (Robson, 2002).

Advantages of interviews include their flexibility, openness and adaptability. Face to face interviews can result in rich interactions and answers where the interviewer is available to pursue inquiry paths not initially planned and which may develop into new insights (Adams, 2001; Robson, 2002). In addition, it allows for the interviewer to gather secondary level information from the interaction such as body language or tone of voice which may have implications in the meaning of the message being conveyed by the interviewee (Adams, 2001; Robson, 2002). On the other hand, the flexibility of this data collection method comes at the expense of standardisation and consequently reliability (Robson, 2002). It is also difficult to avoid bias when researcher and interviewee are face to face and can see each other reactions and expressions. This bias will be bigger the larger the difference in economic status or age between interviewer and interviewee (Iachello and Hong, 2007). Interviews are time-consuming to develop, arrange, carry out, record and they also do not scale well. They do not address the issue that attitudes and behaviour may not match (a problem shared with surveys) and the information gathered is bounded by interviewees' ability for introspection and knowledge of the context or system (Robson, 2002; Iachello and Hong, 2007).

In privacy research, interviews have been used to study privacy perceptions in specific contexts (e.g.: Adams, 2001; Barkhuss and Dey, 2003); personal information disclosure attitudes and behaviour (e.g.: Olivero and Lunt, 2002; Razavi and Iverson, 2006); and also privacy perceptions in organisations (e.g.: Smith, 1993; Stone et al., 1983). Because they can be flexible and allow rich interactions to emerge, interviews are well suited for the study of complex and nuanced topics such as privacy. However, one particular difficulty of using survey-style methods of enquiry in privacy research is that individuals have difficulty thinking about privacy in the abstract (see Section 2.3.1), which harms the external validity of the findings.

### *3.2.3 Focus groups*

Focus groups are a type of interview where a group of people are asked to answer questions and engage in discussions on a specific subject. The group size is usually between 3 and 12 participants. The researcher assumes the roles of moderator and facilitator, i.e., making sure the discussion follows the script and is focused on the topic and that it keeps flowing. The groups can be composed of people with similar (homogeneous) or different (heterogeneous) backgrounds (Robson, 2002; Kontio et al., 2004).

The main goal of this research technique is for people to interact with each other in order to produce a rich outpour of ideas, opinions, attitudes and experiences. Focus groups are considered efficient, since it is possible to gather large quantities of insightful information from a group of people in a short period of time and they're not expensive to organise. Additional advantages include the fact that members usually like to participate and that extreme views are kept in check by the group. General limitations of focus groups comprise the difficulty in managing the discussion – avoiding conflicts or the emergence of dominating personalities, small sample sizes which make it difficult to generalise results and bias due to group dynamics (Robson, 2002; Kontio et al., 2004).

When researching privacy, the impossibility of maintaining confidentiality in a focus group (Robson, 2002; Kitzinger, 1995) is a particularly important issue. In fact, this is related to a more general – and paradoxical - issue of privacy research: to study perceptions of privacy and personal data researchers have to ask study participants to discuss sensitive topics openly, potentially making them feel their privacy is being invaded. In focus groups, this problem can be aggravated since participants have to talk about these issues not only with the researcher but also with other participants.  The opposite can happen, however. Kitzinger (1995) argues that, in a group situation, the "*less inhibited members of the group break the ice for shyer participants"*. Furthermore, *"participants can also provide mutual support in expressing feelings that are common to their group but which they consider to deviate from mainstream culture [...]."*

### 3.2.4 Diary methods

Diaries are used to capture information in their natural contexts and as substitutes for observation in situations where it is difficult or not desirable for the researcher to be present (Robson, 2002). One of the biggest benefits of these methods is that the report of an experience is very close in time to the actual experience. Participants both generate and record all the information themselves which is both good and bad. Since the researcher is not on hand to clarify questions diaries are open to misinterpretation and therefore require a great deal of training and briefing beforehand (Bolger et al., 2003). They are also very time consuming for participants and require a great deal of commitment (Bolger et al., 2003) which can in turn lead participants to want to please the researcher and thus bias the results (Robson, 2002). Diary studies can be combined with a follow up interview to allow researcher to clarify and collect additional information and therefore offset some of the potential bias introduced  (Rieman, 1996).

Diary studies can be time-based, such as *experience sampling methods* (ESM), or event-based (Bolger et al., 2003). Time-based designs consist in asking the participants to assess some specific experience or emotion at specific times according to either a fixed schedule (e.g.: every hour) or a variable schedule (e.g.: researcher randomly calling participant). In event-based designs the self-report is triggered by some event which was described in detail by the researcher when the participant is briefed.

Barkhuus and Dey (2003), for example, used a fixed schedule time-based diary (also combined with follow up interviews) for eliciting privacy concerns regarding location based services.

Consolvo et al. (2005) used an ESM design to investigate participants' replies to hypothetical requests for their location from individuals they knew. In this study, participants were given PalmOS PDAs and were sent 10 random questionnaires a day which asked where they were and what they were doing.

### *3.2.5 EXPERIMENTS*

Experiments are employed to investigate casual relationships between variables. Researchers manipulate the *independent or predictor variables* (e.g. number of personal data items requested in web form) to observe the effect of the manipulation on the *dependent or outcome variables* (e.g. completion of web form). Participants in the experiment are assigned to different experimental conditions by the researchers. The conditions differ only with regard to the independent variables, while the remaining variables are *controlled*, which typically means keeping them constant (Robson, 2002). The main criticism attributed to experiments and, in particular, laboratory experiments is their artificiality, which impairs their ecological validity. At the same time, the artificiality of the laboratory environment is exactly what allows variables to be controlled and manipulated and cause-effect phenomena to be isolated.

In the particular case of privacy research, the main challenge of experiments is to create situations where participants exhibit their real privacy behaviour. For that to happen, participants must perceive there is a real risk of suffering a privacy invasion (Iachello & Hong, 2007). For example, in an experiment investigating the effect of security warnings on user behaviour, Krol et al. (2012) asked participants to bring their own laptops, so that they would experience the security risk as real. Experiments on the economics of privacy take a similar approach and make participants trade their own money for privacy (e.g. Preibusch et al., 2013) or vary their reward depending on amount of disclosure (e.g. Hui et al., 2007). Another common practice in privacy research to increase the level of realism is to avoid mentioning that the focus of enquiry is privacy (Iachello & Hong, 2007).

### *3.2.6 QUALITATIVE DATA ANALYSIS*

#### 3.2.6.1 Grounded theory

Grounded theory consists in "*theory that was derived from data, systematically gathered and analysed through the research process*" (Strauss and Corbin, 1998). Grounded theorists avoid the generation and verification of hypothesis focusing instead on collecting data in the field related to a specific topic and waiting for the theory to "emerge" from that data. It is their belief that such a theory will be closer to reality – this method has post-positivist roots (Denzin and Lincoln, 1998) - than one derived from experience and speculation (Strauss and Corbin, 1998). Charmaz (2006) denies this view of an underlying reality opting for a constructivist perspective of grounded theory. Grounded theory has been criticised for lack of repeatability, for its subjective nature and for being complex to apply appropriately (Adams, 2001).

In grounded theory, analysis comprises the identification of categories and respective properties and dimensions and determination of relations between the concepts. This is accomplished by examining qualitative data segment by segment (words, sentences, etc.) and through the iterative phases of open coding, axial coding and selective coding (Strauss and Corbin, 1998). Open coding consists in conceptualising - labelling underlying phenomena (ideas, events, objects) present in the data as concepts; grouping concepts into categories; and finally identifying the properties and dimensions of each category (Strauss and Corbin, 1998). An example of a category could be "*surveillance*" with a property "*frequency*" with a dimensional range going from "*never*" to "*often*" (Adams, 2001). Axial coding is about relating categories at their dimensional level. The process of relating phenomena (the categories) is guided by the search for answers to the why, when, where and how of the phenomena. The goal is to identify conditions, actions/interactions and consequences pertaining to a phenomenon (Strauss and Corbin, 1998). For example: "high peer pressure" (conditions) lead to "soft drugs consumption" (action) which in turn causes someone to "get stoned" (consequence) (based on Strauss and Corbin, 1998). Finally, selective coding is an iterative phase where the theory is refined and integrated. This is done by identifying a main category (phenomenon) on which all others are anchored and which has a big influence in the others' variations. Around this category a story can be written which explains what is happening in general terms. If the story seems to capture the essence of the research it is then rewritten with the inclusion of the other categories. This theory is then validated internally (looking for logic gaps) and externally (seeing if it fits with all the data) (Strauss and Corbin, 1998).

Grounded theory has been employed in the study of privacy to investigate privacy perceptions in multimedia communications (Adams, 2001); willingness to disclose personal data in e-commerce exchanges (Olivero and Lunt, 2001); personal information disclosure behaviour in personal learning spaces (Razavi and Iverson, 2006) among others. Grounded theory's flexibility in allowing participants perspectives to emerge from the data during analysis (Olivero and Lunt, 2001) makes it a good candidate method to study individual perceptions of concepts such as "privacy", "personal data", "sensitive data" or "value". Furthermore, by avoiding the statement of hypothesis, it is easier to approach new or seldom studied research topics.

##### *3.2.6.1.1 Thematic Analysis*

Thematic analysis is commonly used in qualitative research, but not clearly defined. In fact, thematic analysis is part of most qualitative data analysis methods and, as such, can be interpreted as a technique for coding qualitative data more than a method in itself (Braun & Clarke, 2008). Braun and Clarke (2008) define thematic analysis as the identification of *themes*, or patterns of interest, in the data that are relevant to answer the research questions. The researcher systematically tags interesting parts of the data with a code and then groups related codes in themes. In this respect, thematic analysis seems to be remarkably similar to the open coding phase of grounded theory, where codes are grouped into categories. However, thematic analysis does not continue on to find the dimensions of these themes or categories, making it a faster method to apply. Thematic analysis can be inductive (*bottom-up*), or theory-driven (*top-down*).

#### 3.2.6.2 Discourse analysis

The main focus of discourse analysis is people's use of language to perform specific social functions like persuading, blaming, or justifying. Discourse analysts reject the view that language is an indicator of underlying cognitive processes, such as attitudes or beliefs, and instead argue that when a person is employing language he or she is constructing versions of the social world. This construction is made clear through the variation of language, i.e., individuals' accounts will vary depending on the purpose of the discourse. However, this is not necessarily done in a conscious way (Potter & Wetherell, 1987).

The construction of versions of events draws on pre-existing linguistic resources. By using some resources and not others, linguistic versions are built which perform specific functions (Potter & Wetherell, 1987; 1994; 1995). One such type of linguistic resources are *interpretative repertoires*. Interpretative repertoires are sets of related terms organised around a central metaphor which evolve with time and are *"part of the 'common sense' of a culture"* (Potter, 1996).

In computer science, discourse analysis has been used to capture the interpretative repertoires users employ when talking about network applications in order to build a lexicon which could be used in the design of future applications (Rimmer et al. 1999). Weirich (2006) used discourse analysis in a similar fashion in order to identify the interpretative repertoires that individuals relied on to describe phenomena related to password security. His goal was to find out which repertoires were associated with desired password practices and undesired password practices and use this knowledge to design security campaigns which reinforced the desired practices.

Despite the potential usefulness of interpretative repertoires for system and campaign design, the identification of this kind of resources is not the main focus of discourse analysis. Discourse analysis goes beyond the identification of repertoires and tries to understand how specific social functions are achieved through discourse and which devices and procedures are used to build factual versions of the world (Potter, 1996).

Due to its contextual nature, privacy research lends itself to the use of discourse analysis. Vasalou et al. (2010) analysed language datasets containing privacy-related discourse from multiple sources. These transcripts were parsed by privacy experts who identified which words were related to privacy. These words and the contexts in which they appeared were successively refined to yield a privacy dictionary aimed at facilitating automatic content analysis in privacy research. Bodea et al., (2013) employed discourse analysis to the conceptualisation of privacy and security in UK, the Netherlands, and EU policy documents. In the UK analysis, for example, they concluded that the government was more aligned with the discourse of "balancing privacy and security", while civil society actors were more aligned with privacy protection discourse.

## 3.3 Methods Used in This Thesis

### *3.3.1 Use of Qualitative and Quantitative Methods*

The complex nature of the concepts involved in the study of privacy and human decision-making suggests that an exclusively quantitative approach would not be appropriate for this thesis. Moreover, different contexts of interaction and individual-organisation relationships are investigated, some of which have seldom been studied from a privacy perspective (e.g. loan applications or serious games). Qualitative methods, like interviews and grounded-theory, are more appropriate in these situations, i.e. when research is exploratory in nature and the goal is to identify phenomena and generate possible explanations for them (Robson, 2002). In this thesis, they are used in the initial capture of individuals' perceptions of the collection and use of their personal data and in understanding how they decide to comply or not with organisational data practices.

Quantitative methods are more adequate when attempting to identify and validate causal relationships between factors (Robson, 2002). In this thesis they are used to quantify and compare how different types of data are perceived (e.g. measuring the perceived sensitivity of different data items – see Chapter 4: and Chapter 6:) or validating whether certain factors have an actual impact on disclosure and privacy protection behaviours (e.g. likelihood of falsification of answers given an increase in perceived irrelevance of a data request – see Chapter 9:).

The combination of both qualitative and quantitative research methods has several advantages (Bryman, 2006). First, it allows the triangulation of findings from different methods to be cross-validated resulting in an increased validity of the research. Second, a more complete understanding of the phenomena under study can be obtained because research is conducted from multiple perspectives. Third, the weaknesses of qualitative methods are offset by the strengths of quantitative ones, and vice-versa. Fourth, the findings from one method can be explained by another method. For example, experiments can tell researchers how one variable affects another, while interviews could shed light on why the relationship exists.

### *3.3.2 Addressing Limitations of Past Research*

#### 3.3.2.1 Interviews

Different types of interviews were conducted as part of this thesis. In Study 1 in Chapter 4: (Section 4.3), semi-structured interviews were done with experts of personal finance and credit risk assessment. Privacy in loan applications is an under-researched topic and, as such, a research method that would generate rich data and allowed a broad view over the problem space, as is the case of semi-structured interviews, was considered appropriate. As these were expert interviews most of the limitations of qualitative privacy research did not come in play. The interviews allowed the identification of interesting privacy related phenomena and generate research questions to pursue in future studies.

Group interviews were conducted in Studies 1 and 2 of Chapter 5: (Sections 5.2 and 5.3). The goal of these studies was identifying privacy risks of a system that was in the early stages of development. The main limitation of group interviews when used in privacy research is that participants are asked to discuss sensitive topics in front of other people. This limitation did not apply to the first study since it was carried out with developers of the system. In the second study, confidentiality and sensitive topics discussion were less of an issue, albeit still relevant, because the participants were trying to anticipate the privacy concerns that end-users would have and not openly stating their own concerns. As a result, it was considered that the advantages of quickly collecting a rich set of perceptions about the system outweighed other methodological concerns.

Study 3 of Chapter 5: (Section 5.4) consisted of a series of semi-structured interviews with participants who fitted the profile of future users of the system being developed. As in the previous two studies, the goal was to identify potential privacy issues related to how the system collected and processed personal data of its users. One limitation of privacy sensitive design is eliciting privacy requirements in the abstract, i.e. participants are asked to discuss privacy concerns in a de-contextualised environment (see Section 2.3.1). This limitation was addressed by: (1) showing participants a video-demo of the system in action before the interview; (2) asking questions in the context of scenarios that depicted potential data flows in the system; and (3) asking participants to assume the system would be deployed at their workplace. While bridging the gap between the abstract and the concrete, this study still asked participants to answer to hypothetical scenarios and, as a result, excessive abstraction was still a limitation. However, this is unavoidable when the actual system being studied does not yet exist.

Lack of contextualisation was less of a limitation in Study 1 of Chapter 6: (Section 6.2). Participants were interviewed about their perceptions of the UK census of 2011 while filling in the actual census form.  The artificiality of the lab environment, however, can have a negative impact on the external validity of the findings. To address this limitation, an online questionnaire using a national representative sample of the UK was conducted as a follow-up of this study. This and other questionnaires carried out in this thesis are discussed in the next section.

#### 3.3.2.2 Surveys

Online surveys were used in this thesis for several reasons. Surveys allow the inquiring of large samples of individuals, increasing the chances of detecting medium and large sized statistical effects (Cohen, 1992) In the Studies 2 and 3 of Chapter 4: (Sections 4.4 and 4.5), the use of surveys was appropriate to collect quantitative data on the sensitivity and perceived effect of disclosing different data items and for exploring the relationship between these two variables. Moreover, surveys are a good solution when asking sensitive questions, such as the questions related to debt or financial exclusion as was the case of Study 4 in Chapter 4: (Section 4.6). Individuals may not feel at ease discussing their experiences face to face or by phone and may feel more comfortable answering an online survey anonymously. Finally, online surveys scale well, allowing the concurrent inquiring of many participants at the same time. This is particularly advantageous when it is important to collect answers on a timely topic, such as perceptions of the UK Census of 2011 (Chapter 6:).

Privacy surveys have been criticised for having a biased design and leading participants to reveal an inflated concern for privacy (see Section 3.2.1). To limit the biasing of participants, the word “privacy” was avoided both in recruitment and throughout this thesis’ surveys. Instead, these surveys were framed as studies on perceptions of data requests. Moreover, abstract attitudinal questions were avoided. Instead, questions were focused on participants’ comfort with disclosure of concrete data items to a specific data receiver within a determined context. For example, in Study 2 of the Chapter 6: (Section 6.3), participants were asked how comfortable they had felt answering each of the census questions four weeks after the census deadline.

#### 3.3.2.3 Experiments

As mentioned before in this chapter, both interviews and surveys rely on self-reports and, as a result, capture only attitudes and not actual behaviour. This is a particularly serious weakness in privacy research since there is indication that privacy attitudes and behaviours do not match (see Section 2.1.2). To address this limitation, laboratory and field experiments were conducted to confirm findings based on self-reports and increase their validity.

A criticism of laboratory experiments in general, and privacy experiments in particular, is their artificiality (see Section 3.2.5). To address this limitation, deception and a real financial reward were used in Study 5 of Chapter 4: (Section 4.7). In this study, participants were told they would be more likely to get an additional monetary reward if they disclosed more data and were honest in those disclosures. Moreover, participants (and experimenters) were told they were part of a commercial study for a real bank looking into new ways to assess credit worthiness and that all their answers would be sent to that bank. The goal was to simulate the disclosure behaviour in loan applications where participants have a strong incentive to disclose all the data items that are requested by the lender.

Also, to avoid the lower external validity of laboratory experiments, the final validation study of this thesis (Chapter 9:), consisted of a field experiment involving deception and a website featuring a professionally designed layout and logo. Participants were unaware they were part of a study looking at their disclosure behaviour and were told their answers would be sent to a credit card company to be used for a market study.

| **Limitations Addressed** | |
|---|---|
| **Limitation** | **Improvement** |
| Reliance on self-reports | Laboratory and field experiments |
| Artificiality of lab-setting | Deception and field experiments |
| Biased survey design | No mention of privacy focus; neutral questions; contextualised questions |
| Discussing privacy in the abstract | Contextualisation through demos; scenarios; artefacts (e.g. census form) |
| **Limitations Accepted** | |
| Self-selection bias | |

**Table 3.1: Limitations of past research**

# Chapter 4: Applying for Credit

## 4.1 Introduction

It is in both the interest of lenders and the borrowers that debt repayments remain affordable. Credit can improve the lives of individuals. Borrowing to buy a car, for example, can allow someone to take on a job that pays better but is further away from home. However, if borrowers take on debt they cannot repay they will fall into financial hardship. In the UK, 331 people are declared insolvent or bankrupt every day (Credit Action, 2011). Lenders also want borrowers to remain able to make their regular repayments throughout the length of the loan to protect the profitability of their business and allow them to lend to more people.

For this reason, lenders collect and process personal data of loan applicants to try to determine how likely they are to default on the loan. These data can be collected directly from applicants through a loan application form – online or on paper – or from organisations like credit reference agencies that maintain records of debt repayment history for a large proportion of the market. These data is then processed by credit scoring algorithms, which calculate the level of risk associated with lending to a particular applicant. Applicants whose risk is above a certain threshold are denied the loan. Denying loans to applicants that are too risky should ensure that the business remains viable and that applicants are not drawn into financially fragile positions. To improve the accuracy of the risk assessment process, lenders look to update their credit scoring algorithms by collecting more types of data and linking it in different ways.

While more or less sophisticated loan application processes have existed for some time, applicants' perceptions of the collection, use and transfer of their data for this purpose have been under-researched. There are several reasons that make these perceptions unclear. First, applicants are usually in a weak bargaining position when asked by the lender to disclose certain data items. It is possible that the perceived benefits that the loan has for the applicant will override any potential privacy costs associated with the disclosure making most applicants disclose anything they're asked. This, however, does not mean that applicants do not experience discomfort when answering these data requests – i.e. would prefer not to answer - nor that they will not engage in privacy protection behaviours – e.g. omitting or falsifying data. Second, the risk assessment process undertaken by lenders is purposefully obscure as to prevent applicants from manipulating it. This lack of transparency makes it difficult for applicants to determine the consequences of their disclosure or the relevance of certain questions. Third, the data that applicants disclose is only part of the data used by lenders to assess their risk. Credit reference data can, in fact, have a bigger impact on the decision to lend than data voluntarily disclosed by the applicant.

The studies described in this section aim to fill this gap in research and investigate how loan applicants perceive data requests from lenders and how those perceptions affect their disclosure behaviour. The next section provides some background information on the collection and use of personal data in credit scoring, issues of data quality in credit scoring, and relevant privacy research. The studies that were carried out on this topic are then presented in chronological order (see Table 4.1). In Study 1 (Section 4.3), 10 experts of personal finance and credit scoring were interviewed to explore the motivation lenders to collect and use specific personal data items and potential privacy issues in the loan application process. Studies 2 and 3 (Sections 4.4 and 4.5) focused on the impact of perceived *sensitivity* and *projected image* on attitudes towards disclosure of personal data in this context. Study 4 (Section 4.6) investigated applicants' experiences of being denied credit and, in particular, instances where participants had not applied for credit due to the data being requested by the lender. Study 5 (Section 4.7) consisted of an experiment with the aim of observing actual disclosure of personal data in the context of a simulated credit application and determining which factors influenced disclosure.

| | **Applying for Credit** | | | | |
|---|---|---|---|---|---|
| | **Study 1** | **Study 2** | **Study 3** | **Study 4** | **Study 5** |
| **Section** | 4.3 | 4.4 | 4.5 | 4.6 | 4.7 |
| **Topic** | Personal data in risk assessment | Loan applications data requests | Loan applications alternative data requests | Collection and use of personal data by lenders | Loan applications alternative data requests and disclosure behaviour |
| **Method** | Semi-structured expert interviews | Online survey | Online survey | Online survey | Lab experiment |
| **N** | 10 | 283 | 285 | 298 | 48 |
| **Date** | Jun 2009 – Aug2010 | Aug – Sept 2010 | Aug – Sept 2010 | Aug – Sept 2010 | Mar 2011 |

**Table 4.1: List of Studies in this Chapter**

Studies in this chapter were designed and conducted in collaboration with Dr. Charlene Jennett and Dr. Sacha Brostoff. In Study 1 (Section 4.3), interviews were planned and carried out by the author and Dr. Sacha Brostoff and analysed by the author. Studies 2, 3, and 4 (Sections 4.4; 4.5; and 4.6 respectively) were planned by Dr. Sacha Brostoff, Dr. Charlene Jennett, and the author. The author implemented the three corresponding online questionnaires. Data analysis was done by the three researchers. Results were re-framed or re-analysed by the author for the purpose of this thesis. For example, in Study 4, qualitative answers were re-coded in light of the research goals of this thesis. Study 5 (Section 4.7) was designed by Dr. Sacha Brostoff, Dr. Charlene Jennett, and the author. The author designed the website used in the experimental setup. The experiment was conducted by undergraduate UCL Psychology students Madalina Vasilache, Diana Franculescu and Jessica Colson. All results were analysed by the author.

## 4.2 Background

The process of credit scoring, which consists in trying to predict how likely someone is to repay a debt, has existed since the 1940s. Initially, it relied on what was called "The 5 Cs":

> *"The character of the person – do you know the person or their family?*
>
> *The capital – how much is being asked for?*
>
> *The collateral - what is the applicant willing to put up from their own resources?*
>
> *The capacity – what is their repaying ability. How much free income do they have?*
>
> *The condition – what are the conditions in the market?"*
>
> *(Thomas, 2000)*

When an individual applied for a loan, the credit analyst would use his best judgement to assess these five factors based on the application form and what he knew of the applicant.

Modern credit scoring is done by statistical algorithms that process data from three main sources to assign a risk level to the applicant: loan application form data; data relating to the applicant's past business with the lender; and the applicant's credit report obtained form a credit reference agency (RBS, 2011). These algorithms compare an applicant's data to the data of past borrowers and infer the risk of the applicant defaulting from the proportion of similar borrowers who defaulted before (Collard and Kempton, 2005; Jentzsch, 2010). Evidence suggests these algorithms are better than human analysts at predicting debt repayment behaviour (Thomas, 2000). Moreover, they are more consistent, efficient, and less biased than humans.

However, there are several issues that limit the performance of credit scoring algorithms. First, data quality issues can impact how well the algorithm is at classifying applicants and may lead to good risks being considered bad and vice-versa. The statistical models underlying the algorithms are trained only with data from applicants who were given loans (no data exists if the applicant is not converted into a borrower). This is a problem called reverse-inference (Hand, 2001) and could be attenuated by providing loans to a sample of applicants who are thought to be bad risks and observe how they fare. This is something that is rarely done, though. Second, human behaviour changes with time and diminishing the predictive power of some variables or outdating their relationships. Finally, some determinants of bankruptcy are difficult to predict, such as divorce, health problems, or unemployment (Jentzsch, 2007).

To tackle these limitations, statisticians try to update their models regularly. This can be done by changing the way variables are weighed and linked or by collecting more types of data. The latter is seen as the approach with the most potential for improvement. However, the increased collection of personal data for the purpose of credit scoring can only exacerbate applicants' feelings of privacy invasion. The extent to which this could negatively affect the quality of the data provided or service drop out is unknown. It is also unknown which factors affect applicants' perception of the loan application forms. A better understanding of - the under-researched phenomena of - privacy attitudes and personal data disclosure behaviour in the context of credit scoring - could help design more privacy sensitive loan application procedures while maximising data quality provided to the credit scoring algorithms.

## 4.3 Study 1: Expert Interviews

### *4.3.1 Aims*

10 interviews were conducted with experts in personal finance and credit risk assessment (see Table 4.2). The aim of these interviews was to explore the problem space surrounding the use of loan applicants' personal data by lenders for risk assessment purposes. This was approached from two sides: the applicant's and the lender's. On the applicant's side the goal was to understand the expert's views on how applicants perceive the questions in loan application forms: which factors affect their perceptions of specific questions; whether they perceive feelings of privacy invasions; how they behave when they experience such feelings. On the lender's side the focus was on which personal data items they were interested in collecting and why.

| Expert | Role | Organisation | Interview Date |
|---|---|---|---|
| E1 | PhD Student studying personal experiences of debt | University | 23 June 2009 |
| E2 | Partnership Development Manager | Charity | 30 July 2009 |
| E3 | Consultant Lawyer | P2P Lender | 19 August 2009 |
| E4 | Creditor Liaison Policy Officer | Charity | 4 September 2009 |
| E5 | Risk Management Consultant | Regulatory Body | 28 September 2009 |
| E6 | CEO | P2P Lender | 29 September 2009 |
| E7 | Psychologist / Writer | N/A | 19 March 2010 |
| E8 | Professor / Head of Statistics | University | 27 April 2010 |
| E9 | Manager | Credit Union | 14 May 2010 |
| E10 | Professor in Accounting | University | 19 May 2011 |

**Table 4.2: List of Expert Interviews**

### *4.3.2 Method*

Interviews were semi-structured due to their exploratory nature, but different for each interviewee because of their different expertise and experiences. Interviews lasted between one and two hours. They were transcribed by the researchers. Thematic analysis (see Section 3.2.6.1.1) was used to analyse the data.

### *4.3.3 Findings*

While analysis of the interviews provided a range of insights on issues related to personal debt management and financial and social exclusion in this section only the findings relevant to this thesis are presented. The focus is, therefore, exclusively on what drives financial organisations to collect specific data items and which factors affect how individuals perceive loan application forms. 8 relevant themes were identified.

#### 4.3.3.1 Theme 1: Predictive Power

Scorecard models are based on data from the last 10 years and because of this they end up degrading, i.e. they become progressively worse at predicting behaviour because people do not behave in the same way. Thus, lenders are always trying to find new ways to improve the accuracy of their risk assessment process. This can be done by collecting additional data or by using existing data and combining it in different ways. Data items that have the most *predictive power* are considered to be the most valuable by lenders and credit reference agencies. Behavioural data like credit card spending is considered to be more predictive than application form data because it is harder to falsify and is dynamically generated in real-time (E5 and E8).

While borrowers generally want to understand how the credit rating system works and which data items are more important, lenders want to keep the risk assessment process obscure, so that borrowers cannot manipulate it to appear better risks than what they really are (E6).

Debt collection agencies have data warehouses that they mine to find the debtors they are more likely to be able to collect money from. Debt collection agencies have proprietary algorithms to make this selection based on data such as court appearances, post-codes, credit reports, and missing payment data (E1).

There are personal details of an individual that, while potentially connected to financial risk, are not collected by borrowers. An individual's relationship with his parents, how his parents dealt with money, self-esteem issues, and experiences of loss while growing up may all affect how he manages his finances later on life (E7). While current credit scoring models are entirely empirical, there is a chance models could be theory-based in the future (e.g.: based on behavioural psychology) (E8). These personal data items are intuitively too sensitive to ask, but there is a possibility that other, not so invasive, details could be used by financial excluded individuals to prove their ability to repay loans.

#### 4.3.3.2 Theme 2: Projected Image and Predicted Outcome

Applicants want to disclose items that they think will make them appear to be a good risk. They like to talk about things they are proud about. They may even want to disclose more data than what is being asked of them if they thing that will improve their chances of getting a loan. Some questions in a loan application form at a P2P lender were added to manage the applicants' perception of the form, but were not actually used for risk assessment (e.g.: additional income). (E5 and E6).

#### 4.3.3.3 Theme 3: Data Receiver

According to E1, individuals who are in debt management are more worried about friends and family knowing they have financial problems than strangers, like researchers. This is related with the previous theme, *projected image*, and has been identified in past privacy research: Adams (2001) notes that individuals are more uncomfortable disclosing negative data to people they know than to people they do not know.

There is a risk of financial data leaking when financial institutions call their customers at home. If someone other than the customer answers the phone they could find out the customer is in financial difficulty, for example. Because they do not know whether the customer shares their financial circumstances with family members, financial institutions are careful to make sure they are talking to the right person when they call (E3). Customers are also sometimes annoyed by these calls; however, they may appreciate offers for help if they are struggling and looking for assistance  (E4). This could make customers reluctant to share their phone details.

#### 4.3.3.4 Theme 4: Perceived Relevance

Some data items cannot be collected even though lenders think they had good predictive power because they are not perceived as relevant by borrowers. One example of this is car make, model and colour, which were tested by a P2P lender to assess risk and found to have good predictive power. Borrowers have to be able to understand the purpose of a question (E5 and E6).

Other questions are included in the application form to purposefully mislead the applicant on how the credit scoring system works (E5) to prevent gaming of the system. In this case, the questions may have perceived relevance when in fact they are not relevant (e.g. additional income is not actually an important data item to establish credit worthiness) (E6).

#### 4.3.3.5 Theme 5: Falsifying and omitting data

Some questions are not perceived by loan applicants as acceptable. To determine how acceptable a question is lenders monitor: the omission rate, the number of people who answer “Other”, and how well answered the question is (E5).

Because applicants can lie on application forms it is important to have a high number of verifiable data items.  Brokers that are trying to increase the chance of their client getting a loan can also falsify some of the data in the form (E5).

Applicants sometimes lie when asked about income. Unless the number is very large it is difficult to detect the lie (E6).

#### 4.3.3.6 Theme 6: Automatic vs. manual processing of data

Borrowers of the P2P lender interviewed have the perception that lending decisions are made by a human when in fact they are automated by an algorithm. This false perception, however, leads to higher levels of trust in the lender (E6).

#### 4.3.3.7 Theme 7: Effort

The P2P lender interviews tries to keep application forms short and easy to fill in to improve the experience of the applicants filling it in (E5 and E6).

The credit union manager interviewed mentioned that around 10% of their customers will be unhappy going through the application process because of the effort involved in answering all the questions. For some people it is difficult to get all the data needed, such as bank statements for the previous three months, which they will have to go and ask their bank (E9).

#### 4.3.3.8 Theme 8: Cost of collecting and using personal data

In the UK, large-scale personal data collection programs are often seen by governments as the answer to varied issues of public safety (e.g.: child safety). Because these public programs have a legal right to request data without bearing the costs and because the main goal of the program is often only to create the perception in the public that the real problem is being addressed, the benefits of holding the data are not considered (E10). The costs associated with these efforts include the costs of collecting the data and transferring to a central database borne by the organisations doing the collecting, privacy costs borne by the individual from whom the data is being requested, and the potential impact of data breaches borne by both organisations and individuals (E10).

## 4.4 Study 2: Perceptions of Loan Application Data Items

### 4.4.1 Aims

An online questionnaire was developed to investigate individuals' perceptions of data requests in the context of a loan application. The aim of this questionnaire was to: (1) determine which loan application data requests individuals feel most and least comfortable disclosing to lenders; (2) further explore the theme of *projected image / predicted outcome* identified in the interviews of study 1 and related it to comfort with disclosure; and (3) investigate which factors shape attitudes to loan application form questions from the perspective of the individuals answering the questions. While the personal finance experts in the previous study had provided some hints on how applicants perceive some of the questions, their perspective of how individuals perceive loan applications was indirect. In this study, the goal was to directly inquire a sample of the UK population about these matters.

### 4.4.2 Method

The open source survey creation tool Limesurvey[1] was used to create the questionnaire. The questionnaire had three sections and took approximately 15 minutes to complete. The first section asked participants weekly net household income and the household composition (number of adults and children) in order to calculate their annual equivalised income, before housing costs, according to OECD scales (Eurostat, 2012). The equivalised income is a standardised measure of income that takes into account number of dependents. It this study, it was used to contextualise the questionnaire scenario. Participants were asked to imagine they were applying for a loan of £500, £2000, or £5000. The loan amount they were asked to imagine depended on their equivalised income. 46 participants were asked to imagine a loan of £500, 148 of £2000, and 89 of £5000.

[1] "Limesurvey." http://www.limesurvey.org/

In the second section of the questionnaire, participants were shown a list of 59 questions that are part of a loan application form[2]. Items asked included "employer's name", "title", or "monthly income". Participants were asked to rate[3] how *comfortable they felt disclosing* each of these items if they were applying for a loan of the amount shown in the questionnaire: "How would you feel about the lender having each of the following pieces of information about you, in order to process your loan application?" They were then asked to briefly describe in writing in a text box why they had rated the items as they did. Participants were never asked to disclose the actual data items, just rate their perception of them. A 5-point Likert scale was used (as opposed to a 7-point one) because of the high number of items participants were asked to rate.

In the third and final section of the questionnaire, participants were again shown the same list of 59 items, only this time they were asked to rate[4] how answering each item would affect their chances of getting a loan (*projected image / predicted outcome*): "For each item, think about what kind of answer you gave (or would have given if you had answered). Then rate whether you think your answer would show you in a positive light or a negative light to a lender." As before, participants were asked to briefly discuss why they had answered the way they did in an open text box.

A nationally representative sample of 375 participants was recruited via a market research company called e-Rewards[5]. The only recruitment criterion was that participants had to be over 18 years old. Each participant was rewarded for completing the questionnaire. 92 questionnaires were excluded due to incomplete or non-sense answers in the open questions (e.g. writing gibberish in response to open questions, sticking to the default responses only). The final sample of 283 participants was comprised of 107 males and 176 females. In terms of age categories, 35 were "under 25", 83 were "25-39", 109 were "40-59" and 56 were "60 and over". 75% of participants had experience of applying for credit.

[2] These items were based on a Royal Bank of Scotland loan application form.

[3] 1="Very Uncomfortable", 2="Uncomfortable", 3="Neutral", 4="Comfortable", 5="Very Comfortable"

[4] 1="Very Negative Light", 2="Negative Light", 3="Neutral Light", 4="Positive Light", 5="Very Positive Light

[5] The company was rebranded as "Research Now" meanwhile: www.researchnow.com

### *4.4.3 Findings*

#### 4.4.3.1 Comfort with disclosure

Table 4.3 shows the mean comfort ratings for the data requests that participants found least and most comfortable. “Not applicable” ratings were excluded on an item-by-item basis. The data items that participants were most comfortable disclosing were: (1) title; (2) currently living in the UK; (3) first name; (4) surname; (5) gender. It is likely that participants perceived these items as having low sensitivity because they are used to disclosing them: all of these items are commonly asked in administrative forms. Furthermore, they are related to the public identity of the participants and are difficult to hide.

The items that participants were least comfortable disclosing were: (1) work phone number; (2) value of other assets; (3) total balance of investments; (4) total savings balance; and (5) mobile phone number. Three of these items are financial data, while the other two are means to contact the individual. Financial data has been identified in past research as one of the types of data individuals feel less comfortable disclosing (Phelps et al., 2000).

Regarding the sensitivity of phone numbers, the open answer responses of some participants suggest participants were afraid to be contacted at inconvenient times or that their number would be passed on to other organisations for marketing purposes. One participant, for example, reveals that s/he is:

> *“Happy giving general information about my finances, do not like to give work details as I work in an open plan office and everyone would be able to hear my personal details on a telephone call.” P210*

While another participant said:

> *“I am fairly comfortable with giving most information, they need it to do their job and work out if you are a risk. The thing I hate the most is if then afterwards my details are passed on and I get unsolicited emails/phone calls.” P166*

These findings are in accordance with past privacy research saying that data items have different levels of sensitivity (see Section 2.1.1.1).

| Data Item | mean | s | N |
|---|---|---|---|
| Work phone no. | 2.50 | 1.20 | 228 |
| Value of other assets | 2.64 | 1.17 | 283 |
| Total balance of investments | 2.69 | 1.20 | 277 |
| Total savings balance | 2.75 | 1.24 | 280 |
| Mobile phone no. | 2.99 | 1.17 | 270 |
| Gender | 4.22 | 1.07 | 283 |
| Surname | 4.23 | 1.11 | 283 |
| First name | 4.25 | 1.11 | 283 |
| Are you currently living in UK (Y/N) | 4.25 | 1.04 | 281 |
| Title (Mr., Ms., etc.) | 4.32 | 1.06 | 283 |

**Table 4.3: Comfort ratings for loan application data requests (Sample: 5 most and 5 least comfortable items)**

#### 4.4.3.2 Participants are more comfortable disclosing items that show them in positive light

To determine whether data sensitivity is affected by how individuals perceive that answering the question will make them look to the lender, *comfort* and *projected image* ratings were compared (see Table 4.4). Pearson correlations between these two variables were positive and significant ($p<0.05$) for 56 of the 59 data requests (no significant correlation was found for "Surname", "First name", and "Middle name"). Effect sizes varied between small ($r = 0.12$) and close to large ($r = 0.43$) This suggests that, when participants perceive that a data item would show them in a positive light they felt more comfortable disclosing it to a lender, and when the item showed them in a negative light they felt less comfortable. An open answer from one participant illustrates this relationship:

> *"[I'm] not so comfortable with them knowing how much I have saved in case they decide not to give me a loan." P219*

This lends support to the finding in Study 1 (see Section 4.3.3.2) which indicates that applicants want to disclose items which will increase their chances of obtaining a loan. Generalising, it suggests that attitudes towards disclosure of personal data depend on *projected outcome* and *projected image* associated with the disclosure.

| **Data Item** | ***p*** | **Pearson's correlation (r)** | **N** |
|---|---|---|---|
| Monthly mortgage | <.001 | 0.43 | 240 |
| How much overdraft do you have | <.001 | 0.41 | 258 |
| Date of starting job | <.001 | 0.41 | 248 |
| Balance of all credit cards | <.001 | 0.40 | 270 |
| How will you be paid | <.001 | 0.38 | 272 |
| How often are you paid | <.001 | 0.37 | 268 |
| Mortgage outstanding on other properties | <.001 | 0.36 | 186 |
| Currently a taxpayer (Y/N) | <.001 | 0.36 | 275 |
| Mortgage outstanding | <.001 | 0.36 | 224 |
| Preferred type of cheque book | <.001 | 0.35 | 272 |

**Table 4.4: Correlation between comfort and projected image ratings (Sample)**

#### 4.4.3.3 Theme 1: Projected Outcome

Some of the items participants were least comfortable disclosing were work phone number and mobile phone number. Three reasons were mentioned in the open text boxes for their discomfort. First, they were concerned they would be contacted at awkward times. Second, they were afraid the number would be passed on and used for telemarketing. Third, they did not want their employer to be called about their loan.

The fear individuals have of the negative consequences of disclosing an item of personal data seems to influence their attitude towards that disclosure. This finding supports Theme 2 in Study 1 (see Section 4.3.3.2), where it was suggested that the *projected outcome* of a disclosure affects how individuals perceive it.

#### 4.4.3.4 Theme 2: Perceived Relevance

Participants mentioned they considered some questions had little or no relevance. For example:

> *"Least comfortable with questions about other assets / savings which aren't immediately relevant in my view." P144*

This suggests that the *perceived relevance* of a data request affects how it is perceived by data subjects, with requests perceived as less relevant being seen more negatively. This is in agreement with Theme 4 of Study 1 (4.3.3.4). Relevance refers to the relationship between a data request and the context where it is being made. When a data item is transferred and used away from the context in which it was collected it loses relevance and there is a bigger potential for privacy invasions (Adams, 2001; Nissenbaum, 2004). The theme of perceived relevance has also been identified in the literature, albeit in other contexts (see Section 2.1.1.2).

## 4.5 Study 3: Perceptions of Alternative Loan Application Data Items

### *4.5.1 Aims*

The main goals of this study were: (1) to investigate how acceptable requests for 53 unconventional personal data items were perceived to be; and (2) verify whether the relationship between *comfort* and *projected image* holds with items different from the ones used in the previous study and with a different sample. It was highly unlikely that participants had been confronted with requests for these items before in the context of loan applications. Thus, they would be forced to think about what it meant to disclose them in this context for the first time.

When interviewing experts of consumer credit in Study 1 (Section 4.3), the idea of collecting additional personal data items as a way to improve the predictive power of credit scoring systems was mentioned. Experiences of loss during childhood and one's relationship with his/her parents, among other factors, can influence financial behaviour later on in life. In this study, the acceptability of using these and other items, such as history of utility payments, in the context of a loan application is explored. A secondary goal of the study is to understand whether it would be viable for individuals with a thin credit record to provide some extra items of personal data that would help them demonstrate credit worthiness.

### *4.5.2 Method*

Study 3 had the same structure as Study 2 (Section 4.4), but inquired participants about a different set of data items. 363 participants responded to the questionnaire. 78 were excluded for providing non-sense answers or leaving all answers on their default values. The final sample size was thus comprised of 285 participants. 45 (15.8%) participants were between 18 and 24, 36 (12.6%) between 25 and 39 years of age, 100 (35.1%) between 40 and 59, and 104 (36.5%) over 60. 181 (63.5%) were female and 104 (36.5%) male. 226 (79.3%) had experience of applying for credit. Based on their equivalised income (see Study 2), 43 (15.1%) were quoted a loan of £500, 126 (44.2%) a loan of £2000, and 116 (40.7%) a loan of £5000.

53 data items that are not part of loan application forms, but are potential indicators of financial behaviour were used. The list of items included data requests such as: "Your relationship history", "Insurance claims", or "List of friends from social networking sites".

These items were chosen based on the experts interviews in Study 1 (Section 4.3.3.1) and literature suggesting index of social capital as an indicator of credit worthiness (Lin et al., 2009).

### *4.5.3 Findings*

#### 4.5.3.1 Comfort with disclosure

Table 4.5 shows the mean comfort ratings for the 53 data requests in the questionnaire. “Not applicable” ratings were excluded on an item-by-item basis. In descending order, participants were most comfortable disclosing: (1) highest level of education; (2) council tax payment history; (3) electricity bills; (4) TV license bills; and (5) gas bills. With the exception of education, these items can be interpreted as utility and non-income tax payments. It is interesting to see that, while these items are related to payments, they were not considered as sensitive as the financial data was in the previous study, suggesting that history of bill payment is a much more acceptable data request than value of assets in the bank, for example. One implication of this finding is that lenders could start asking for the data items in place of other more sensitive items, if the predictive power of their credit scoring remains unaffected by the replacement. This would also help individuals with thin credit histories provide supporting evidence for their ability to repay a debt.

The items participants found the least comfortable to disclose in the context of a loan application were: (1) friends’ profiles from social network sites; (2) list of friends from social networking sites; (3) mobile phone contacts list; (4) names, addresses and phone numbers of friends; and (5) friends’ profiles from professional networking sites. All these items are indices of social capital. Social ties have been used in past research to estimate credit worthiness in the context of peer-to-peer lending websites (Lin et al., 2009). However, the results of this study strongly suggest that explicitly asking for data related to social connections is highly uncomfortable for the individual answering. Thus, it may be unrealistic to expect indices of social capital to be part of o a credit scoring process without a significant consumer backlash.

| Data Item | mean | s | N |
|---|---|---|---|
| Highest level of education | 3.94 | 1.13 | 281 |
| Council tax payment history | 3.76 | 1.07 | 279 |
| Electricity payment history | 3.73 | 1.09 | 274 |
| TV license payment history | 3.71 | 1.06 | 278 |
| Gas payment history | 3.70 | 1.11 | 261 |
| Friends profiles from professional social network sites | 1.79 | 1.11 | 239 |
| Names, addresses and phone numbers of friends | 1.76 | 1.12 | 282 |
| Mobile phone contacts list | 1.70 | 1.10 | 280 |
| List of friends from your social networking sites | 1.68 | 1.07 | 244 |
| Friends' profiles from social network sites | 1.67 | 1.01 | 246 |

**Table 4.5: Comfort ratings for alternative loan application data requests (Sample)**

#### 4.5.3.2 Participants are more comfortable disclosing items that show them in positive light

As in the previous study, significant and positive correlations between *comfort* and *projected image* ratings were found for the vast majority of data items - 51 out of 53. The non-correlated items were "Friends' profiles from professional social network sites" and "Number and length of messages between you and your social network friends". Thus, items participants thought would portray them in a bad light were considered more sensitive and items that participants thought would portray them in a good light were considered less sensitive. Effect sizes varied between small (r = 0.15) and close to large (r=0.42).

Verifying this relationship with different items and a different sample from the one in Study 2 (Section 4.4) gives further support to the conclusion that *projected image* does in fact influence *comfort* with disclosure. Moreover, the relationship holds for both high and low sensitivity items.

| **Data Item** | ***p*** | **Pearson's correlation (r)** | **N** |
|---|---|---|---|
| Council tax payment history | <.001 | 0.42 | 270 |
| Mobile phone bill payment history | <.001 | 0.42 | 259 |
| Gas payment history | <.001 | 0.41 | 255 |
| Recommendation from your most recent previous partner / spouse | <.001 | 0.41 | 224 |
| TV license payment history | <.001 | 0.41 | 273 |
| Weight | <.001 | 0.38 | 273 |
| Satellite or Cable TV payment history | <.001 | 0.38 | 221 |
| Internet payment history | <.001 | 0.37 | 264 |
| History of insurance claims | <.001 | 0.36 | 248 |
| Full NHS medical records | <.001 | 0.36 | 279 |

**Table 4.6: Correlation between comfort and projected image ratings for alternative loan application data requests (Sample)**

## 4.6 Study 4: Experiences of Being Denied Credit

### *4.6.1 Aims*

Study 4 had the goal of exploring individuals' experiences of applying and subsequently being refused some type of credit from a privacy perspective. Out of the many themes surrounding denial of credit this study focused mainly on three issues: (1) instances where participants had decided not to apply for credit because of the personal data requests made by the lender; (2) transparency of the credit scoring process and understanding of the reasons for denial; and (3) credit report and quality of the data on which it is based. In this thesis only the findings related to issue 1 are reported.

### *4.6.2 Method*

As in Studies 2 (Section 4.4) and 3 (Section 4.5), participant recruitment was handled by market research company eRewards using a nationally representative sampling frame. 320 participants responded to the questionnaire, but 78 were excluded to non-sense (e.g.: random text or "N/A") or incomplete answers to the questions. The final sample is thus 298 participants. All participants had experience of having been denied credit, as it was a pre-requisite for participation. There was a larger proportion of females, 202 (67.8%) then males, 96 (32.2%). 37 (12.4%) participants were between 18 and 24 years old, 146 (49%) between 25 and 39; 102 (34.2%) between 40 and 59, and 13 (4.4%) over 60. Regarding employment situation, 158 (53%) participants were employed full-time; 17 (5.7%) were self-employed; 52 (17.4%) were part-time employed; 4 (1.3%) were on temporary employment; 9 (3%) were retired; 12 (4%) were students; 30 (10.1%) were looking after family or home; and 14 (4.7%) were permanently sick or disabled. Regarding their debt situation, 168 (56.4%) participants said they had manageable debt; 52 (17.4%) were debt-free; 60 (20.1%) said they had "problem debt"; 13 (4.4%) were on an Individual Voluntary Agreement (IVA); and 5 (1.7%) were bankrupt.

The online survey was created using Limesurvey and consisted of 34 questions. Some of these questions were open answer. Of relevance to this thesis was the section of the questionnaire that asked participants: "Have you ever not applied for credit because of the information requested?"

The questionnaire took 15 minutes to fill in and participants were paid by eRewards for their participation.

### *4.6.3 Findings*

#### 4.6.3.1 Not applying for credit due to the data requested

One of the questionnaire questions asked participants whether they had ever chosen not to apply for credit because of the data requests present in the application form. If they answered "Yes", participants were asked to further explain their experience in an open text box: which data was asked and why did they not want to disclose it?

36 (12%) participants answered "Yes" to the question and 28 of those provided more detailed descriptions of the situations. These descriptions were analysed using thematic analysis method. The themes identified are presented next.

##### *4.6.3.1.1 Theme 1: Perceived Relevance*

Three participants had not applied for credit because they perceived some of the data requested as not *relevant*, such as data related to their partner:

> *"Credit card companies always want to know about your spouse's income/debts etc., which I don't feel should be relevant if you are applying for a card yourself and you have income." P202*

The perceived relevance theme had already been identified in Study 2 (Section Study 2: Perceptions of Loan Application Data Items4.4) and its emergence here gives further support to the hypothesis that perceived relevance of a data request influences the attitude of the data subject towards that data request.

#### *4.6.3.1.2 Theme 2: Effort (Detail)*

Two participants mentioned that the *level of detail* of the lender's questions had made them not apply for the credit service:

> *"[Store] credit card, they wanted 3 months of bank statements so I didn't progress with the application." P194*

This finding suggests that as the level of detail required to answer a question increases the least likely an individual is to answer it. Since a question which requires a more detailed answered will usually take more time to answer and will, possibly, imply a higher cognitive load on the individual, level of detail can be operationalised as cost.

#### *4.6.3.1.3 Theme 3: Projected Image*

Seven participants said they had avoided a credit service because they did not want to disclose data that would show them in a negative light:

> *"It was a personal loan. When I still had a CCJ [county court judgment] on my record I hated to have to tell anybody because it did not reflect my current attitude to borrowing, or ability to repay." P93*

This gives support to the findings in Studies 1, 2, and 3 (Sections 4.3, 4.4, and 4.5) that suggest that the *image projected* by a disclosure affects individuals' attitude towards the disclosure, making them less likely to disclose data that will show them in a bad light.

#### *4.6.3.1.4 Theme 4: Projected Outcome*

12 participants assumed they would be rejected and did not want to harm their credit record any further, so chose not to apply to a credit service:

> *"I no longer apply for any credit as I do not want to make my credit rating worse by being refused." P37*

Four participants also wanted to avoid the embarrassment of being rejected. They had been denied credit in the past and did not want to experience it again:

> *"Every time I go into a store and they offer me a store card I refuse because I am scared of being rejected." P55*

While in this case it is in the interest of the lender that individuals with a poor credit record do not apply for additional credit, there may be situations where potential customers avoid disclosing personal data because the *projected outcome* of the disclosure is harmful. One such case is individuals' reticence in disclosing phone numbers for fear of being contacted by telemarketing companies (see Section 4.4).

## 4.7 Study 5: Disclosure Behaviour with Uncertain Reward

### *4.7.1 Aims*

The aim of this study was to observe participant behaviour when they are asked to disclose a subset of the data items tested in Study 3 (Section 4.5). These were items that were suggested in the interviews with experts and in the literature as having some potential as indicators of financial behaviour. They are not currently requested in loan application forms due to their sensitivity. While in study 3 participants were asked to give their perception of the sensitivity of these items, in this study the goal was to ask participants to actually answer the questions. Privacy attitudes and behaviour have been shown to have large discrepancies in past research.

Two secondary goals of this study were to: (1) test the effect of privacy concern, as measured by Westin privacy index, on disclosure behaviour; and (2) determine whether providing explanations for the questions being asked, to improve *perceived relevance*, would increase disclosure rates.

### *4.7.2 Method*

#### **4.7.2.1 Choosing the items**

In Study 3 (Section 4.5) 285 participants were asked to rate 53 data items regarding how comfortable they felt disclosing them in the context of a loan application. A principal component analysis (PCA) of the ratings revealed five main factors the items varied on and which explained 53% of the total variance in the data. Because it was easier to interpret, the varimax rotation was used. The five factors were coded based on the items they contained as: (1) personal/sensitive; (2) bills; (3) attitudes; (4) social network; (5) partners and children. 14 items were selected to be used in this study. The aim was to have items that represented the five factors. The items were adapted to have the form of a question.

#### 4.7.2.2 Participants

48 participants took part in the experiment. Average age was 20 years old (s=1.97), and the range of ages was form 19 to 31 years old. 35 (72.9%) of participants were female and 13 (27.1%) were male. 36 (75%) were UCL psychology students. Eight (16.7%) other participants were also students at UCL. Two (4.2%) were students at another university; and one (2.1%) participant was not a student.

#### 4.7.2.3 Experiment

In a laboratory environment the participants were asked to help test:

> *"The acceptability of the application process for a new Super Credit Card that beats all other cards on the market. Because the deal is so good it can only be offered to people who are very reliable at repaying. The bank (we cannot reveal which one because of commercial sensitivity) thinks it has discovered a better way of assessing financial responsibility, but it requires more and also different information than is used in the standard credit reference reports."*

Participants were asked to complete an application form for this card which consisted of 24 questions. Ten of these were *basic items, i.e.* questions commonly asked in application forms, such as "Name" and "Gender" (see Table 4.7). These items were included to increase the realism of the experiment and make participants actually believe that their answers would be processed by the fictitious bank and credit referencing agencies and that they would be identifiable. They also provided a baseline to which to compare the sensitivity of the novel data items.

| Items |
|---|
| 1. Full name |
| 2. Gender |
| 3. Date of birth |
| 4. Current Home Address |
| 5. Mobile phone number |
| 6. Home phone number |
| 7. Nationality |
| 8. Employment status |
| 9. Have you had a credit card before? |
| 10. What is the name of your bank? |

**Table 4.7: List of basic items**

The other 14 questions were the *novel data items* mentioned above, which included data requests like “Did any of your loved ones die while you were growing up? Please give their relation to you (e.g. mother, brother, friend, etc.)” (see Table 4.8). Participants were required to provide an answer in an open text box or tick a box declaring they consented for the bank to obtain specific documentation with their data (e.g.: “Do you give us permission to contact your local council to get a copy of your council tax payment history?”).

| Items |
|---|
| 1. Did any of your loved ones die while you were growing up? Please give their relation to you (e.g. mother, brother, friend, etc.) |
| 2. Do you suffer from any medical conditions? Please list... |
| 3. Did you live with both your mother and father while you were growing up? |
| 4. Could you list the names and either phone numbers or email addresses of three of your closest friends? |
| 5. Do you give us permission to contact your local council to get a copy of your council tax payment history? |
| 6. Do you give us permission to obtain a copy of your TV licence payment history? |
| 7. Do you give us permission to obtain a copy of your gas or electricity payment history? |
| 8. Please provide the name and address (or other contact details) of a previous employer so that we can request a copy of the last recommendation from him / her about you... |
| 9. What is the job of your partner / spouse? Please describe... |
| 10. What are the names of 3 people that you are friends with on a social networking site (facebook, twitter) whose profiles you would be happy share with us? Please list... |
| 11. What are the names of 3 people that you are friends with on a professional networking site (LinkedIn, Orkut) whose profiles you would be happy share with us? Please list... |
| 12. Will you allow us to measure the typical number and length of messages between you and your friends on social networking sites? |
| 13. What is the length of the longest relationship you have had with a partner / spouse? (years/ months/ weeks) |
| 14. May we obtain a copy of your insurance claims (e.g. car, house)? |

**Table 4.8: List of novel items**

Participants could only submit the form when they had answered at least 20 out of the 24 questions. This minimum number of answers was chosen so that, even if participants disclosed all ten basic items, they would have to disclose ten of the 14 novel items. To further nudge participants into answering as many questions as possible a progress bar was put at the top of the form showing how close they were to be able to submit it (see Figure 4.1).

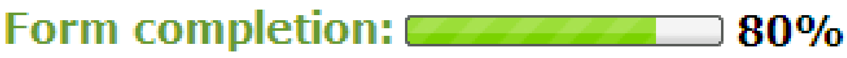
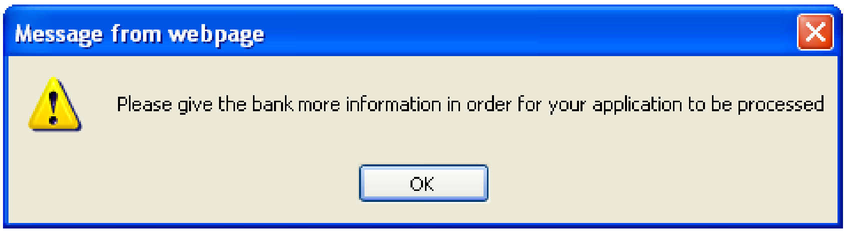


**Figure 4.1: Application form progress bar**

If they tried to click the submit button before they had answered the minimum number of questions an error message was displayed on screen (see Figure 4.2). Whenever participants answered a question with the option “N/A” the progress bar would not fill and the answer would not count towards the tally. This decision was taken to mimic a real loan application process where applicants are forced to submit the necessary documentation and data.


Message from webpage

Please give the bank more information in order for your application to be processed

**Figure 4.2: Insufficient information message**

When participants clicked the submit button no data was saved or transmitted anywhere; it was simply deleted. Thus, no personal data of participants was stored. Experimenters observed participants filling in the form and took notes of which questions they answered (but not the actual answers).

Participants were rewarded with £5 regardless of having submitted the form or not. They were told that no actual credit card would be awarded, but that the most creditworthy participant would receive a £50 reward. This reward was meant to create a real trade-off between disclosing personal data and obtaining an economic benefit similar to what happens in real life credit applications.

To better simulate a real loan application process and minimise falsification of data, participants were told that:

> *"The card can only be offered to people that are completely honest during the application procedure, if you lie on a single item you are not eligible. […] all application data is being sent to a credit reference agency for validation… [using a] … sophisticated combination of cross-comparisons between data in the application form, the individual's current credit record, and also comparison to the Agency's most advance customer profiling system."*

The experiment followed a 2 x 2 matrix design with four different treatments, varying on two variables with two states each: *presence of explanations* and *order of questions.* To test the effect of *perceived relevance* of a data request on disclosure rate, half the participants were exposed to a form that provided text explanations below each question clarifying how each item was necessary for credit scoring purposes. For example, below the question *"Did any of your loved ones die while you were growing up?"* it was written: *"We need this information to help judge how your early experiences might shape your behaviour as an adult – early loss has* *been related to later financial behaviour."* The second half was exposed to a form where no explanation was provided. Privacy literature suggests that individuals are more likely to feel comfortable disclosing personal data when they understand the purpose of its collection in the context where it is being requested (see Sections 2.1.1.2 and 2.1.1.5). To control for item order, forms had a *normal* and *inverse order.* In both of these versions, the ten basic items were shown first and in the same order and only the novel items were in inverse orders.

In a second phase of the study that immediately followed the form, participants' privacy concern was measure using Westin's privacy segmentation scale (see Section 2.1.1.8). This scale consists of three privacy concern statements which participants are asked to rate with regards to their level of agreement (1 = strongly disagree and 4 = strongly agree):

- *"Consumers have lost all control over how personal information is collected and used by companies"*
- *"Most businesses handle the personal information they collect about consumers in a proper and confidential way"*
- *"Existing laws and organizational practices provide a reasonable level of protection for consumer privacy today"*

Based on their answers respondents to Westin's privacy segmentation are assigned to one of three groups: (1) *privacy fundamentalists*, who agree with the first statement and disagree with the other two; (2) *privacy unconcerned*, who disagree with the first statement and agree with the other two; or (3) *privacy pragmatists*, who comprise everyone else.

A short interview followed, where participants were asked how acceptable they thought each of the 24 questions was. If they had chosen not to submit the form they were also asked why they had made that choice. Finally, they were asked whether they had lied or omitted any details from their answers. Participants were reassured that this phase of the study did not concern the bank, but only the researchers own inquiry. They were also told that their answers would not be passed on to the bank and would remain with the researchers.

This was a double-blind study: the three experimenters that tested participants were also told the study was part of consumer research for a bank. They were told the study's aim was to gauge the acceptance of the application process and determine how likely participants were to lie. Like the majority of students, the experimenters were UCL psychology students, and the double-blind nature of the study also prevented any leakage of information regarding the true intent of the study.

The study was reviewed and approved by the university's ethics approval process. Participants and experimenters were informed they had been deceived and that no bank had commissioned the research. One of the participants that had submitted the form was chosen randomly to receive the £50 reward.

### 4.7.3 *Findings*

#### 4.7.3.1 Submission and answer rates

28 (58.3%) participants answered at least 20 questions and submitted the form. Table 4.9 shows the answer rates per question. Excluding "Not Applicable" answers from the analysis, six *basic items* were answered by all participants. Three other basic items were not answered by one participant. The remaining basic item was not answered by two participants. This results in an average response rate of 99% for basic items.

Answer rates for *novel items* ranged from 44.4% to 100% (excluding "Not Applicable" answers from analysis). Every participant answered the item "Grew up with both mother and father". Average response rate among novel items was 85%. This suggests novel items were indeed considered more sensitive, but not as sensitive expected given the answer rates were still high.

#### 4.7.3.2 Answer rate for items is correlated with the sensitivity

The percentage of participants who answered an item (excluding "Not Applicable" answers) was inversely and significantly correlated with the comfort ratings of that item as measured in Study 2 (Section 4.4), $\rho = 0.624$, $p<0.01$.

The association between *sensitivity* of a disclosure (or comfort with disclosure), and disclosure rate has also been verified in past research (see Metzger, 2007). This finding is important because it provides an insight into the actual disclosure behaviour of individuals as opposed to attitudes towards disclosure, which may or may not correspond to their actual behaviour. The fact that the behaviour of this sample was consistent with the sensitivity rating of a different nationally representative sample also suggests that application or registration forms can be evaluated *a priori.* It would be possible to estimate the likelihood of applicants withholding some items and determine the impact of the missing data on the organisation's business processes to decide whether it is actually worth requesting it.

#### 4.7.3.3 No effect for providing an explanation for the data request

It was expected that providing an explanation for the collection of a specific item would increase the *perceived relevance* of the item and boost disclosure rated, but such was not the case. Participants in the experimental treatments where justifications were provided for asking each question did not disclose significantly more data: (1) there was no association between providing explanations and participants submitting the form ($\chi^2(1) = 0.34$, below the critical value of 3.84, p=0.05); (2) there was no association between explanations and number of questions participants answered (t value was not significant); (3) there was no association between explanations and whether participants answered a question in particular (Pearson's Chi Square or Fisher's Exact Tests not significant, p=0.05).

| Item | N | Answered | Did Not Answer | N/A | Answer Rate | Answer Rate (exc. N/A) |
|---|---|---|---|---|---|---|
| Grew up with both mother and father | 48 | 48 | 0 | 0 | 100.0% | 100.0% |
| Current home address | 48 | 48 | 0 | 0 | 100.0% | 100.0% |
| Employment status | 48 | 48 | 0 | 0 | 100.0% | 100.0% |
| Gender | 48 | 48 | 0 | 0 | 100.0% | 100.0% |
| Mobile phone number | 48 | 48 | 0 | 0 | 100.0% | 100.0% |
| Nationality | 48 | 48 | 0 | 0 | 100.0% | 100.0% |
| Full name | 48 | 48 | 0 | 0 | 100.0% | 100.0% |
| Date of birth | 48 | 47 | 1 | 0 | 97.9% | 97.9% |
| Ever had a credit card | 48 | 47 | 1 | 0 | 97.9% | 97.9% |
| Loved ones passed away while growing up | 48 | 45 | 3 | 0 | 93.8% | 93.8% |
| Name of your bank | 48 | 45 | 1 | 2 | 93.8% | 97.8% |
| Copy of TV licence payment history | 48 | 28 | 1 | 19 | 58.3% | 96.6% |
| Medical conditions | 48 | 45 | 3 | 0 | 93.8% | 93.8% |
| Copy of gas / electricity payment history | 48 | 38 | 3 | 7 | 79.2% | 92.7% |
| Home phone number | 48 | 24 | 2 | 22 | 50.0% | 92.3% |
| Length of longest relationship | 48 | 34 | 3 | 11 | 70.8% | 91.9% |
| Copy of council tax payment history | 48 | 24 | 3 | 21 | 50.0% | 88.9% |
| Previous employer contact details | 48 | 26 | 4 | 18 | 54.2% | 86.7% |
| Social networking profiles of 3 friends | 48 | 37 | 6 | 5 | 77.1% | 86.0% |
| Copy of insurance claims | 48 | 23 | 4 | 21 | 47.9% | 85.2% |
| Job of partner / spouse | 48 | 17 | 3 | 28 | 35.4% | 85.0% |
| Number and length of mobile text messages | 48 | 33 | 13 | 2 | 68.8% | 71.7% |
| Name and phone number / email of 3 friends | 48 | 33 | 15 | 0 | 68.8% | 68.8% |
| Professional networking profiles of 3 friends | 48 | 4 | 5 | 39 | 8.3% | 44.4% |

**Table 4.9: Answer rates**

### 4.7.3.4 Partial effect of privacy concern on disclosure

It was expected that *privacy fundamentalists* (according to Westin's categorisation) would be less willing to disclose personal data. That was indeed the case, but only when comparing *fundamentalists* with the two other categories – *privacy pragmatists and privacy unconcerned* – grouped together. No statistically significant effect was detected when these two categories were considered independently. One possible reason is that the study did not have enough participants, and thus the test did not have enough power to detect an effect. It should also be noted that Westin's privacy category has not been shown to be a particularly good predictor of behaviour (see Section 2.1.1.8). In any case, whether a participant was a *fundamentalist* or not did have a significant association with whether they had submitted the form $\chi^2(1) = 4.39$, $p < 0.05$. In fact, a fundamentalist was 5.6 times less likely to submit the form than a non-fundamentalist.

#### 4.7.3.5 Factors that affect perception of data requests

The thematic analysis of the interview transcripts revealed several factors which influence individuals' perception of data requests (see Figure 4.3, number of participants who mentioned each factor indicated in parentheses).

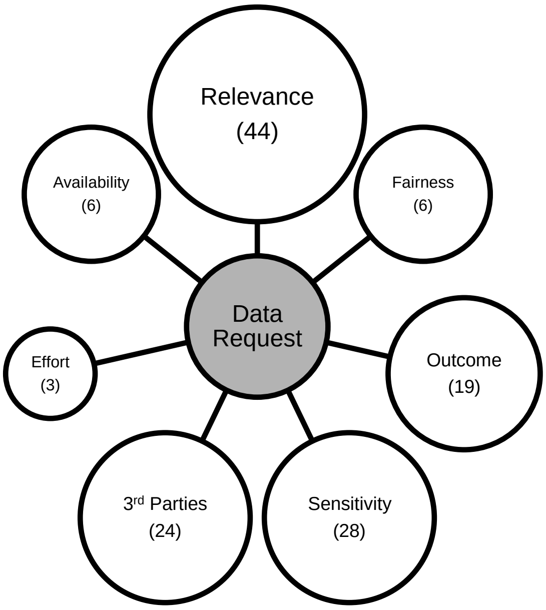


**Figure 4.3: Factors that influence perception of data requests**

##### *4.7.3.5.1 Theme 1: Perceived Relevance*

A data request considered to be relevant was one where the data item was perceived to relate to financial behaviour, personality of the applicant, or probability of debt repayment. Relevant data requests were perceived more positively than irrelevant ones:

> *"I don't think it's acceptable, it's got nothing to do with my credit status" P6*

> *"Yeah it's good, because the bank needs to know how much income you've got" P13*

The impact of the factor *perceived relevance* had already been identified in Studies 2 and 4 (Sections 4.4 and 4.6)

### *4.7.3.5.2 Theme 2: Fairness*

Perceptions of *fairness* were related to how ethically acceptable it was, form the point of view of the participant, to use an item to draw conclusions about an applicant. While *perceived relevance* concerns the alignment between the perceived purpose of usage and context of data collection, *fairness* was interpreted more as an ethical consideration. In this perspective, the two dimensions are orthogonal, an item can be seen as relevant for the interaction but unfair to collect (e.g.: health details in the context of an insurance premium calculation).

> *"Acceptable? I don't know if it's acceptable... you might discriminate on the basis of the answer to that question. But I don't know if there's such a thing as fair discrimination, like say you've got a strong disability it might be useful to know what kind of... whether you need more stuff paid for, and you might get problems with your account of something. But I'm not sure, I would probably... I wouldn't demand a person to answer a question like that, because it could cause discrimination from your side." P24*

### *4.7.3.5.3 Theme 3: Projected Outcome and projected image*

Disclosures which participants thought would result in more positive *outcomes* and would show them in a good light were perceived in a more favourable way:

> *"I did disclose it on the answers because again I had nothing to hide, it would all go in my favour." P29*

Disclosures which participants thought could harm them or portray them in a bad light were perceived as more negative:

> *"I did reply, I answered, but only because I don't suffer from a medical condition. Probably if I did I might have reacted differently." P17*

This supports the findings in Studies 1, 2, 3 and 4 (Sections 4.3, 4.4, 4.5, and 4.6).

#### *4.7.3.5.4 Theme 4: Sensitivity*

Data requests that were perceived to be too personal, sensitive, or privacy invasive were considered less acceptable, supporting the finding that sensitivity of the data requests affects how it is perceived and also supporting the relationship between sensitivity and disclosure rate identified above:

> *"I found that very intrusive. I don't think that's acceptable." P48*

#### *4.7.3.5.5 Theme 5: 3rd Parties*

Requests for data related to friends, partners, or relatives of participants were seen in a more negative way:

> *"[S]haring other people's details is always something I find like quite hard to do." P48*

Participants did not want their friends to be contacted by the bank; they felt the data was not theirs to give; and that they had not given permission for the data to be disclosed:

> *"I wouldn't really want them to impose on my friends' personal space without them giving consent to that." P25*

#### *4.7.3.5.6 Theme 6: Effort*

The *effort* of answering a data request affects how it is perceived. Requests that are difficult to answer, take longer to answer, or require the participants to get the data from somewhere are perceived less favourably:

> *"It would be difficult to get hold of the information, so again I was less inclined to provide it." P30*

Effort had already been identified as a relevant factor in Study 4 (Section 4.6).

#### *4.7.3.5.7 Theme 7: Availability*

Questions asking for data that was already *available* elsewhere were perceived by participants in a more favourable way:

> *"Yes I thought this was acceptable, insofar that social networking sites are sort of publicly accessible, and so giving the details of people with whom I have connections on these sort of sites is a reasonable thing to ask." P23*

Some participants said they answered requests they considered unacceptable because they thought the data was already publicly available. This finding suggests that, once a data item is publicly available, individuals do not feel that disclosing it again implies an additional privacy cost.

#### 4.7.3.6 Discrepancy between acceptability and disclosure

While the *acceptability* of data requests was significantly correlated with the *sensitivity* ratings collected in study 3 ($\rho = 0.607$, $p<0.01$), for 21 items there was no association between *acceptability* and *disclosure*. The three items for which an association between these two variables was found were: *insurance claims* $\chi^2(2) = 10.44$, $p<0.05$, *council tax* $\chi^2(2) = 10.10$, $p<0.05$, and *emails and phone numbers of friends* $\chi^2(2) = 8.42$, $p<0.05$.

As can be seen in Table 4.10, a large proportion of participants found items unacceptable, but still disclosed them. These participants were asked in the follow-up interview why they had done so. 10 participants said that they may consider a question *generally unacceptable*, but that in their personal case they may not have an issue with answering it. For example, Participant 28 said:

> *"Again I did disclose it, but I don't think the general public would be happy […] because I see myself as quite an open person, so I would be happy." P28*

This justification for answering unacceptable data requests suggests that the assessment of the questions in terms of privacy and acceptability may be separate from the actual cost-benefit assessment of disclosing the data. Thus, an individual may perceive a data request as *sensitive* or *unfair* while at the same time expecting to obtain a positive *outcome* from answering it. Further support for this hypothesis can be found in the fact that five participants admitted they answered unacceptable data requests because they wanted to submit the form and be eligible for the reward:

> *"I did disclose some things mainly just to complete the questionnaire. But it didn't seem a great question." P27*

Two other justifications given by participants were aligned with the themes identified above: (1) four participants said that answering the questions would not cause them harm indicating that they did not *expected a negative outcome*; (2) and two other participants said that the data was *publicly available* anyway.

Another explanation for this behaviour is that participants were exhibiting social desirability bias and answered questions they deemed unacceptable because they thought that was expected of them. This is a potential limitation stemming from the artificiality of lab experiments (see Section 3.2.5).

| Item | N[6] | Found unacceptable but disclosed | % found unacceptable but disclosed | % found unacceptable but disclosed (excl. N/A) |
|---|---|---|---|---|
| Loved ones passed away while growing up | 46 | 26 | 56.5% | 56.5% |
| Social networking profiles of 3 friends | 47 | 25 | 53.2% | 61.0% |
| Name and phone number / email of 3 friends | 47 | 20 | 42.6% | 42.6% |
| Number and length of mobile text messages | 46 | 19 | 41.3% | 43.2% |
| Length of longest relationship | 47 | 18 | 38.3% | 50.0% |
| Grew up with both mother and father | 44 | 18 | 40.9% | 40.9% |
| Medical conditions | 46 | 11 | 23.9% | 23.9% |
| Professional networking profiles of 3 friends | 45 | 3 | 6.7% | 33.3% |
| Job of partner / spouse | 46 | 3 | 6.5% | 15.8% |
| Copy of insurance claims | 41 | 2 | 4.9% | 7.1% |
| Previous employer contact details | 46 | 2 | 4.3% | 6.7% |
| Copy of TV license payment history | 45 | 2 | 4.4% | 7.1% |
| Copy of gas / electricity payment history | 45 | 1 | 2.2% | 2.8% |
| Copy of council tax payment history | 46 | 1 | 2.2% | 3.8% |

**Table 4.10: Acceptability vs. disclosure**

[6] Participants who, in the interview, did not answer clearly whether they found an item acceptable or not were deleted pairwise

#### 4.7.3.7 Privacy protection behaviours

As part of the post-experiment interview, participants were asked if they had engaged in any privacy protection behaviour, such as lying or omitting information in their answers in the form. 11 (23%) participants admitted they had. Examples of privacy protection behaviours included writing their friends initials instead of their full names or agreeing for the bank to check their utility bills when in fact they are not the ones paying them. Two reasons were provided for these coping techniques: (1) increase the number of items provided so that they could submit the form and be eligible for the reward; and (2) protect the privacy of their friends.

## 4.8 Discussion

Lenders want to protect the viability of their business and, to that effect, aim to minimise the number of borrowers who default on their loans. To do that, they attempt to predict how likely each individual who applies for a loan is to not be able to make the repayments and based on that prediction decide whether to grant the applicant a loan or not. These predictions are made by credit scoring algorithms and to make them, they process several items of personal data from the applicants. Lenders have the goal to constantly improve their ability to predict likelihood of default. One way to do this is to update their algorithms by collecting more data or by combining in different ways. Expert interviews conducted in Study 1 confirm this and suggest that, from the perspective of the lenders data items that have the most predictive power are the most valuable (see Theme 1: Predictive Power in Section 4.3.3.1).

On the other side of the interaction, loan applicants have a strong incentive to want to appear creditworthy to lenders and want to disclose data items that make them look like good risks. This was mentioned in Study 1 (see Theme 2: Projected Image and Predicted Outcome in Section 4.3.3.2). In fact, results from the five studies in this chapter, indicate that *projected image* and *projected outcome* are two important factors in disclosure decision making in this context. Studies 2 and 3 (Sections 4.4 and 4.5) show a clear positive correlation between how individuals think a disclosure will make them look and their level of comfort with that disclosure. In these two studies, participants were more comfortable with disclosures that they perceived would improve their chances of obtaining a loan and less comfortable with negative disclosures. Study 4 (Section 4.6) gives further support to the hypothesis that projected image (Section 4.6.3.1.3) and projected outcome (Section 4.6.3.1.4) affect the decision to disclose items of personal data in the context of a loan application. Finally, in Study 5, participants explained their disclosure behaviour *post hoc* by saying they answered some questions because they expected a positive consequence or, at least, did not expect a negative one

(Section 4.7.3.5.3). The factor projected image as an antecedent of privacy perceptions has been observed in the context of multimedia interactions (Adams, 2001).

Studies 2 and 3 (Sections 4.4 and 4.5) also suggest that different types of data have different levels of *sensitivity*, i.e. individuals are not equally predisposed to sharing all types of personal data, which is in agreement with past research (see Section 2.1.1.1). In these studies participants revealed a higher level of comfort with sharing items such as name, gender, or whether they were currently living in the UK. These have in common the fact that they are commonly asked in application and administrative forms. It is likely that participants had been asked to disclose these items before and, thus, they may have felt they were not paying an additional privacy cost by disclosing them again. In fact, this reason is given in Study 5 (see Theme 7: Availability in Section 4.7.3.5.7) to justify the low level of concern with disclosing some items: the data was already available (to the data receivers) elsewhere. This raises the issue of the difficulty in controlling personal data once it was disclosed. While the right to edit one's data and ask for its deletion are part of data protection law in the UK (UK Data Protection Act, 1998), in practice it is very difficult to manage one's personal data after it is shared. Several factors contribute to this: the individual may not be aware the data is being collected; the individual may not know which channels to use to communicate his/her wish to have the data deleted; the data may have been shared with unknown third parties.

Lenders monitor the rate of omission and answers like "Other" in loan applications to infer the perceived acceptability of the question and adjust the forms accordingly (see Theme 5: Falsifying and omitting data in Section 4.3.3.5). Privacy research acknowledges that individuals may omit or falsify answers when they do not see it as beneficial to answer truthfully (see Section 2.1.5). However, no research has been conducted on *privacy protection behaviours* in the context of loan applications. To avoid relying on self-reports (which are especially limiting in privacy - see Section 2.1.1.8) in Study 5 (Section 4.7) actual disclosure behaviour is observed. As in the experiments reported by Metzger (2007) and Horne et al. (2007), both focused on e-commerce, a correlation between perceived sensitivity of a question and its answer rate was found. These results suggest that sensitivity of data requests may affect disclosure decision regardless of the context.

In Study 5, sensitivity ratings of one nationally representative sample were compared with the disclosure behaviour of a different sample. This suggests that average sensitivity ratings provided by a large and representative enough sample can be used to estimate the proportion of individuals in a new group that will disclose a specific data item. This finding gains relevance when one considers that current measures of privacy concern have limited predictive power (see Section 2.1.1.8). Exploring new privacy concern measures based on sensitivity ratings seems to be a promising avenue for future privacy research.

In Study 1, a lender explained that they could only collect data items that applicants perceived as relevant in the context of a loan application (see Theme 4: Perceived Relevance in Section 4.3.3.4). Some items might help determine how risky it is to lend to an individual but could never be asked – e.g.: car make, model and colour – because applicants would see them as irrelevant. Relevance of data requests has been identified in literature as being linked to privacy perceptions (see Section 2.1.1.2). In Study 2 (see Theme 2: Perceived Relevance in Section 4.4.3.4) *perceived relevance* was linked by participants with comfort with disclosure. In Study 4 (see Theme 1: Perceived Relevance in Section 4.6.3.1.1) irrelevant data requests were mentioned as a reason not to apply for credit. In Study 4 (see Theme 1: Perceived Relevance in Section 4.7.3.5.1), this was also the most commonly mentioned factor in relation to the acceptability of different data requests in the context of a credit card application. These findings suggest perceived relevance is an important factor in forming perceptions of loan application data requests.

When a data request is not perceived as relevant, individuals will start creating their own interpretations of why the item is being asked (Culnan, 1993; Hine and Eve, 1998; Ackerman, 1999). These interpretations often assume nefarious purposes behind the data collection. Lenders should try to assuage these fears by clearly and effectively communicating why data items are asked. However, lenders explicitly avoid explaining why certain items are needed because it conflicts with their goal of keeping the credit scoring process obscure to prevent manipulation (see Section 4.3.3.1). A direction for future research is how to communicate the true purpose of data collection without undermining the risk assessment efficacy.

Expert interviews in Study 1 (Section 4.3) suggest that the *effort* involved in filling in the application form can have a negative impact on applicants' perceptions of the application process (see Theme 7: Effort in Section 4.3.3.7). Thus, lenders try to keep applications forms short and easy. This is in agreement with form design literature (Jarrett & Gaffney, 2009) that suggests that the number of questions asked should be kept low and not involve too much effort. As much as possible it should be possible for the respondent to just "slot in" their answers without cognitive load or having to look for the answer somewhere else. Effort was mentioned as an important factors by participants in Study 2 (see Theme 2: Effort (Detail) in Section 4.6.3.1.2) and Study 5 (see Theme 6: Effort in Section 4.7.3.5.6), suggesting that the more effort required to answer a data request the less likely an applicant will be to do it. In fact, effort has been linked to willingness and likelihood of disclosure in past research (see Section 2.1.1.6).

Findings from Studies 3 and 5 (Sections 4.5 and 4.7) indicate that participants do not consider acceptable collecting personal data related to social relationships for the purposes of credit scoring. Items related to social network contacts and communications with friends were considered uncomfortable to disclose. Past research (Lin et al., 2009) has advanced the idea of using an index of social capital to assess the likelihood of someone repaying their debts. While there may be predictive power in that method, these results suggest it would risk incurring a significant backlash from the consumers. On the other hand, items related to utilities and other types of payment history were considered acceptable. Participants were generally comfortable with the idea of using these items for credit scoring purposes. Some utility payments are already used as an indicator of debt repayment behaviour. For individuals with a thin credit file (e.g.: young adults) this could be provide them an alternative to demonstrate their creditworthiness without having to take on credit just to prove they can repay it.

Study 5 (Section 4.7) results show a very high average disclosure rate even for data items considered very sensitive. Participants also disclosed items that they previously had considered unacceptable to request. One possible explanation consistent with the literature (see Section 2.1.4) – and that participants mentioned in the follow-up interviews – is that the potential reward for disclosing the data overrode the privacy concerns. When asked to assess the acceptability of some questions participants may be making a (ethical) value judgement disassociated from a decision making process. When asked to disclose these items they assess the actual costs and benefits of disclosure and likely in this case they perceived the reward for completion to outweigh the privacy or discomfort cost. The literature has several examples of instances where individuals are willing to trade their personal details for seemingly small rewards (see Section 2.1.4).

Surprisingly, providing a justification for each question asked in Study 5 (Section 4.7) did not significantly increase the number of answers. Privacy research has determined that individuals feel more comfortable disclosing personal data if they understand and agree with the purpose of its collection (see 2.1.1.5). In this study this was not observed. It is possible users either: (1) did not notice the explanatory text; (2) noticed, but already felt comfortable disclosing. The latter may have been due to a research bias – participants felt reassured because they were part of a study – or because the consent form of the study provided justification enough for the questions asked.

The five studies described in this chapter clarify how applicants perceive data requests in loan applications and how those perceptions shape their decision to comply or not with the requests. The factors identified allow a preliminary model of disclosure decision making - in the context of loan applications – to be proposed (see Figure 4.4).

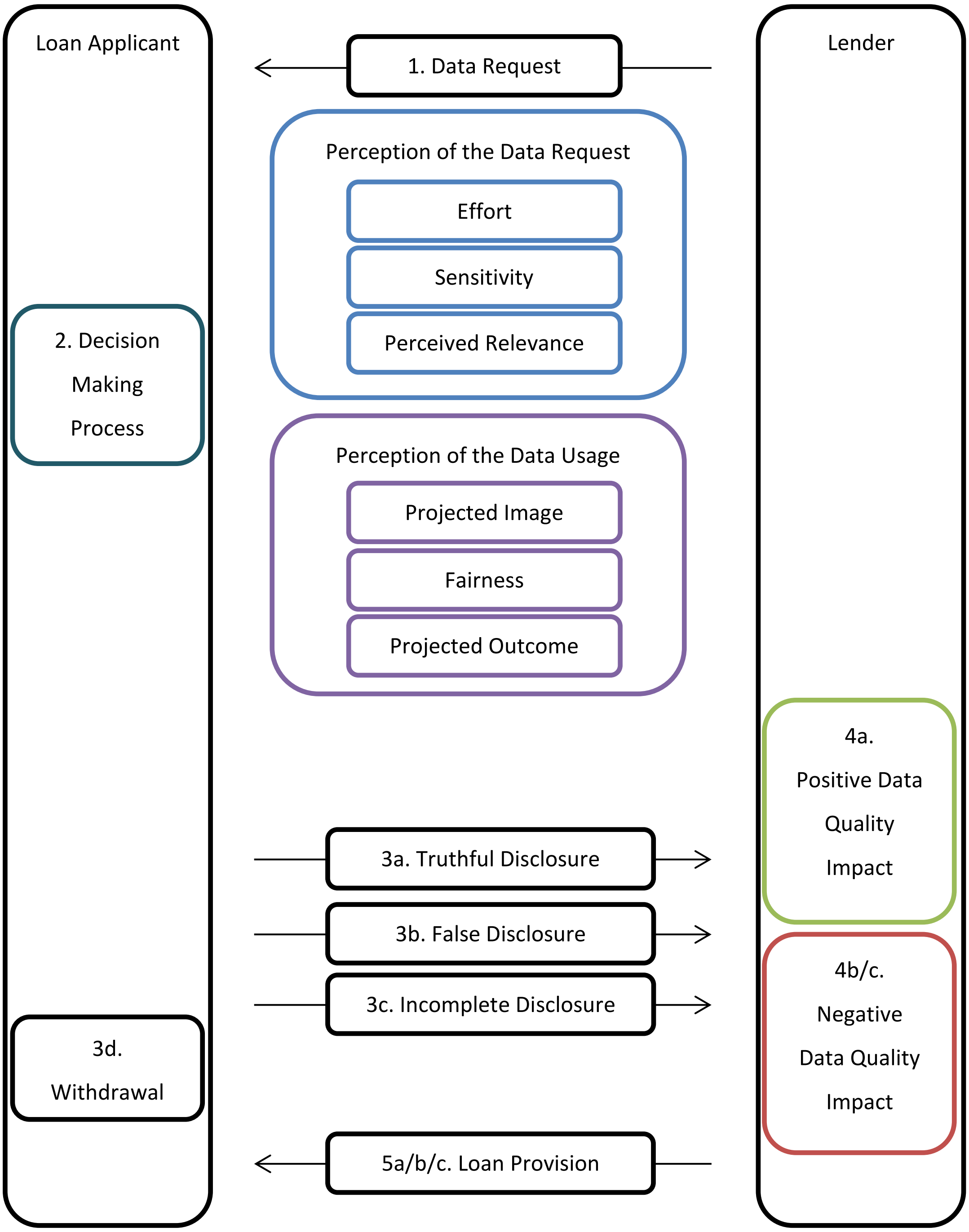


**Figure 4.4: Loan Application Disclosure Model**

# Chapter 5: SERIOUS-GAMES STUDIES

## 5.1 BACKGROUND

To avoid the costs associated with traditional training, organisations are making more use of e-learning tools to fulfil their training needs (Clark & Mayer, 2007). Serious-games are one type of e-learning approach. They simulate real-world situations to improve the transfer of learning to the actual contexts where it is needed by the user (Van Eck, 2006; Fletcher & Tobias, 2006). At the same time, they make use of game elements like competition to make the interaction with these systems more entertaining and motivating.

Serious-games collect personal data from their users, which can have privacy implications. Past research has already identified privacy issues as a relevant concern in the field of e-learning. In particular, *linkability* of data, *observability* of data, *identity disclosure* and *data disclosure* have been pointed out as important privacy risks (Anwar et al., 2006; Jerman-Blazic & Klobucar, 2005; Nejdl & Wolpers, 2004). However, this view reflects a data-centric perspective that assumes that specific data items are sensitive and does not take into consideration how users' privacy perceptions are created. Furthermore, the solutions proposed to deal with privacy risks have been limited to generic privacy-enhancing technologies (PETs) (El-Khatib et al., 2003) and have focused too much on identity protection (Anwar et al., 2006).

These approaches do not consider the importance of contextual factors in forming privacy perceptions. Users' privacy concerns will depend on several features of their interaction with a system that collects their personal data. Adams' (2001) model for privacy in multimedia interactions proposes that users look at three main factors when judging the privacy implications of an information system: (1) data receiver; (2) data usage; and (3) data sensitivity. Trust in the receiver, fair and beneficial uses of data, and lower sensitivity of data collected all contribute towards a more positive perception of the system on the grounds of privacy.

The collection and use of employees' personal data by organisational systems presents its own problems as well. Risks associated with a negative perception of workplace monitoring include: low employee morale, chilling effects, deterioration of work relationships, reduced commitment to the organization, lower productivity and economic loss (Fairweather, 1999; Ariss, 2002; Snyder, 2010; Chen & Sanders, 2007).

There is a gap in the literature concerning privacy and trust issues of learning systems when deployed in organisations that employ the user. It is not clear what are users' perceptions regarding the collection, storage, transfer and use of their personal data by the different stakeholders of these systems. It is possible these perceptions may impact system acceptance and the effectiveness of the learning experience.

The aim of the studies described here was to identify the privacy risks with a serious-games platform called TARGET (Transformative, Adaptive, Responsive and enGaging Environment) and create privacy guidelines for the development, deployment, and operation of learning systems in organisational contexts. TARGET was developed as part of a European Community Seventh Framework Programme. The first game being developed within it, and the one used in these studies, is aimed at developing competence in project management skills. The player controls an avatar in the game that has to complete certain project management scenarios and tasks – e.g. procuring additional human resources for a project to ensure it completes on time. After completing each scenario the player's performance is assessed and the game provides feedback on how to improve it.

To achieve its goals the system collects and stores data on learner-users' results, their performance assessments, and the skills they possess.  It also allows learners to interact with each other through multi-player gaming and virtual social spaces. Enterprise and academic organisations will be the main users of TARGET; however, these studies focus on the enterprise deployment scenario where learners are employees of a large company.

To identify privacy risks, the studies focused on clarifying how learner-users perceived different data practices and what impact those perceptions could have on system acceptance. Study 1 (Section 5.2) consisted of a workshop with TARGET developers aimed at anticipating privacy risks for learners. Study 2 (Section 5.3) built on the conclusions of Study 1 and inquired a small number of focus group student participants about their views on potential collection and use of certain types of data by TARGET. Study 3 (Section 5.4) used the findings from Study 2 to create scenario-based interviews with potential end-users of TARGET to understand how they would perceive its handling of learners' data.

| | **Serious Games** | | |
|---|---|---|---|
| | **Study 1** | **Study 2** | **Study 3** |
| **Section** | 5.2 | 5.3 | 5.4 |
| **Topic** | Privacy risks in a serious-games platform | Collection and use of data by a serious-games platform | Collection and use of data by a serious-games platform |
| **Method** | Group interview (Developer workshop) | Focus Groups | Semi-structured interviews |
| **N** | N/A | 8 | 32 |
| **Date** | Oct 2009 | Feb 2010 | Jun – Nov 2010 |

**Table 5.1: List of Studies in this Chapter**

## 5.2 Study 1

### 5.2.1 *Aims*

A one-day workshop was organised with representatives of the several TARGET stakeholders. System designers and developers of the system and representatives of a large business organisation that would be one of the first adopters of the system were all present.

The goal of this workshop was to identify privacy risks for users playing TARGET serious games in an organisational environment at an early phase in the project's development cycle. The workshop was also aimed at gathering TARGET system designers and developers' views on the types of data the system would collect and use and the types of users who would have access to them.

The workshop was organised by Dr. Will Seager and moderated by both Dr. Seager and the author. The data was analysed by the author.

### 5.2.2 *Method*

The first part of the workshop consisted of a brainstorming session where participants were free to share their perspective on the potential privacy implications of the project. The second part of the workshop was more systematic discussion on: (1) the types of player data the system would generate, collect, store, use, and transfer; (2) the types of users besides players that the system would have; (3) the minimum level of access to each data type required by each user type. To guide the discussion and support the identification of potential privacy issues, a "data/user" table was created cooperatively by the workshop participants. Types of player data were represented in columns and user types in rows. For each cell in the table, the workshop participants discussed whether that user should have access to the data type for TARGET to achieve its goals. While there was unanimous agreement for some of the cells, for others there was debate with some participants arguing for a more liberal data access policy and others pointing out the potential privacy issues that could arise from those policies. A sample of the final agreed table is shown below (Table 5.2).

### 5.2.3 *Findings*

#### 5.2.3.1 Theme 1: Projected Outcome and projected image

One developer (D1) present in the workshop warned that employees selected for training might feel stigmatised. By using a competence development system they could be portraying themselves as needing special education and assistance. D1 mentioned he had worked in a training program aimed at improving employees' technical skills. This program had been resisted because the employees it was targeted at perceived that being asked to participate in the program meant their future employability in the company was in risk. D1 said they thought:

> "I am one of these who will be the first to be laid off when the company shrinks" D1

This suggests that the simple fact of being a user of TARGET may constitute sensitive data.

#### 5.2.3.2 Access Control Matrix

| **User Type** | **Data Types** | | | |
|---|---|---|---|---|
| | ***Learner Profile Data*** | ***Competence Profile*** | ***Social Contact Data*** | ***Learning Plans*** |
| Other Learners | Yes, but anonymous | Yes, but anonymous | No | No |
| Mentor | Yes for people they are responsible for | Yes | No | Yes |
| Supervisors | Yes for people they are responsible for | Yes | No | Yes |
| Competence Managers | No | Yes in an aggregated way | No | No |
| Internal Recruiter | Yes, but anonymous | Yes, but anonymous | No | No |

**Table 5.2: Data Access Requirements Table (Sample)**

## 5.3 Study 2

### 5.3.1 *Aims*

Study 2 had the aim of collecting prospective learners' perceptions of TARGET with regards to the collection and use of certain types of data. As in study 1, the focus was on anticipating privacy issues with the system. As the system did not have any actual learners at this point in time, focus groups with student participants were organised[7].

### 5.3.2 *Method*

In three focus groups, with duration of 90 minutes each, eight participants were shown a video demonstration of TARGET. This demonstration displayed a 3D "lounge" area where players

[7] These focus groups sessions were designed and mediated by Dr. Will Seager and did not, at first, include questions on privacy. The author was able to join the last three of these sessions and to extend the interview protocol to include privacy related questions.

could interact with each other through their avatars and a game scenario where players had to complete a project task by interacting with a computer controlled character.

Participants were asked to express their impressions freely while the demonstration was playing and after it finished. Following a semi-structured interviewing technique, they were asked to point features they liked and disliked in the game. They were also asked about their perceptions of the collection of specific types of data, such as game performance data, and its subsequent potential uses, such as internal recruitment. They were inquired about the possibility of their identity and game performance being visible to other players (e.g.: were they comfortable with game profiles having their real names). Focus-group data was analysed using thematic analysis to find interesting patterns.

These three groups were moderated by Dr. Will Seager and the author. The data was analysed by the author.

### *5.3.3 Findings*

#### 5.3.3.1 Theme 1: Projected Image and projected outcome

Participants in the first focus group were concerned that if game performance scores were visible to all players it would create tension in the organisation. A player would be able to use the game performance of a colleague against him/her in the real world. The same was said regarding the possibility of posting feedback about a fellow player's performance in the game. Players would want to hide negative feedback they had obtained to preserve their reputation.

When asked about the possibility of game performance being used to guide internal recruitment decisions by the human resources most participants reacted negatively. One participant (P4) said that if game data were used in this way she would approach the game in a different way and only play the scenarios where she thought she would get a good score. If game score were anonymous, this same participant said she would:

> *"Feel free to explore stuff that I am not good at and try to learn from it." P4*

This finding suggests that players are less comfortable disclosing performance data that shows them in a negative light compared to data that shows them in a positive light. This is intuitively understandable and, in fact, two participants (P4 and P6) mentioned that they would have no problem sharing game performance results if they were positive. This gives support to the conclusion that *projected image* of a disclosure affects how that disclosure is perceived, which was also supported by other studies in this thesis.

#### 5.3.3.2 Theme 2: Fairness

Participants questioned whether a learning system could correctly assess how good they were at a certain skill and whether decisions based on that assessment could ever be fair. One participant said:

> *"You can just click something in that game and it doesn't really say if you do it as good in real life." P6*

Three participants identified a trade-off between a more human but potentially more prejudiced face-to-face assessment versus a less prejudiced but less contextualised automatic assessment.

This suggests that individuals may perceive certain uses of their data as unfair or without validity. Thus, *fairness* of a data practice seems to be linked to a positive perception of that data practice.

#### 5.3.3.3 Theme 3: Linkability to identity

Participants suggested that it should not be able to identify a player from his or her game identity to prevent negative real world consequences, such as being targeted for having a bad score. This is in agreement with privacy literature that indicates that more personally defining items are usually considered more sensitive (e.g. Adams & Sasse 2001). One participant added that now knowing who other players were would force players to engage in social interaction and through that build relationships:

> *"One part of team building is getting to know people and that involves asking questions and talking to people."P8*

This is agreement with intimacy definitions of privacy (see Section 2.2), which suggest relationships are built through selective-disclosure of personal data.

## 5.4 Study 3

### *5.4.1 Aims*

This study continued to explore how potential users of TARGET perceive the collection and use of different types of data by the system and its other users. The aim was to identify the factors that influence how players perceive different data practices in the context of using a learning tool such as TARGET in their own organisational environment. In particular, the goal was to understand: (1) what specific privacy risks would players identify in the game; (2) how players expected their data to be used by key stakeholders in the organisation deploying the game – e.g. managers and other employees; (3) which design recommendations could be made to support privacy in TARGET and other learning systems.

32 semi-structured interviews were conducted with potential end-users of TARGET. Since the learning system was not developed at the time of the interviews and because it is a challenge to gather non-contextualised privacy perceptions, the study relied on: (1) a video-demo of TARGET to help participants understand how the system would work and how players would interact with it; and (2) written scenarios describing potential uses of player related data, such as performance scores, to contextualise the questions and collect more realistic perceptions from participants (for other examples of scenario use in privacy research see Iachello and Hong, 2007). 16 of the 32 interviews were conducted by Dr. Charlene Jennett and focused on trust perceptions. These interviews were re-analysed by the author. The other 16 interviews were conducted and analysed by the author and focused on privacy perceptions.

## *5.4.2 Method*

### 5.4.2.1 Participants

Participants all had at least one year work experience in an organisation with more than 100 employees. 27 were recruited from a university participant pool and five through personal contacts. 17 were female and 15 male. Their ages ranged from 20 to 59 years old; median age was 26 years old. 18 worked in the commercial sector, 11 in the public sector and 3 in "other". The median number of employees at participants' employers was 800 employees. 25 participants reported that they had experience playing digital games.

### 5.4.2.2 Video Demo

The demo showed how the player's avatar would interact with different elements within the game. It first showed a scenario in which the player was required to complete a project management task. To achieve this, the player avatar had first to negotiate with an in-game character representing a human resources employee.  After a successful negotiation the player avatar was able to finish the task and complete the scenario.

### 5.4.2.3 Scenarios

The scenarios that supported the privacy interviews depicted potential data practices that, according to the stakeholders, could take place once TARGET was deployed in an organisation. These practices varied on: (1) data receiver; (2) type of data; and (3) use of data. Six scenarios were created, representing the following situations:

1. Displaying performance data as a score on a public scoreboard and alternatives to that option;

2. The use of aggregated performance data at the team level to guide training decisions;
3. The use of performance data to guide internal recruitment decisions,
4. Playing a scenario with other players with everyone using pseudonyms;
5. The player profile, the information it contains, and other players' access to it;
6. Interaction with a mentor and what type of information they would have access to;

For example, Scenario 2 was:

> *You discover that the human resources (HR) department within your organisation are compiling your game scores and the scores of other players to build-up a profile of the competences in different parts of the organisation. They use this data to help identify skills shortages within the organisation and use this information as a basis for identifying training and development needs. You have been told that it is not possible to identify individual scores from these data i.e. the scores are aggregated at the level of work group and above.*
>
> *What are your reactions to this scenario?*
>
> *Would use of the scores for these purposes affect how you play the game?*
>
> *What would be the advantages of using performance data in this way? And what are the drawbacks?*

The trust scenarios looked at two types of trust: (1) trust in the system; and (2) trust in other players of TARGET:

1. What is the best way for a game to be implemented in an organisational setting?
2. Who should have access to the data?
3. How should the data be used? E.g. score boards, internal recruitment, identifying training needs.
4. How would you like to go about making initial contact with other players?
5. How would you like to go about maintaining / limiting contact with other players?
6. Would you prefer real identities or pseudonym identities?

#### 5.4.2.4 Procedure

Participants were first briefed on the goals and features of TARGET and then showed the video demo describe above. After watching the demo, participants were asked to imagine TARGET was being deployed in their organisation and to interpret the written scenarios in that context. After reading each scenario description participants were inquired about their perceptions of the data practices depicted in it. Privacy focused interviews lasted between 60 and 90 minutes and participants were rewarded with £15. Trust focused interviews lasted between 30 and 60 minutes and participants were rewarded with £10.

Interviews were audio-recorded and the transcripts were analysed using grounded theory (Strauss and Corbin, 1998). According to this method, data is analysed in different stages: open coding, axial coding, and selective coding. Dr. Charlene Jennett and I first analysed the data separately and created distinct grounded theories for trust and privacy respectively. The codes created were then pooled and went through a new stage of selective coding to create a joint model spanning both trust and privacy factors. This model is presented below.

### *5.4.3 Findings*

Analysis of interview data revealed several concerns participants had about TARGET and how it handled player data (see Figure 5.1). These concerns were traced to a number of factors that can be divided in two main groups: (1) factors relating to how the system collects, stores and uses data; and (2) factors relating to in-game interactions with managers and colleagues.

According to the project's specification at the time of the study, TARGET has two main game areas: game scenarios and the lounge. When playing a scenario, players interact with different game elements to achieve a specific goal. The game assesses and provides feedback on their performance. Thus, performance data is recorded and used by the system. History of scenarios played and the time playing each one could also be recorded. In the lounge players can chat with each other using text or voice. Technically, these conversations between players could be recorded by the system. Additional data relating to the real-life identity of the player, such as demographic or job data, could also be used to create a profile attached to each player's avatar.

In addition to players, TARGET specified the existence of at least two other types of users: mentors and managers. Both these user types could monitor the performance of the player, although the extent to which they could do so was not decided at the time of this study. Their roles in the game were similar to the goals of these roles in real-life organisations. Mentors were expected to provide feedback on player's performance and advise them on which type of skills to develop (and which scenarios to play to achieve that development). Managers were also expected to provide feedback on players' performance, to define skill development goals and to inform the player of skills s/he was required to develop to perform better in future real-life projects.

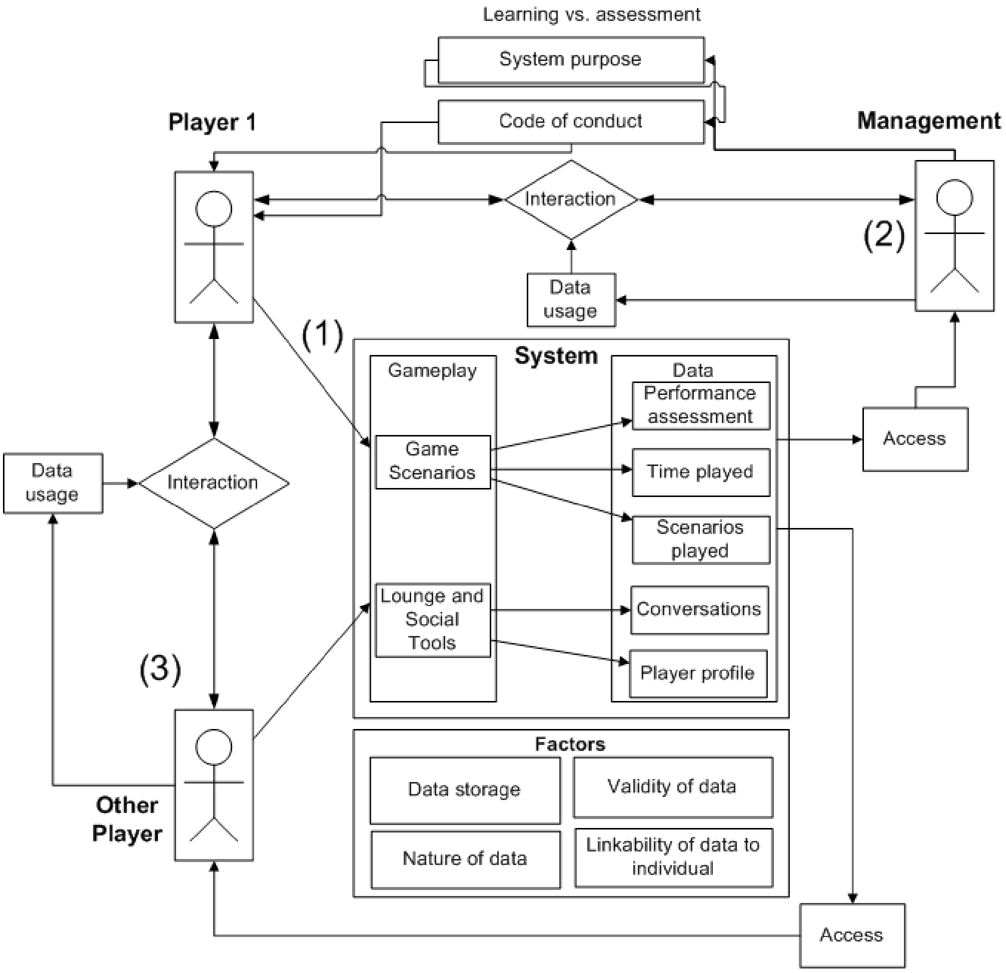


**Figure 5.1: Factors affecting perception of TARGET's data practices**

### 5.4.3.1 Theme 1: Data Security (Data Storage in the model)

5 participants mentioned it was important to know where data generated by the TARGET game would be kept and what security measures would be used to protect it.

> *"[I]'d like to know […] where they are keeping the data, […] what kind of security they are using, what kind of protocols - I would ask a lot of questions." P8*

One particular concern was that management of the system's data could be outsourced to a company other than their employer and that it could even be transferred outside the UK or the EU.

> *"Of course they were trying to cut costs so they went off to India. And because obviously the data has been moved outside the EU they had to seek the approval of every employee for their data to be moved. And I actually said no I don't want it to be moved. So it's funny. I was quite happy for it to be outsourced to someone who was in the UK but it's like the moment it goes to India - and that's purely because of you hear the media stories about some of the call centres offshore not being quite so secure as they should be." P9*

There was also a concern with unauthorised individuals getting access to players' personal data as a result of a security breach.

#### 5.4.3.2 Theme 2: Projected Image (Nature of Data in the model)

As in Study 2 (see Theme 1: Projected Image and projected outcome in Section 5.3.3.1), participants pointed out that they would not mind sharing performance related data that showed them in a good light, but that if data revealed weaknesses in their competences they would not like it to be available to other people.

> *"If you did poorly then no, you wouldn't want anyone else to know would you" P7*

> *"Maybe if you think you're going to do well then you wouldn't mind your results being displayed." P3*

15 participants mentioned that bad performance assessments might be interpreted as a sign that the player was not fit for his or her job in the company.

> *"Will they look at them differently, because if they feel that they have got a bad score and they feel that they have underperformed or they are not very fit enough for the job, or you know, so this is the reason why someone may look at someone else in a disadvantaged way." P2*

> *"'Cause definitely you wouldn't want a competence level minus [laughs]. […] No I don't think anybody would want that! [Laughs] Yeah I think anything that's got competence in it. If somebody scores low it might put them in a foul mood [laughs]. [...] 'Cause it doesn't sound very good […] because if it's in negative then its incompetent isn't it? I suppose that's the implication." P12*

There was also a risk that if players spent too long playing specific scenarios that could reflect badly on them. The scenarios played by a player could also be considered sensitive data because they could potentially indicate what weaknesses the player has.

#### 5.4.3.3 Theme 3: Fairness (Validity of Data in the model)

25 participants questioned the ability of the game to correctly assess the competence level of players. One reason given was that the scenarios in the game might not portray actual job tasks realistically or cover all the nuances of the job domain.

> *"I suppose it would depend on the actual game as a tool, that would be the first thing in like how accurate is the game for actually measuring what it says it measures, so that would be the first question, so I'd be thinking 'Well is it actually measuring what it says, am I being disadvantaged in a particular way?'" P4*

Another was that player actions in the game were artificialised because they were mediated by a computer.

> *"So even if this RPG is fantastic, it's not the real thing and that's what you have to keep in mind, it's not the real thing. So, it's very good, you can identify a lot of training gaps or performance mistakes or skills gap, I'm not saying this is not good, but this shouldn't be confounded, it shouldn't be taken by the real thing." P8*

> *"I think this case, what comes to my mind at first is that you cannot really replace the reality with a game" P13*

As a result, assessing players based on game performance was considered unfair.

> *"Well in some ways it doesn't seem fair because I'm employed to do work and I feel I should be assessed on my work, not on other things which aren't my work. She's assessing me on something which isn't work, it's a… […] You can argue that it's a simulation of what my work might be. Somehow it seems wrong that…I feel that if I'm employed to do work that's what I should be assessed on rather than other things." P10*

6 of these participants mentioned that human and automatic assessment of competences had differences. This issue had already been brought up in Study 2 (Section 5.3.3.2). 5 participants argued that a human assessor could contextualise the assessment process by asking questions to the player, while a computer could not. Another participant, thought an automatic assessment was fairer since it was not reliant on subjective considerations or biases.

A final related concern was the potential impact of confounding factors on game performance. Experience with computer games was one of these factors that could affect how well a player was at playing the game. Other factors that could impair player performance included: (1) technical issues, like the system crashing; and (2) personal issues, like returning from maternity leave. Participant suggestions to deal with these problems were that the whole personal context of players was considered when assessing them and that there should be a mechanism for players to correct erroneous data in the system.

#### 5.4.3.4 Theme 4: Linkability to Identity (Linkability of Data to Individual in the model)

13 participants mentioned that the use of pseudonyms instead of real names in the game would make them interact in a more relaxed manner with it, since they would feel less threatened by the potential embarrassment of having bad performance assessments.

> *"If that was a pseudonym and the names were only available upon request, like when you asked the person, then perhaps there's a slight bit more leeway. Like, it helps to make people focus on the game instead of focus on who is playing it and what I have to do to perhaps interact with those people. You just focus on the game instead of the pseudonyms. Like if the game is trying to impart knowledge to you, then it's a lot easier to have pseudonyms. People just focus on the right thing." P31*

> *"…from the perspective of the people doing the training, if they have… if they are anonymous, that means if they make a mistake then their bosses wouldn't think they are stupid." P30*

One participant argued against the use of pseudonyms, saying that could make players lose interest in the game since their performance could not be traced back to them. There would be less motivation to take the seriously. Another drawback to using pseudonyms was the potential impact on socialisation. 14 participants said that they would be wary of interaction with other players in the social areas of the game if they did not know who they were talking to. One concern was that players might not feel accountable for their actions and thus behave inappropriately. Another, was that they would find difficult to judge the benefit of talking to someone if they did not know who they were.

Aggregation of performance data was seen by 7 participants as having a soothing effect on how the game was perceived. They argued players would feel freer to experiment and take risks within the game without fear of making mistakes that could be linked directly to them.

> *"Well assuming it was a large enough group and that it was hard to disaggregate me out of it I think it would not really affect how I played the game, no. I think I would probably try and play the game to the best of my ability in order to make use of the opportunity to learn because I would not feel threatened by it." P10*

> *"Yeah. You wouldn't feel like it's a bad tool to use. Everyone would be more open, and receptive to getting advice from this game, because it's a group thing." P11*

3 of these participants suggested that, since most work in companies is done collaboratively, performance data should be aggregated at the team or work group level. 6 participants provided a counterpoint to this argument. They suggested that aggregation of data could lead to "tarring everyone with the same brush". This could cause players to be assigned training they did not need simply because the group had underperformed in a specific task. 3 of these participants mentioned that some players might work less as result of data aggregation, and another 4 stressed the importance of having feedback at the individual level to develop one's skills.

### 5.4.3.5 Theme 5: Data receiver

#### *5.4.3.5.1 Relationship*

25 participants argued that individuals with different roles in the organisation should have differentiated levels of access to player data; however, there was no agreement among these participants about which data each role should have be able to access.

> *"It depends again, so for me I'd be thinking to myself "Well is it just me or is it me and my manager?" or "Is it just me or is it me and the system administrator who has access?" so I'd be concerned about access issues […]" P4*

19 of these participants said that managements should have access to player data, but not colleagues.

> *"I wouldn't mind my manager seeing it. Colleagues, maybe a different story. Cause it's your manager mainly deals with your professional development. Colleagues you can discuss things, but when it comes to professional development, and meetings it is always with a manager." P2*

The remaining 6 participants revealed the opposite perception: colleagues should be able to access the data, but not management.

> *"It's precisely ... these people who can make decisions about me are precisely the people who I don't want them to have access to this information. If you said that they are my colleagues or eventually someone who works for me, but if it's my boss, he's the guy or he's the one that I don't want to have access to my personal data." P8*

#### *5.4.3.5.2 Perceived relevance (Need to know)*

An important factor was whether the data receiver had a legitimate purpose for accessing the data, such as providing guidance to the player. This is very similar to the *perceived relevance* of a data request theme identified in the literature review (see Section 2.1.1.2).

> *“It’s just you don’t want everyone to know how you’re doing. Everyone who doesn’t actually have a reason to know that kind of information.” P7*

> *“But is there a real need for me to know that Helen, who I’ve never heard of only got 65%? […] I don’t think that’s appropriate.” P16*

#### *5.4.3.5.3 Trust*

Also important for 3 participants was the level of trust in the data receiver. Players who trusted their organisations, or specific departments or people in it, would me more likely to be comfortable sharing game related data with them.

> *“[…] I think most people within a corporate environment trust their HR Department to keep things secret […]” P9*

> *“[…]I’m used to an organisation to say one thing ‘Oh we’re only going to do it like this’ and they collect all the data and then six months down the line they change their mind and use the same data to do the thing they said they weren’t going to do so…” P4*

### 5.4.3.6 Theme 6: Projected outcome

The expected consequences of playing the game could have either a positive or negative impact on perceptions of TARGET. As was mentioned above (see Theme 2: Projected Image (Nature of Data in the model), participants expressed concern regarding how negative performance assessment would be interpreted and how they would reflect on players.

> *“It depends on what’s the kind of outcome of that assessment, what does it mean for my …? Is it just … as it’s called a game so is it just kind of a learning tool game, here’s your assessment, like any other game you score points or you do whatever, but more seriously speaking kind of what does it imply I guess for my role and my job and my responsibilities, my salary, all of that? I don’t know. It depends on how that is all linked.” P14*

Extending this theme, 14 participants said there was potential for the players' peers to humiliate them if they had a bad assessment. Humiliation could take the form of gossip, ridicule, or bullying.

> *"You might be ridiculed if you're getting low scores in a business environment." P1*

> *"They're looking at cold hard statistics without any context. And it could lead to nasty things like bullying and stuff, if someone's got really poor scores." P9*

According to 14 participants there was further risk of career-oriented colleagues to use these negative data to gain leverage on players when competing for the same positions in the organisation or if they had a previous conflict.

> *"[You] might feel funny about your score being on the system because people might want to use that strategically against you in other ways […] If they're like … well if people are trying to position themselves for promotion and things like that in the organisation then people tend to collect bits of information about their so called opposition as they're kind of moving up, so if they're doing that then just little things they can kind of drop in to try and kind of put you down or kind of diminish you in whichever way to make themselves look better. […] So it depends, they would use information from all sorts of different sources to do that." P4*

## 5.5 Discussion

Most concerns that emerged from the three studies were related to the *projected image* resulting from playing a serious-game in an organisational context and also the potentially negative consequences - i.e. *projected outcome*. Several risks related to negative game data "leaking" to the real-world were identified. In Study 1 (see Section 5.2.3.1), the simple fact of being a user of training system within a company was identified as a sensitive fact, since these employees could be seen as lacking some skills and being in a more fragile job position. In Study 2 (see Section 5.2.3.1) and Study 3 (see Section 5.4.3.2) the reputational impact of negative performance in the game being seen by other employees was mentioned as a risk for players. In particular, participants seemed concerned with the possibility of looking incompetent in front of their peers and even being humiliated or the source of gossip. There was also concern with the potential impact of negative game performance on one's career. On the other hand, if data showed participants in a good light, they were more receptive to sharing it. This is agreement with past research that suggests that negative data is more sensitive (Adams, 2001). The implication for organisations deploying this type of systems is that the learning experience can be affected because taking risks and not being afraid to make mistakes is a vital part of the learning process.

One way to address this issue is to insulate the game experience from real world identities using pseudonyms or by anonymising the data. In fact, how linked game performance was to the identity of the player was mentioned as an important factor in both Study 2 and Study 3. Anonymisation and pseudonymisation were seen as protecting players from looking bad and other negative consequences, and, consequently, allowing them to play in a more relaxed manner. On the other hand, this split between the game world and real world could have some negative consequences. Some players may experience a lower level of motivation if they perceive there are no rewards for good performance in the game. It is part of the philosophy of serious games to make use of elements such as competition between players to improve the transfer of knowledge. Preventing players from comparing their performance to each other could potentially harm the learning effectiveness. Moreover, it would make it more difficult for players to get meaningful feedback from managers and mentors. At the organisational level, it would impair the leveraging of the game environment and data to create social networks and communities of practice. One possible way to balance these two views is to allow players to control their own data and selectively disclose their game data to other parties, such as colleagues or management.

How linked the in-game identities are to real-life identities also exposes a trade-off between trust and privacy. Having the player's real name associated to his avatar supports temporal, social, and institutional embeddedness in the game increasing the likelihood of trustworthy behaviour (Riegelsberger, 2005). However, it can work against players if their game data is used in a way that they find invasive, such as if management uses performance data to make decisions that have a negative impact for players' careers. Also, real life prejudices and biases could negatively affect the interactions between players and the experience of playing the game. The use of anonymous avatars supports privacy insofar as game data and experiences will not be linked to a real-life identity, but it undermines trust by not allowing stable identities across time. A promising middle-ground is the use of pseudonyms, which can provide stable identities to increase embeddedness without reducing privacy.

Participants in Studies 2 and 3 also revealed mistrust about a game being able to correctly simulate real world professional tasks and reliably assess players performance. Evaluating an individual according to game performance was perceived as *unfair.* It was suggested that human assessment could be fairer, but this exposed a trade-off between automatic and human assessment. If the player's performance is reviewed by a person who then provides feedback, then the player has a chance to contextualise and justify their actions in the game. It gives her an opportunity to clear misunderstandings or explain the why of a particularly bad performance. Automatic assessment does not allow this contextualisation. On the other hand, human assessment is subject to the biases and prejudices of the assessor. While more deterministic, automatic assessment would judge a player solely on in-game performance and in an unbiased way.

Features of the data receiver - both organisational and individual data receivers - were also mentioned as relevant for the perception of the data practices surrounding the deployment of the game in Study 3. At the organisational level, the main concern was that data would be kept secure and not transferred outside the country. At the individual level, wanted their game data to only be accessible to individuals whom they trusted, who had a specific role within the organisation, and who had a legitimate reason to have access to the data. This is consistent with privacy literature: individuals' privacy perceptions depend both on their perception of the data receiver (see Section 2.1.1.4) and whether that receiver requires the data to fulfil the communicated purpose of the data collection (see Section 2.1.1.2).

These three studies revealed a series of factors that may impact player perceptions of TARGET with regard to the collection, storage, use, and transfer of players' personal data. These factors are synthesised in the model in Figure 5.2.

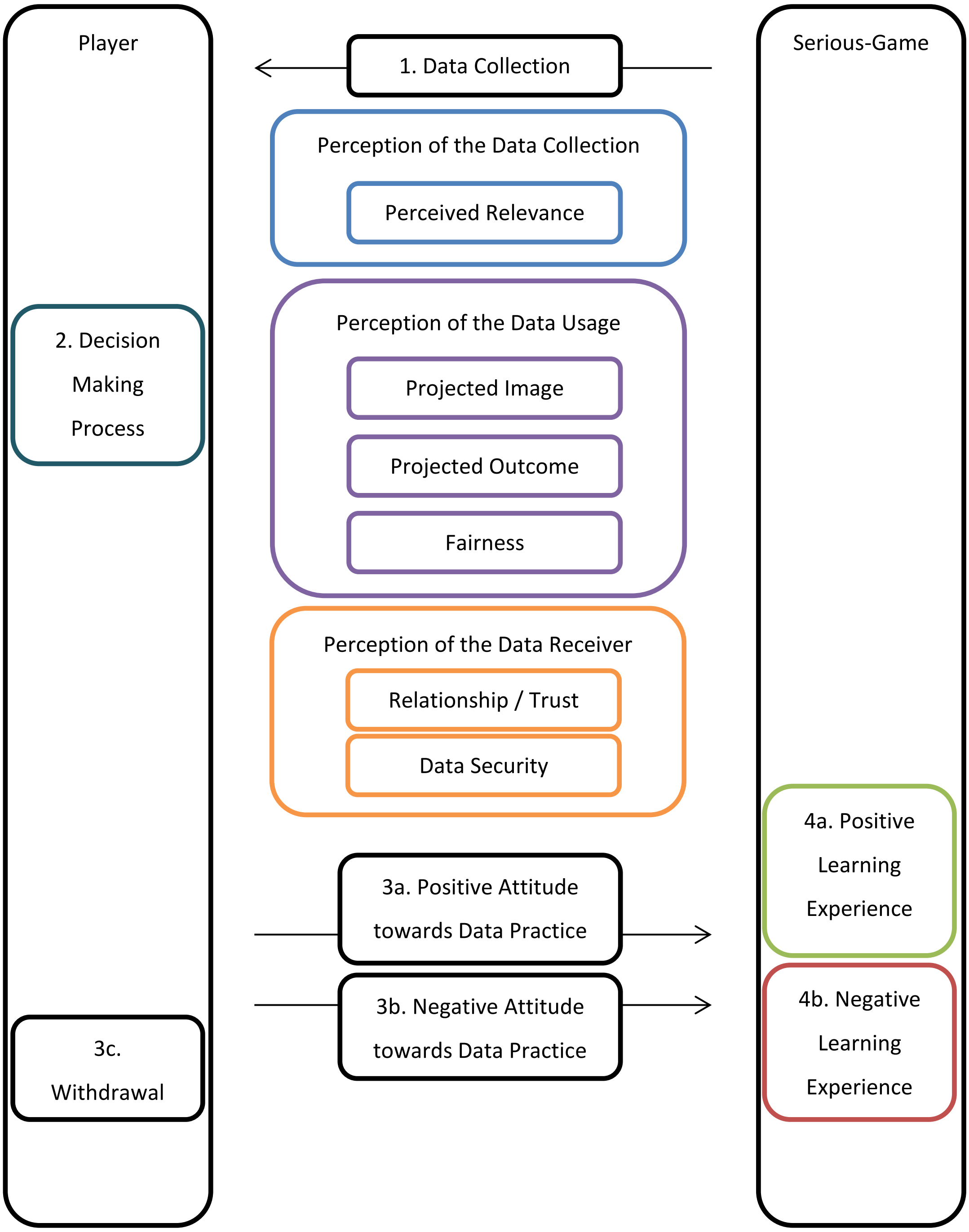

Player
1. Data Collection
Serious-Game
Perception of the Data Collection
Perceived Relevance
2. Decision Making Process
Perception of the Data Usage
Projected Image
Projected Outcome
Fairness
Perception of the Data Receiver
Relationship / Trust
Data Security
4a. Positive Learning Experience
3a. Positive Attitude towards Data Practice
3b. Negative Attitude towards Data Practice
4b. Negative Learning Experience
3c. Withdrawal

**Figure 5.2: Perceptions of data collection and usage in serious-games deployed in organisational contexts**

# Chapter 6: CENSUS STUDIES

## 6.1 BACKGROUND

The 2011 UK census was sent to every household in the country and asked for details on age, job, education, ethnicity, and religion of its members among other questions. In the UK, a census of the population has been taken every ten years since 1801, with the 2011 one being the 21st. While originally only the number of births, deaths, and marriages were registered, the census evolved to collect a much larger range and quantity of data.

The main goal of the census is to obtain a snapshot of the UK population on a given day to provide a basis for planning public services such as health, education, or transport (ONS, 2013). A census undercount (missing significant numbers of responses) can lead to local populations being underestimated, which means they receive less money from central government. For instance, in the 2001 census, Westminster's population was estimated to be 181,000 - 65,000 less than the 2000 estimate - causing the council to lose 6 million pounds in annual grants from the government (Boyle & Dorling, 2004).

In 2011, census staff tried to combat non-response by identifying people who had not completed the forms. If they persisted in their refusal they could be fined up to £1000 or face criminal charges (Ross, 2011). It was also the first year that it was possible for UK citizens to submit their census online. However, neither of these measures tackles one of the causes of non-response: not all citizens are comfortable disclosing the personal data asked in the census to the government.

### *6.1.1 PRIVACY CONCERNS*

The census data collection has been criticised as an invasion of privacy. Even before the first UK census, one member of the House of Commons, in 1753, called the idea of taking an annual account of the population "an interference into domestic concerns" (The Sidney Morning Herald, 1851). More recently, privacy advocates have raised concerns that census data can be used for purposes other than the ones stated in the forms (Boyle & Dorling, 2004). The fact it contains rich details about a whole country, including small communities, makes it a valuable resource for scientists: it allows them to understand migration flows, changes in circumstances of specific populations, or estimate birth, death, and disease rates. But census data is also employed by marketing companies to profile individuals according to their geo-demographic details (e.g. Mosaic UK; Experian, 2013). This can result in social sorting, where individuals are offered services under harsher conditions (e.g. high insurance premiums or interest loans) or simply denied services because of the way they have been profiled (Lyon, 2003).

It has been argued that these uses of census data are not part of the social contract between the state and the citizen completing the form (Heeney, 2012). Individuals do not expect their details to be used in such ways and thus, the contextual integrity of the data is violated (Nissenbaum, 2004). The ONS assures individuals of the confidentiality of census data, stating that their "personal census information is not shared with any other government department, local councils or marketing companies" and that the data will only be used to "produce statistics and for statistical research" which "will not reveal any personal information." (ONS, 2013) This assurance ignores that with modern machine learning and data mining techniques statistical data can be de-anonymised or used for profiling purposes that have real consequences for individuals (Heeney, 2012). One does not have to go further than the stated goal of the census, making public funding decisions, to see this. While based on statistical data, decisions on how much money to grant each council will undoubtedly affect the citizens that live there.

### *6.1.2 Previous Research*

Research into the factors that influence census response rates has mainly been conducted in the US. A low-level of response to the 1990 US census led the Bureau of the Census to commission a study into the causes of non-response (Singer et al., 1993; Couper et al., 1998), which revealed that privacy and confidentiality concerns significantly affected the likelihood of submitting the census forms. The authors defined confidentiality as keeping data given to one receiver inaccessible to other receivers and privacy as keeping personal data inaccessible to others in general. They also found race to be a significant determinant for response behaviour: black non-Hispanic individuals were significantly less likely to submit their census than White non-Hispanic or Hispanic individuals. The study was repeated for the 2000 US census with similar results (Singer et al., 2003): the concern that census data could be misused was again a predictor of response behaviour. Furthermore, the length of the form participants received at home (in the US there is a long and a short version of the census) had a significant effect on response: individuals who received the short form were more likely to submit it compared to the ones who received the long version.

Privacy concerns were also behind the census boycotts in Germany in the 1980s (Efferink, 2012). Vague statements about sharing data between different government organisations in the census guidelines led to activists protesting against the 1983 census and calling a boycott. Many young citizens had suffered harassment from security forces and were deeply suspicious of the government data collection efforts. Technological advances had also made it easier to share data between institutions. The planned boycott started to get support from other citizens. The census was eventually deemed unconstitutional by the constitutional court, which ordered the government to redesign it. It was then re-launched in 1987, only to be boycotted again.

In the UK, Simpson (2003) provides some information regarding the 1991 and 2001 censuses non-response rates. Non-response was higher among young adults or socially excluded individuals, such as people who had recently migrated, were living by themselves, or were unemployed. In terms of item non-response, the 2001 census was worse than the 1991 one, with items like employment status, qualification, and workplace address having a non-response rate between 5% and 10% across the whole country. The items with the lowest non-response rates were age, sex, and marital status (less than 1%). The different levels of non-response for the census items support current privacy theory, which states that personal data items have different levels of sensitivity which directly affect disclosure rates (see, for example: Metzger, 2007). The ONS uses several techniques to compensate for missing data, such as filling empty fields with estimates, but the quality and value of the data are still undermined.

The consequences of both census and item non-response underline the importance of minimising negative reactions to the census. In this chapter, two studies that investigated people's perceptions of the 2011 UK census questionnaire – and, in particular, their privacy concerns – are described. The goal was to capture citizens' opinions while the experience of filling in the census was still recent; thus, both studies were conducted in early April - a week after the census day, 27 March, had passed. In the first study, 11 participants from an opportunity sample were asked to fill in their census forms in the presence of an experimenter while they thought aloud about their perceptions of the census questions. The interviewees were probed about their attitudes towards the different questions and the reasons for their perceptions. Interview findings informed the design of a second study, an online questionnaire inquired a national representative sample of 174 participants about their comfort disclosing each of the census items and whether they had chosen to engage in privacy protection behaviours, e.g. non-response when filling the 2011 census.

| | **UK Census 2011** | |
|---|---|---|
| | **Study 1** | **Study 2** |
| **Section** | 6.2 | 6.3 |
| **Topic** | Census data requests | Census data requests and privacy protection behaviours |
| **Method** | Semi-structured interviews | Online survey |
| **N** | 11 | 174 |
| **Date** | Mar - Apr 2011 | Apr - May 2011 |

**Table 6.1: Studies in this Chapter**

## 6.2 Study 1

### 6.2.1 Aims

A series of interviews aimed at getting an insight into how individuals perceived the UK 2011 census questions from a privacy point of view were conducted. The goal was to collect participants' overall experiences of filling in the census form (e.g.: when they submitted the form, whether they completed it online or on paper) as well as their perceptions of the value proposition of answering and submitting the census, i.e.: whether participants considered it worthwhile to complete the census given any potential privacy concerns regarding the data they were asked to disclose.

### 6.2.2 Method

11 participants were recruited via an opportunity sample (6 female, 5 male). Their ages ranged from 19 to 56 years (mean age=28 years, SD=10.38). 4 were full time students, 4 were unemployed, 2 were full-time employed, and 1 was part-time employed/student. All participants were eligible to complete the 2011 UK census. For the majority (8 participants), it was the first census they had been required to complete. One participant had also completed the 2001 census, and another could not remember whether or not she had completed a previous census.

Participants were given a document containing the text describing the purpose of the 2011 census:

> *"A message to everyone - act now. Everyone should be included in the census - all people, households and overnight visitors. It is used to help plan and fund services for your community - services like transport, education and health. Taking part in the census is very important and it's also compulsory. You could face a fine if you don't participate or if you supply false information. Your personal information is protected by law and will be kept confidential for at least 100 years. So help tomorrow take shape and be part of the 2011 Census."*

Participants were also given printed copies of the 2011 census, which consists of three sections:

1. Household questions: 14 items, to be completed on behalf of all household members;
2. Individual questions: 43 items, to be completed by each member of the household; and

3. Visitor questions: 4 questions, to be completed on behalf of anyone visiting on the census day, Sunday 27 March 2011.

One-on-one semi-structured interviews were conducted in a lab setting. First, participants were asked if and when they had submitted the form and what their general knowledge about the census was before they filled it in. They were then asked how they felt about the census being compulsory and how important they thought it was to complete it. After, they were asked to fill in a copy of the census while “thinking aloud”, i.e.: voicing their perceptions of each of the census’ questions. At the end of the interview participants were again asked about their general impressions of the census form and its questions, potential privacy issues, and the benefits of submitting it.

Interviews took between 30 and 45 minutes and were audio-recorded. At the end of the interview, all participants were fully debriefed and received £5 for taking part. Filled-in census copies were either taken home by the participant or destroyed.

### *6.2.3 Results*

Interviews were transcribed and analysed using the thematic analysis method (see Section 3.2.6.1.1) to identify passages of text which are representative of some interesting pattern, coding them in consistent fashion, and then grouping those codes in themes that help make sense of the data and answer the research questions. Of particular interest for this study were quotes that revealed the factors that influence participants' perceptions of the census in general and of particular census questions. Six themes discovered in the interview data are discussed next.

#### 6.2.3.1 Perceived Relevance

The most commonly expressed theme (10 participants) in the interviews was that of perceived relevance of a question. Participants perceived a question as relevant if they understood why it was being asked in the context of the census, and how it related to the stated aims of the census: planning and improving local community services. When participants understood the purpose of a question, they had a more positive perception of that question. For example, Participant 3 (P3), when discussing census question: "How do you usually travel to work?" said:

> *"I think that would be quite important. They need to know those things, for transport and that, I think that's really important." P3*

Another participant, when discussing census question: "What type of central heating does this accommodation have?" said:

> *"So it probably wants to get a measure of the sort of heating, and perhaps how the government can target things like loans for solar powers and things like that, trying to be more environmentally friendly. So in a way I was kind of pleased that was in there, strangely enough." P5*

Questions not perceived as relevant were those where participant did not understand why it was being asked in this context. When this was the case, participants would question why the data receiver needed that data, and what they would do with it:

> *"The only problem I had was with overnight visitors. I don't know why they would count if they are just staying for a short time frame." P8*

When they did not understand the purpose of a question, participants would sometimes advance their own interpretations for why a question was being asked which were often wrong:

> *"I don't see the relevance of this question either really. Is it to catch people out, this question's in to prove people are an illegal immigrant, I don't know." P5*

#### 6.2.3.2 Projected Outcome (Secondary Data Use)

Six participants mentioned the data being collected would be used for purposes other than the ones stated in the census form: planning and improving local community services. Their main criticism was lack of transparency of data usage and data receiver. While four of these participants suggested ways in which census data might be abused, the two others were simply sceptical that the data would be put to good use, without pinpointing specific fears or concerns:

> *"What good are they going to do with our other information not related to health, education, transport? Like, what good could come out of that information really? It's only negative, if you think about it now." P10*

Potential secondary uses of census data mentioned by participants included fighting terrorism or doing "ethnic-based" stats; checking if people were hosting lodgers and not paying tax on their earnings; or passing on health information to the NHS or health insurance companies so that they could charge more for their services. Participant statements implying data could be used for secondary purposes had a negative connotation. Participant did not mention secondary data uses they thought could be beneficial. For example, a participant, when discussing census question 13: "How is your health in general?" said:

> *"Well they could use that... they could pass your information on to health insurance, and then if you want to get health insurance they might try and charge you more money" P11*

### 6.2.3.3 Convenience and Effort

The effort required in answering a question seemed to have an effect on how that question was perceived and how participants chose to answer, ignore, or lie. For example, questions about visitors were considered by five participants to take too much time and effort to answer because they required participants to remember if they had visitors on a specific (past) date, and to find out and fill in their details if they did. These participants admitted that they might have said they did not have any visitors even if they actually had:

> *"First of all, maybe I won't know all the information of theirs. And I don't think I would go the extra step of calling them and asking them for all their details. I would just leave it blank, honestly. Yeah." P4*

Participant 5, when asked whether s/he would answer the census questions relating to visitors said:

> *"Probably not. Because nobody is really ever going to find out, and I don't see the point. And if you have a lot of visitors over then I really don't want to spend another half hour filling boxes [laughter]" P7*

Convenience also played a part in the format participants chose to submit their form. A majority of eight participants chose to fill in the paper version of the census. The fact that the paper census form was "right there" in front of them made it simpler for them to fill it:

> *"I had the paper version sent so I just filled that in, rather than get my laptop out and login... it just seemed easier to do the paper version." P10*

> *"I'm quite a technical person, so you would thought that I would have gone for the computer version, but it just seemed easier. You have it [the paper form] there in front of you and you can for it at your own pace." P5*

### 6.2.3.4 Sensitivity

Eight participants categorised some data items being requested as "personal" or "not personal". They were less comfortable disclosing items they categorised as personal and more comfortable disclosing non-personal items. When a data item being requested was considered too personal to disclose five participants mentioned they would equate not disclosing it or even lying:

> *"I think I would put no, because y'know I have had a health problem, which I think is sort of significant, but I think that is a bit too personal so I would put 'no' there." P3*

Participants seemed more likely to be comfortable with the disclosure of items not seen as personal:

> *"As long as nothing is personal, personal things, then I wouldn't disclose. But these things are fine." P4*

Three participants described questions as asking for "statistical" data, "demographic" data, "common" data, or "descriptive" data. All these categorisations were associated with a decreased sensitivity of the data:

> *"Q4 is also demographic question, so it also makes it comfortable with that." P7*

> *"Yeah, it's just one of those questions that's always there, in that particular order, you know ‘name, gender, date of birth, address, marital status, country of birth' and so on. It's something that you just get used to filling in and you don't really think about it anymore, why it's going to be used or how it's going to be used." P10*

Contact data, on the other hand, was seen as more sensitive because it could be used to contact the respondent or his/her employer:

> *"Well anything on how to contact me, that I wouldn't have had appreciated." P10*

#### 6.2.3.5 Privacy Protection Behaviours

In addition to omitting data due to the effort involved in answering, five participants also implied they might not answer or lie in some questions due to privacy concerns, such as in health or visitor related questions:

> *"My mum did put incorrect information on the form, because my mum thought some of the information was inappropriate. For example, how many... have any lodgers been in your house in the last two weeks, my mum felt why does she need to be telling the government this type of information? Because it's her property, she should be allowed to have there who she wants, when she wants, and not have to explain to the government why." P11*

Regarding having to provide his/her phone number participant 10 said:

> *“That was probably the only thing I hesitated to add. And then I just thought, should I just rip up the form and throw it away anyway?” P10*

One participant (P5) considered other respondents were likely to lie on housing and immigration-related questions for fear of the consequences. Another participant (P10) thought some people might lie on job related questions if they were evading taxes for example.

#### 6.2.3.6 Projected Image

The image projected by responding to a specific question in a certain way seems to impact the likelihood of the respondent actually answering. Three participants expressed that they might not have answered questions on qualifications if they thought it did not make them look good. On the other hand, they did not have any problems giving answers that portrayed them in a positive light, like the fact that they worked for a reputable company or had high qualifications:

> *"I think if people are not educated they wouldn't want to answer that question. I'd feel obviously comfortable to answer it, but if I wasn't educated I wouldn't want to answer it. […] I'd feel like they might underestimate my intelligence or they might look down...." P2*

The same idea seemed to be implicit in the "nothing to hide" comments of four participants. They did nothing wrong or criminal or that makes them look bad therefore they do not mind providing the data:

> *"I don't think I engage in too many bad things, such criminal acts, so I don't mind disclosing all that" P4*

## 6.3 STUDY 2

### *6.3.1 AIMS*

Study 1 explored individuals' perceptions of the 2011 UK census. Several themes that seem to impact perceptions of the census questions and the census overall were identified. The goal of Study 2 is to investigate further, and in a quantitative way, the relationship between two of these themes: sensitivity and privacy protection behaviours. The aim was to understand whether discomfort with the census could have led participants to engage in privacy protection behaviours or delay the return of the census form.

Based on Study 1's findings and past research, the following hypotheses were generated:

- **H1**: The later participants submitted their census forms the more likely they engaged in privacy protection behaviours.
- **H2a**: More privacy concerned individuals submitted their census later.
- **H2b**: More privacy concerned individuals were less comfortable answering the census questions.

- **H2c**: More privacy concerned individuals (according to Westin's privacy segmentation index) are more likely to engage in privacy protection behaviours.
- **H3**: Individuals who are more uncomfortable disclosing census data items are more likely to engage in privacy protection behaviours.
- **H4**: Individuals who are more uncomfortable disclosing census data items submitted the census later.
- **H5**: Non-White individuals submitted the census later.
- **H6**: Non-White individuals are more likely to engage in privacy protection behaviours.

### *6.3.2 Method*

In April 2011, an online survey was set up with market research company e-Rewards. Being eligible to complete the census was a pre-requisite for participation. The survey took approximately 15 minutes to fill in. Respondents were rewarded by e-Rewards for their participation. 174 UK participants (100 female, 74 male) were recruited according to a nationally representative sampling frame. Their ages ranged from 18 to 79 years (mean=46 years, s=16.06). In terms of ethnicity, 160 were White (92%), five were Asian (2.9%), three were Black African/Caribbean (1.7%), two were Mixed (1.1%) and four gave no answer (2.3%). Compared to the 2011 census estimates for the UK, Whites are overrepresented (estimate = 87%) and other ethnicities underrepresented (Asian or Asian British estimate = 7%; Black or Black British estimate = 3%; and British Mixed estimate = 2%) in this sample.

The online survey was created using the open source software Limesurvey. The survey had several components. First, respondents' privacy concern was assessed using the 3-item Westin privacy segmentation index (Harris and Associates Inc. and Westin, 1998) which categorises individuals into three groups. Reliability was questionable (Cronbach's α=0.68), which is common for the Westin index.

Second, respondents were asked whether they had completed their census form yet and, if yes, on which day did they had submitted it. Third, respondents were presented with the full list of census items (household, individual, visitors) and asked to rate how comfortable they felt disclosing each item on a 5-level scale of comfort (1=Very Uncomfortable, 5=Very Comfortable). Reliability of this scale was excellent (α=0.98).

Finally, respondents were asked to rate to what extent they agreed or disagreed with four statements about privacy protection behaviours on a 7-level scale (1=Strongly Disagree, 7=Strongly Agree) - e.g. "To protect my privacy some questions I could have answered I did not answer at all." The four questions covered withholding data, providing incomplete data, providing incorrect data, or providing both incomplete and incorrect data. Reliability was excellent (α =0.90).

### 6.3.3 RESULTS

Three participants claimed they had not completed their census as of the date of this study. 35 participants (20.1%) answered they had completed the census on the day of the deadline: March 27, 2011. Completion dates for the census form ranged from 30 days before the deadline to 38 days after the deadline. On average, participants submitted their census seven days after the deadline.

According to the Westin Index, 40 (23%) participants were categorised as privacy fundamentalists, 90 (52%) as privacy pragmatists and 44 (25%) as privacy unconcerned.

Average comfort ratings with answering the census questions ranged from 4.43 to 3.54 (see Table 6.2), with gender being the item participants were most comfortable disclosing and another address where you stay for more than 30 days a year the least comfortable item.

| Item | N | mean | s |
|---|---|---|---|
| Gender | 173 | 4.43 | .80 |
| Country of birth | 173 | 4.38 | .89 |
| Language | 174 | 4.32 | .90 |
| Number of residents | 172 | 4.30 | .91 |
| Residents | 172 | 4.28 | .93 |
| Another address 1 | 141 | 3.81 | 1.20 |
| Visitors | 157 | 3.79 | 1.23 |
| Employer address | 164 | 3.70 | 1.33 |
| Landlord | 121 | 3.61 | 1.21 |
| Another address 2 | 100 | 3.54 | 1.28 |

**Table 6.2: Comfort ratings for census items (Sample)**

When asked how comfortable they felt disclosing data about other people in their household as compared to data about themselves 63.2% of participants said they felt "as comfortable", while 31% answered they felt "less comfortable." When asked specifically how they felt disclosing data about people who had visited their household, a higher percentage of participants answered "less comfortable": 48.3%, while 44.3% said they would feel the same level of comfort as if disclosing data about themselves.

Regarding participants' level of agreement with whether they had engaged in privacy protection behaviours or not, 8% agreed (slightly agreed, agreed, or strongly agreed) that they had withheld data when answering the census. 10.3% agreed that they had provided incomplete data. Fewer participants, 4% agreed that they provided incorrect data in the census. Only 2.3% agreed they had provided both incomplete and incorrect data.

### 6.3.3.1 Privacy Protection Behaviours and Census Return Date

The census return date variable was measured in days away from deadline: it was positive if the participant had been late in returning the census, negative if the participant had returned the census before the deadline, and zero if the census had been returned on the day of the deadline. There was a significant and positive correlation between participants' self-reported census return date and their level of agreement on having engaged or not in each of the privacy protection behaviours (see Table 6.3).

| Privacy Protection Behaviour | Spearman's ρ | p |
|---|---|---|
| Withholding data | 0.15 | <0.05 |
| Provided incomplete data | 0.13 | <0.05 |
| Provide incorrect data | 0.15 | <0.05 |
| Provide incomplete and incorrect data | 0.15 | <0.05 |

**Table 6.3: Relationship between census return data and privacy protection behaviour**

Therefore, the later participants completed their census form, the more likely they were to agree they engaged in privacy protection behaviours. H1 was thus supported. Levels of agreement with having engaged in privacy protection behaviours were also highly significantly ($p<0.01$) and positively correlated between themselves.

### 6.3.3.2 Effect of Privacy Concern

There was no significant effect of Westin privacy category on census return date. H2a was thus not supported. There was also no significant association between Westin's privacy category and average comfort ratings. H2b was also not supported. The level of agreement on whether they had engaged in privacy protection behaviours such as withholding data, disclosing incorrect data, or disclosing incomplete data, was not significantly affected by Westin's privacy category. H2c was thus not supported.

### 6.3.3.3 Comfort with Disclosure and Privacy Protection Behaviours

The average comfort of participants with item disclosure was significantly and negatively correlated with their level of agreement on whether they had engaged in privacy protection behaviours (see Table 6.4).

| Privacy Protection Behaviour | Spearman's ρ | p |
|---|---|---|
| Withholding data | 0.37 | <0.01 |
| Provided incomplete data | 0.37 | <0.01 |
| Provide incorrect data | 0.37 | <0.01 |
| Provide incomplete and incorrect data | 0.36 | <0.01 |

**Table 6.4: Relationship between average sensitivity and privacy protection behaviour**

Thus, participants with lower reported average comfort with disclosure of census items tended to agree more that they had engaged in privacy protection behaviours supporting H3.

#### 6.3.3.4 Comfort with Disclosure and Census Return Date

The average comfort of participants with item disclosure was not significantly correlated with census return date. However, participants' census return date was significantly and negatively correlated with their level of comfort with disclosing some of the data items (see Table 6.5).

| Data Item | Spearman's ρ | p |
|---|---|---|
| Type of central heating | -0.20 | <0.01 |
| Country of birth | -0.13 | <0.05 |
| Description of national identity | -0.13 | <0.05 |
| Ethnic group | -0.18 | <0.05 |
| Main language | -0.13 | <0.05 |
| Level of English | -0.15 | <0.05 |
| Religion | -0.14 | <0.05 |
| Passports held | -0.15 | <0.05 |
| Qualifications | -0.13 | <0.05 |
| Whether you have ever worked | -0.13 | <0.05 |
| How you travel to work | -0.15 | <0.05 |

**Table 6.5: Relationship between average sensitivity and census return date**

H4 was thus only partially supported.

#### 6.3.3.5 Effect of Ethnicity

When analysing the effect of participants' ethnic group on their answers non-White participants were grouped together to make up for their small numbers and because it was considered relevant to investigate whether ethnic minority participants' census perceptions differed from White participants, as was observed in the US (e.g.: Singer et al., 2003).

Average census return date did not significantly differ for Whites and non-Whites, not supporting H5; however, on average, non-Whites tended to agree significantly more than

Whites that they had engaged in privacy protection behaviours when answering the census supporting H6 (see Table 6.6).

| Privacy Protection Behaviour | Mann-Whitney U | p |
|---|---|---|
| Withholding data | 284.0 | <0.01 |
| Provided incomplete data | 400.5 | <0.01 |
| Provide incorrect data | 348.0 | <0.01 |
| Provide incomplete and incorrect data | 470.5 | <0.05 |

**Table 6.6: Effect of ethnicity on privacy protection behaviours**

Moreover, for 21 items non-Whites reported significantly lower levels of comfort with disclosure than Whites (see Table 6.7).

| Data Item | Mann-Whitney U | p |
|---|---|---|
| Number of residents | 424.5 | <0.01 |
| Residents' names | 396.0 | <0.01 |
| Number of rooms | 361.5 | <0.01 |
| Number of cars | 364.5 | <0.01 |
| Country of birth | 407.5 | <0.01 |

**Table 6.7: Effect of ethnicity on sensitivity (Sample)**

## 6.4 Discussion

Due to the privacy concerns about census data raised in the first study and evidence in past research it was predicted that the more people postponed the completion of the census the more likely they were to also omit or lie on their answers. This was supported by the survey study data. The later participants completed their census form the more likely they were to agree they engaged in privacy protection behaviours. This seems to indicate that more privacy conscious individuals will delay their disclosure of data given the choice. Delaying disclosure can therefore be seen as a privacy protection strategy as well. More importantly, it suggests that the later the census form is submitted the more likely it is to contain false data or omissions. To the author's knowledge, this is the first time this phenomenon is observed and it seems to warrant further investigation. For example, it would be interesting to determine whether data quality is high in the censuses returned before the deadline and decays steadily as more days pass. If this was confirmed to be the case then more resources could be allocated by the ONS to verify data submitted later.

It was expected that individuals who are more concerned about privacy, as measured by the Westin index, to submit their census later and be more likely to engage in privacy protection behaviours, but these hypotheses were not supported by the data. It was also hypothesised that more privacy concerned individuals would be less comfortable disclosing individual data items, but this was also not supported. Thus, the effect of privacy concern as measured according to the Westin index seems improbable.

However, if one looks at privacy concern as measured by the average comfort with item disclosure revealed in the survey study, then there is a significant effect on stated likelihood to engage in privacy protection behaviours. Sensitivity of data was also raised as an important issue by interviewees in the first study. This supports the assertion that privacy concerns can in fact negatively impact data quality and undermine the aims of the census program. In past research, sensitivity has not only been linked to privacy attitudes (see Section 2.1.1.1), but also to actual disclosure behaviour with more sensitive questions more likely to lead individuals to lie or omit answers. Thus, addressing the privacy concerns of citizens should be a priority if the ONS wants to maximise data quality. One possible solution for this would be to calculate the benefit obtained by each question asked in the census and compare it to the privacy cost inflicted on respondents. If an item is too sensitive and does not provide enough value, then it should be removed from the census. Another option is to make census forms shorter while complementing the data with other government sources. This is already done in countries like the Netherlands. As a side effect the census would require less effort and time from respondents.

The effort required to fill in the census was raised as an issue by participants in the interview study who tended to see the census as a nuisance, and not as a valuable effort that can benefit their community. Effort has been associated to disclosure behaviour before (see Section 2.1.1.6). Both from a privacy and usability perspective, the visitor questions in particular, seem to be seen as too invasive and requiring too much time and effort to answer. Survey findings indicate that a substantial proportion of individuals are less comfortable disclosing data about other people in their household (31%) or visitors (48%) than about themselves. Moreover, past research suggests individuals are not comfortable disclosing data about third-parties without their permission (Malheiros et al., 2012a). It is unclear how beneficial, from a statistical point of view, these questions were to the ONS, so it may be advisable to remove them in future census efforts.

In the survey study, ethnicity had a clear effect on privacy concern, with non-White participants being significantly more likely to admit to privacy protection behaviours and significantly less comfortable with disclosing 21 of the census items. This supports findings of studies conducted in the US (Singer et al, 2003) where black individuals were found to be more likely to not-respond to the census. It would be important to inquire further into this issue in the UK: why do ethnic minorities in the UK feel disaffected towards census efforts and what are their reasons?

Other themes were identified in the interview study as being linked to perceptions of the census. Perceived relevance has been linked to privacy attitudes before (Culnan, 1993); with questions seen as less relevant in the context there they are asked being perceived more negatively. This is also the case with the projected image theme. As observed in other contexts, data that portrays the individuals in a bad light is usually seen as more sensitive (Jennett et al., 2012; Malheiros et al, 2012a), especially when disclosed to people close to her or him (Adams & Sasse, 2001). The fact that this theme emerged in the context of the census demonstrates a potential risk for misrepresentation of respondents if they do not want the government to have a bad image of them. In fact, while census and item undercount have been looked into, research into census misrepresentation is, to the author's knowledge, inexistent and this would likely be a promising avenue of research in the future. The risk of misrepresentation may be increased if they perceive that data can be transferred to organisations other than government ones, which can impact the individual in different ways. In fact, concern with secondary data use - i.e. data collected for the census being passed to other organisations to be processed for different purposes - has been one of the main concerns identified in citizens with regards to the census (Singer et al., 1993; Couper et al., 1998). Figure 6.1 presents a model of disclosure behaviour for the census based on the factors identified in this chapter. Individual difference factors, such as ethnicity, are left out of the model because they are outside the scope of this thesis.

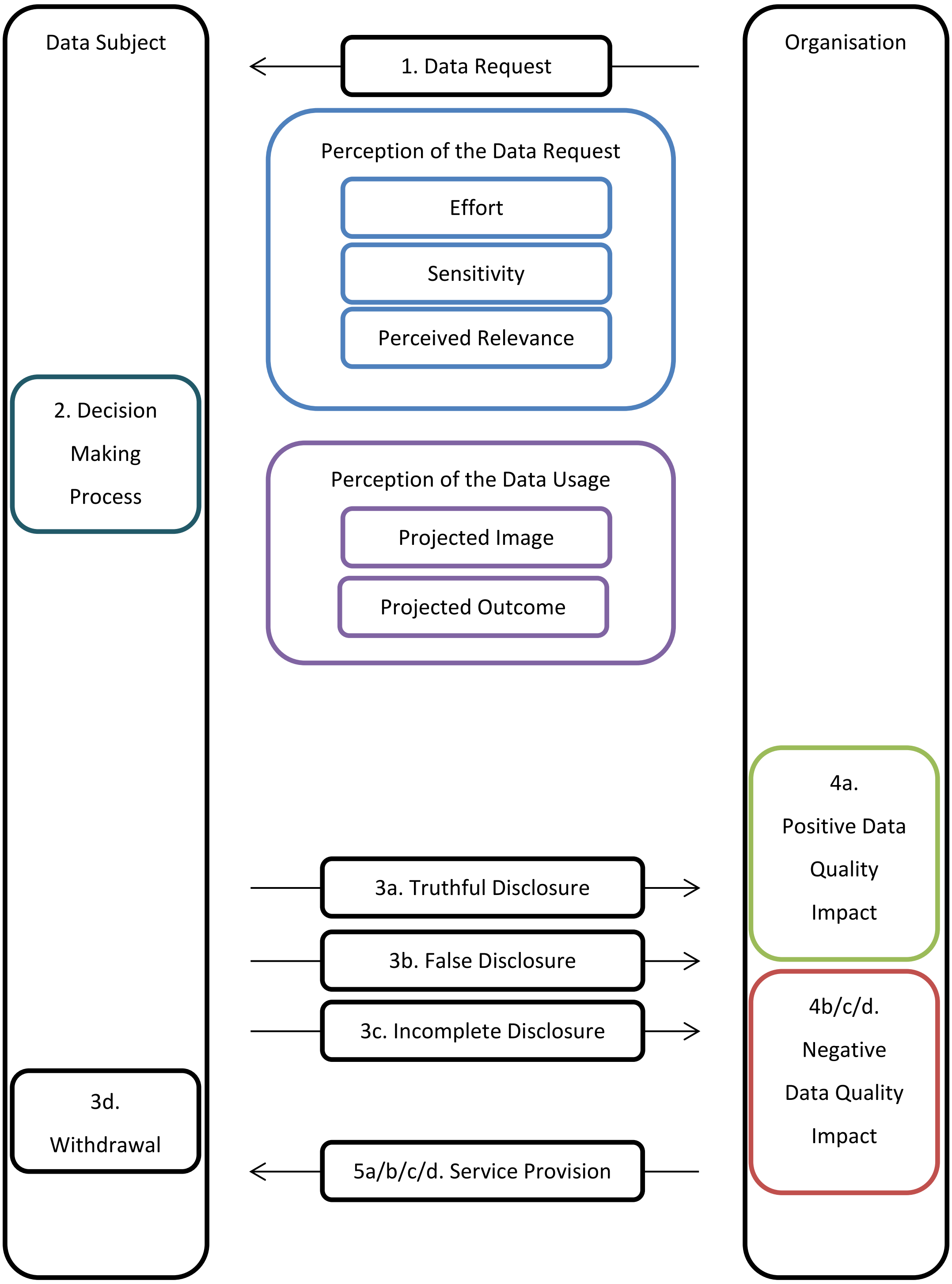

Data Subject
1. Data Request
Organisation
Perception of the Data Request
Effort
Sensitivity
Perceived Relevance
2. Decision Making Process
Perception of the Data Usage
Projected Image
Projected Outcome
4a. Positive Data Quality Impact
3a. Truthful Disclosure
3b. False Disclosure
3c. Incomplete Disclosure
4b/c/d. Negative Data Quality Impact
3d. Withdrawal
5a/b/c/d. Service Provision

**Figure 6.1: Census disclosure decision model**

While the research presented here sheds light on privacy attitudes towards the census it could benefit from a larger, and equally representative, sample. Furthermore, in addition to effort, other non-privacy issues that may influence disclosure behaviour should, ideally, have also been investigated.

The implications for practitioners are substantial. In particular, if the link between late submission of the census and decreased data quality is confirmed then any organisations that use census data must take this fact into consideration when analysing the data. The fact that some individuals - ethnic minorities in particular – are more sensitive to some of the data collection should also be addressed. Census authorities are advised to abstain from collecting data items that bring little value to the overall goals of the census and that are considered invasive and aim to collect low-sensitivity/high-benefit items instead.

These findings also open new avenues of inquiry to other researchers. Little research has been done into the determinants of census and item undercount in the UK or misrepresentation in censuses in general. More research should be carried out to determine why ethnic minorities seem to engage less with the census and how to tackle this issue. Also, from a usability point of view, there seems to be room for improvement since the interviews suggest that most people avoided using the online forms. Usability researchers could explore this topic further to determine the causes for this choice.

# Chapter 7: ADVERTISING STUDIES

## 7.1 BACKGROUND

Web users have become desensitised to display ads such as banners or pop-ups (Drèze & Hussherr, 2003; Hollis, 2005). To increase response rates of web users, advertisers have started using techniques such as targeted and personalised advertising. Targeted ads are ads that try to match the user's interest to become more appealing. Personalisation of ads refers to the practice of including personal data that identifies the user –e.g.: user's name - in the ad to make it more noticeable and attractive. Personalisation and targeting are sometimes used together.

There are two main types of targeted advertising: contextual advertising and behavioural advertising. In contextual advertising, the text of the webpage the user is visiting is analysed in real-time and an ad related to that content is picked to be displayed to the user. For example, if the user is visiting the webpage of an airline company he would get ads related to travel destinations. Behavioural advertising groups web users into different profiles based on their web activity (websites visited, search queries made, and topics viewed) and shows them ads related to that profile. For example, if a user regularly visits travel websites and searches for flight tickets and travel guides she could be profiled as "travel enthusiast" by ad networks. As a result, she would be shown more travel related ads.

There is evidence that behavioural ads can be much more effective than normal ads, with click-through rates 670% higher (Yan et al. 2009) and with 6.8% of ads resulting in sales versus the 2.8% for normal ads (Beales, 2010). Past research also indicates that users are more likely to enjoy ads that they perceive as being relevant and less likely to enjoy those they perceive as irrelevant (Kean & Dautlich, 2009). While these techniques can make ads more effective some users may perceive them as too privacy invasive (Turow et al., 2009). In 2012, Facebook introduced a type of ad called "sponsored stories" where pages "liked" by users could trigger the appearance of ads on their friends' feeds showing they had liked the page (Fiveash, 2012). However, there was a significant backlash from users who felt these ads were invasive and misleading and the social network website was forced to drop them (Delo, 2013).

Research looking at the overall perception that users have of targeted advertising have yielded mixed results. Table 7.1 (Malheiros et al, 2012b) summarises some of these results. Targeted advertising is considered by some individuals as too invasive (Kean & Dautlich, 2009; McDonald & Cranor, 2010) and has been associated with feelings of "creepiness" (Knowledge@Wharton, 2008). Other issues that raise privacy concerns are also mentioned in the literature, including: (1) the use of cookies in the user's browser (OFT, 2010); (2) unfair labelling of the user by advertisers (Turow et al., 2009); or the collection the users' personal data without their knowledge (Kean & Dautlich, 2009), among others.

| Researchers | Year | N | Population | Survey Method | Findings |
|---|---|---|---|---|---|
| Internet Advertising Bureau and Olswang | 2009 | 1,004 | UK | Online | 23% found the concept of BA appealing and 20% found it unappealing. When asked whether they would prefer BA as opposed to non-targeted ads, 27% opted for BA while 17% preferred non-targeted ads. |
| Turow et al. | 2009 | 1,000 | US | Phone | 66% did not want ads tailored to their interests, compared to 32% yes and 2% maybe. |
| McDonald and Cranor | 2009<br>2010 | 14<br>314 | US<br>US | In-depth interviews.<br>Online | Only 21% wanted the benefits of relevant advertising. 40% said that they would be more careful online if they knew that advertisers were collecting data; 15% said that they would stop using sites with BA. |
| Hastak & Culnan | 2010 | 2,064 | US | Online | 46% were uncomfortable with BA, 31% were neutral and 22% were comfortable. |
| Office of Fair Trading | 2010 | 1,320 | UK | Not Reported | 40% held neutral views about BA, 28% disliked it and 24% welcomed it. 57% said that the practice of BA would make no difference to their internet use, 5% that they would limit their internet use, and 1% that they would stop using the internet altogether. |
| TrustE | 2011 | 1,004 | US | Not Reported | 54% did not like BA and 37% had experienced a time when they had felt uncomfortable with a targeted online ad. |

**Table 7.1: Surveys on targeted advertising (Malheiros et al., 2012b)**

The rationale behind personalisation of ads is that users will find ads that use their personally identifiable information (PII) to be more associated to them (Anand & Shachar, 2009). The drawback is that they may experience *personalisation reactance*, a feeling of discomfort brought about by the perception that the ad company knows too much about them. According to White et al. (2008) personalisation reactance is influenced by: (1) the level of personalisation; (2) whether a justification for the personalisation is given; (3) perceived utility of the service being advertised. This suggests that, if users are shown ads for services that have high utility for them, then they will be less sensitive to personalisation. If the services advertised have low utility, then personalisation reactance will be more likely.

Research on perceptions of targeted and personalised advertising suggest a trade-off between a potential increase in effectiveness of ads and the possibility of raising privacy concerns or feelings of uneasiness. However, the majority of this research has been conducted through surveys and focused on attitudes making it difficult to understand how users actually react when they see these types of ads during their normal browsing of the web. If personalisation and targeting become the rule for online ads how will users react? Will it contribute to higher rates of user conversion and bigger revenue for the companies that use them, or will these ads be faced with negative reactions from user as in the Facebook "sponsored stories" case? To try and answer these questions a study investigating participants' responses to ads with varying degrees of personalisation, including ads that use the participant's name and photograph, was conducted.

This study was designed by the author and UCL MSc student Snehalee Patel. Data was collected by Snehalee Patel. Eye-tracking data was analysed by Dr. Charlene Jennett and thematic analysis of interview transcripts was done by the author. This background section is based on the background section of (Malheiros et al., 2012b) which was mostly written by Dr. Charlene Jennett.

## 7.2 Study 1

### *7.2.1 Aims*

This study aims to address limitations of past research on targeted and personalised advertising which has, for the most part, focused on surveys asking users to rate their level of agreement with several statements. This is a common limitation of privacy research in other contexts as well. To address this limitation, a study design where participants are observed and asked to think aloud while browsing a website that displays these types of ads is proposed. In a lab setting participants were asked to complete a holiday booking task using a travel website designed for the purposes of the study. As the participants went through the different pages and forms necessary to complete the task, they were exposed to: (1) contextual ads about holidays; (2) ads based on their holiday destination choice; (3) ads that used their name and photo. By contextualising their actions and perceptions in a realistic scenario, the expectation is that more reliable and valid results are obtained.

The study aimed to answer the following research questions:

1. Which ads did participants notice most / least?
2. Which ads did participants find the most / least comfortable?
3. Which ads were participants most / least likely to take an interest in?

### *7.2.2 Method*

The study was advertised as an experiment to investigate "perceptions of a travel website". A fictitious travel website called "Flyaway" was created. 30 participants (15 female and 15 male) were recruited from an opportunity sample. 22 were UCL students and 8 were UCL staff. The mean age was 28 years and ages ranged from 19 to 55 years (s=10.1). Participants were asked to complete a simulated holiday booking task on this website and to "think aloud" while they did it. The task took place in a lab setting and took approximately 30 minutes to complete.

The website consisted of three webpages and each page contained four banner adverts positioned at the top left, top right, bottom left, and bottom right. Ads had the same size (221 x 336 pixels) and used only text and pictures. Page 1 contained a form where participants could select journey related options, such as travel destination and departure and return dates. Additionally, the form contained requests for data items like relationship status, car ownership status, age, among others. The page informed participants that depending on the answer they might "qualify for our exclusive offers". The ads shown on this page were contextual ads related to holidays and travel destinations (see top-left ad in Figure 7.1 for an example). On the second page of the website participants were asked to select how many tickets they wanted and provide their name, address, and payment method. The ads on this page were targeted using the data items disclosed by the participant in the previous page, such as travel destination and whether they were single or owned a car (see top-right ad in Figure 7.1). The third page confirmed participant's booking. Ads on this page were picked based on participants' age bracket (e.g. clubbing ads for younger participants vs. life insurance for older participants) and addressed them by first name (see bottom left ad in Figure 7.1). One of the ads used the participant's photo (unaltered and also modified) to advertise a cosmetic product. The photo was collected from UCL staff and student database before the study and modified using Photoshop. Modifications included changing the hair-style and colour or aging the participant's face in the picture by 40 years (see bottom right ad in Figure 7.1).

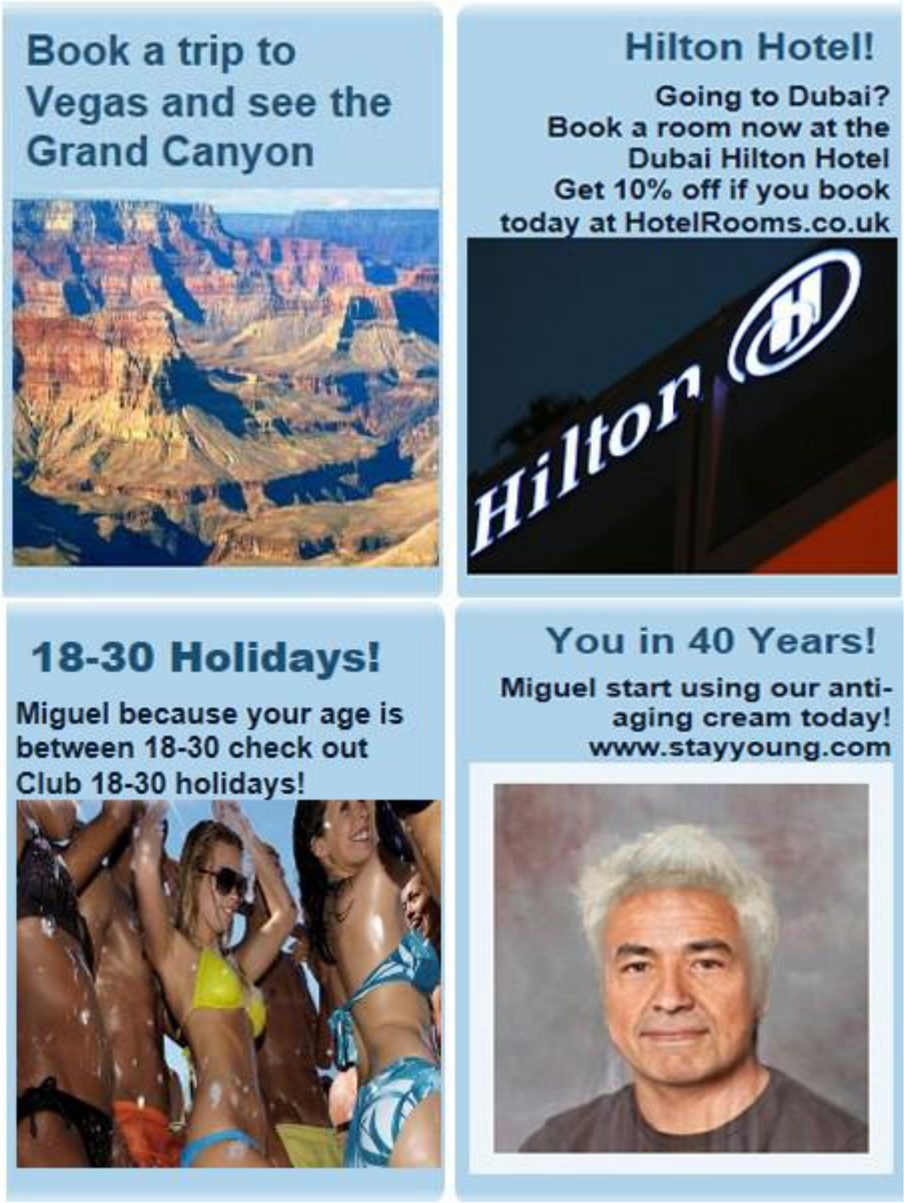

Book a trip to Vegas and see the Grand Canyon
Hilton Hotel!
Going to Dubai? Book a room now at the Dubai Hilton Hotel Get 10% off if you book today at HotelRooms.co.uk
Hilton
18-30 Holidays!
Miguel because your age is between 18-30 check out Club 18-30 holidays!
You in 40 Years!
Miguel start using our anti-aging cream today! www.stayyoung.com

**Figure 7.1: Examples of "Flyaway" Ads (Malheiros et al., 2012b)**

While they carried out the task participants’ eye movements were captured using a Tobii X50 eye-tracker. Total fixation duration (TFD) measurements were collected to assess how noticeable ads on the different pages were, with longer TFD corresponding to more noticeable ads.

When they had completed the holiday booking task participants were given a questionnaire. The questionnaire asked participants to rate, on a 5-level Likert-scale, how much they agreed with 13 statements. The first statement asked whether participants had noticed the ads on the website. The remaining questions asked participants how much they had (1) noticed; (2) found comfortable; and (3) found likely to elicit interest ads that used their:

- holiday destination;
- age;
- name;
- photo.

An interview followed, exploring their perceptions of targeted and personalised advertising in the context of the experiment they had taken part in. This interview was audio recorded.

The study was approved after going through UCL's ethical review process, and permission was granted to collect participants' university photos from a publicly accessible page and use them in the study. All participants signed a consent form that described the experimental procedure and the equipment used, explained that data collected would be held in accordance with data protection law, and that they could withdraw from the study at any point without penalty. Participants were not told about the study's true aim nor that their photo would be used. After the study they were debriefed and told that their photos and data they had disclosed in the website forms could be destroyed if they wished. Participants were paid £5 for their participation.

### *7.2.3 Results*

#### 7.2.3.1 Finding 1: Personalised ads are more noticeable

The ads on the third page of the website received twice as much attention as the ads on the first and second pages (see Table 7.2). The mean TFDs of each page were compared in a repeated measures one-way ANOVA which confirmed the differences were significant, F(2,48)=10.16, p<0.001. Bonferroni-corrected pairwise comparisons (sig. level = .016) showed that the TFD of page 3 was significantly longer than page 1 (p=0.009) and page (p<0.001).

| Page | Total Fixation Duration (s) | |
|---|---|---|
| | Mean | SD |
| 1 | 4.6 | 3.8 |
| 2 | 4.7 | 5.4 |
| 3 | 9.5 | 6.3 |

**Table 7.2: Total Fixation Duration Per Page (n=25[8]) (Malheiros et al, 2012b)**

### 7.2.3.2 Finding 2: Ad with photo more noticeable than ad with age

To isolate the effect of the ad that used the participant's photo on page 3, it was compared against another ad in the same page that used the participant's age and a standard picture. On average, participants looked at the ad with the participant's photo for 13.0 seconds and at the other ad for 7.2. The difference was significant[9], t(24) = 3.2, p=.003.

### 7.2.3.3 Finding 3: Type of data used in ad affects self-reported noticeability, interest, and comfort

Questionnaire responses indicated that the type of personal data used to create an ad has a significant effect on noticeability, perceived interest, and comfort.

97% of participants agreed that they would be more likely to notice ads that used their photo (see Table 7.3). Majorities of participants also considered that ads that used their holiday destination (77%) and name (57%) would be more noticeable. Only 27% of participants thought the same for ads that used their age. The differences between the average noticeability ratings were significant, F (3, 87) = 16.0, p<.001. Bonferonni-corrected pairwise comparisons (sig. level =.008) showed that ads that used a participant's photo were considered significantly more noticeable than ads that used their holiday destination (p=.005), age (p<.001), or name (p<.001), providing additional support to the finding in Section 7.2.3.2. Holiday destination was rated significantly more noticeable than age (p<.001).

[8] Five participants were excluded from this analysis due to the poor quality of their eye-tracking data

[9] Data from an additional participant had to be excluded for this test due to poor quality.

| **I am more likely to notice adverts that use my…** | **+ ve** | **0** | **- ve** |
|---|---|---|---|
| Holiday destination (Q2) | 23<br>(77%) | 5<br>(17%) | 2<br>(7%) |
| Age (Q5) | 7<br>(27%) | 13<br>(43%) | 9<br>(30%) |
| Name (Q8) | 17<br>(57%) | 6<br>(20%) | 7<br>(23%) |
| Photo (Q11) | 29<br>(97%) | 0<br>(0%) | 1<br>(3%) |

**Table 7.3: Self-Reported Noticeability of Ads. +ve = Strongly Agree or Agree, 0 = Neutral, - ve = Disagree or Strongly Disagree (n=30) (Malheiros et al., 2012b)**

Majorities of participants disagreed they would feel comfortable with ads that used their photo (80%) or name (66%) (see Table 7.4). 87% agreed they would feel comfortable with ads that used their holiday destination. The differences between the average comfort ratings were significant[10], F (1, 30) = 26.7, p<.001. Bonferonni-corrected pairwise comparisons (sig. level = .008) showed that ads that used holiday destination were rated significantly more comfortable than ads that used age (p<.001), name p<.001) and photo (p<.001). Also, ads that used participants' age were rated as significantly more comfortable than ads that used their photo (p=.001).

| **I feel comfortable with adverts that use my…** | **+ ve** | **0** | **- ve** |
|---|---|---|---|
| Holiday destination (Q3) | 26<br>(87%) | 3<br>(10%) | 1<br>(3%) |
| Age (Q6) | 7<br>(23%) | 13<br>(43%) | 10<br>(33%) |
| Name (Q9) | 7<br>(23%) | 4<br>(13%) | 19<br>(66%) |
| Photo (Q12) | 3<br>(10%) | 3<br>(10%) | 24<br>(80%) |

**Table 7.4: Self reported Comfort with ads. +ve = Strongly Agree or Agree, 0 = Neutral, - ve = Disagree or Strongly Disagree (n=30) (Malheiros et al., 2012b)**

Most participants (77%) agreed they would be more likely to be interested in ads that used their holiday destination (see Table 7.5). Majorities of participants disagreed they would be more likely to take interest in ads using their photo (67%) and name (57%). The differences

[10] Significance levels were adjusted according to the lower-bound procedure to compensate for violations of the sphericity assumption (Mauchley's W(df=5) = .65, p=.037).

between the average likelihood to take an interest ratings were significant[11], F (1, 30) = 13.7, p<.001. Bonferonni-corrected pairwise comparisons (sig. level = .008) showed that ads that used holiday destination were rated significantly more likely to elicit interest than ads that used age (p<.001), name (p<.001) and photo (p<.001).

| **I'm more likely to take an interest in adverts that use my…** | **+ ve** | **0** | **- ve** |
|---|---|---|---|
| Holiday destination (Q4) | 23 (77%) | 6 (20%) | 1 (3%) |
| Age (Q7) | 7 (30%) | 16 (53%) | 5 (17%) |
| Name (Q10) | 5 (17%) | 8 (27%) | 17 (57%) |
| Photo (Q13) | 10 (23%) | 0 (0%) | 20 (67%) |

**Table 7.5: Self reported Interest in ads. +ve = Strongly Agree or Agree, 0 = Neutral, - ve = Disagree or Strongly Disagree (n=30) (Malheiros et al., 2012b)**

### 7.2.3.4 Theme 1: Understanding data flow / Transparency

Thematic analysis of the interview identified several themes linked to how participants perceived in the ads in the study, and, more generally, how they perceive targeted and personalised advertising in their daily lives. Of relevance to this thesis is the issue of transparency. Not understanding at which point certain data items were collected or how they may potentially be used may lead to violations of the individuals' expectations that can be perceived as privacy violations. This was mentioned by a majority of participants in the interviews.

Not understanding the flow of their personal data and how advertisers may have obtained is a source of concern for participants and was mentioned by 18 of them in the interviews. Cross-site advertising in particular was disconcerting, because it is not clear how one site knows something you have shared in another site.

> "I don't understand how they know what you've been looking at on another website." P10

[11] Significance levels were adjusted according to the lower-bound procedure to compensate for violations of the sphericity assumption (Mauchley's W(df=5) = .47, p=.001).

Understanding the data flow seemed to make participants more comfortable.

> "Yeah, I would prefer targeted adverts as long as I knew how they got the fact that they're targeted. As long as, yeah, I was aware of, it was just you know that I could see that I looked at it before and they were just advertising something, and that was it, then I'd be more comfortable and happy with that […]" P18

For example, in this study, when it was made clear to the participant that the photo used in the website was obtained from a university website, it contributed to making its use more acceptable.

> "The fact that I know that it is a university, that it is my university picture and that I am at university, then it doesn't make me uncomfortable [...]". P5

Not knowing the source of the data and how it was obtained caused discomfort.

> "I think that's weird, because I'm like 'Where did they get that picture?'" P14

A related concern was *consent*, which was mentioned by 5 participants. The use of one's personal data in ads without permission was perceived negatively.

> "I don't think I would want my image being used for something without my knowledge, I mean if they like approached people and asked to use it then that would be different but I wouldn't want it used without my knowledge." P4

#### 7.2.3.5 Theme 2: Projected Image

One concern mentioned by 9 participants was that ads using their data and targeted at them could be seen by other people due to errors in the targeting or because they shared computers with them. For example, if two people had a similar name, an ad using the photo of them could be displayed to the other.

> "Well they have to be rather accurate to know which … I mean there may be … are so many, many names, have the same name so they may get the wrong picture from a person with the same name." P19

Individuals sharing the same machine could lead to one seeing ads based on the behaviour of the others. If there was data perceived as sensitive used in the targeting and that was obvious from the ad there could be a privacy violation.

> "The computer or the website will have the memory of my searching. The next time my friend or somebody else uses my computer they can see what I bought. If I just, I only buy the cream or moisturizer, those kind of things, that's okay. But if it's very private I don't want them to be able to see that." P11

### *7.2.4 Discussion*

Results indicate that depending the personal data used in creating a targeted has a significant impact on how noticeable an ad is. While this may suggest to advertisers to go for the ads that create the strongest impact, the questionnaire results suggest some careful thought should be put into the tailoring of the ad. Type of personal data used in the ad can also influence how interesting it is perceived to be and how comfortable individuals are with them. Ads that are more noticeable are not necessarily considered more interesting and may cause discomfort if individuals perceive they are supported by an abusive use of their personal data. Thus, advertisers should avoid using personal data to increase an ad's noticeability at the expense of user's comfort. Advertisers should aim for sweet-spot personalisation of ads that makes ads more noticeable and interesting using data items that users are comfortable with, such as holiday destination in this study.

Contrary to the other studies presented in this thesis, this study focuses on perceptions of data use as opposed to perceptions of explicit data requests or data collection. Understanding user decision-making at the point of disclosure is important to determine how different perceptions of the data collection process can lead to different reactions of the user, some of them which can be counter-productive for the organisation collecting the data. However, it is also relevant to understand how individuals perceive uses of data that may not have been collected explicitly through a form. Results in this study suggests that if users do not understand the data pipeline that led to a specific outcome, in this case the display of a targeted ad, they experience feelings of privacy invasion. It is likely these experiences will affect how these individuals will assess an explicit data request the next time they are asked to disclose data. In particular, it seems likely it will affect how individuals judge the *projected outcome* factor. If, in the past, their data was passed on to advertisers for the purpose of creating targeted ads, then the next time they see themselves in a similar situation they will take that into account in their decision. This has been observed in past research (Adams, 2001): if an individual has experienced privacy invasions before, they will have an inflated level of privacy concern the next time they assess a situation with regard to privacy which may lead to rejection of the technology or service they are assessing.

# Chapter 8: A CONTEXT-NEUTRAL MODEL FOR INDIVIDUAL DISCLOSURE BEHAVIOUR

The studies conducted as part of this thesis have a common goal: understanding how individuals perceive different organisational data practices, and how those perceptions affect their willingness to disclose personal data, or accept its collection by organisational information systems. While the research presented here focused on different contexts of interactions and types of organisations, many of the same themes were identified across studies - suggesting that the decision-making process of disclosure of personal data relies on the same factors, regardless of context. Moreover, a subset of these same factors had been identified as relevant for privacy perceptions in past research in fields such as marketing or e-commerce.

The model presented here (see Figure 8.1) proposes that individuals, when faced with a request for their personal data from an organisation, assess the request according to a series of factors and, depending on this assessment, decide to comply or not with the request. Compliance leads to truthful disclosure of personal data while non-compliance leads to omission and falsification of personal data, or withdrawal from the interaction.

The model does not attempt to be an exhaustive list of all factors that are considered by individuals when making a disclosure decision. Other factors may be part of the process, and the existing ones may be combined or categorised differently. The remainder of this chapter briefly describes each factor of the model (see Table 8.1).

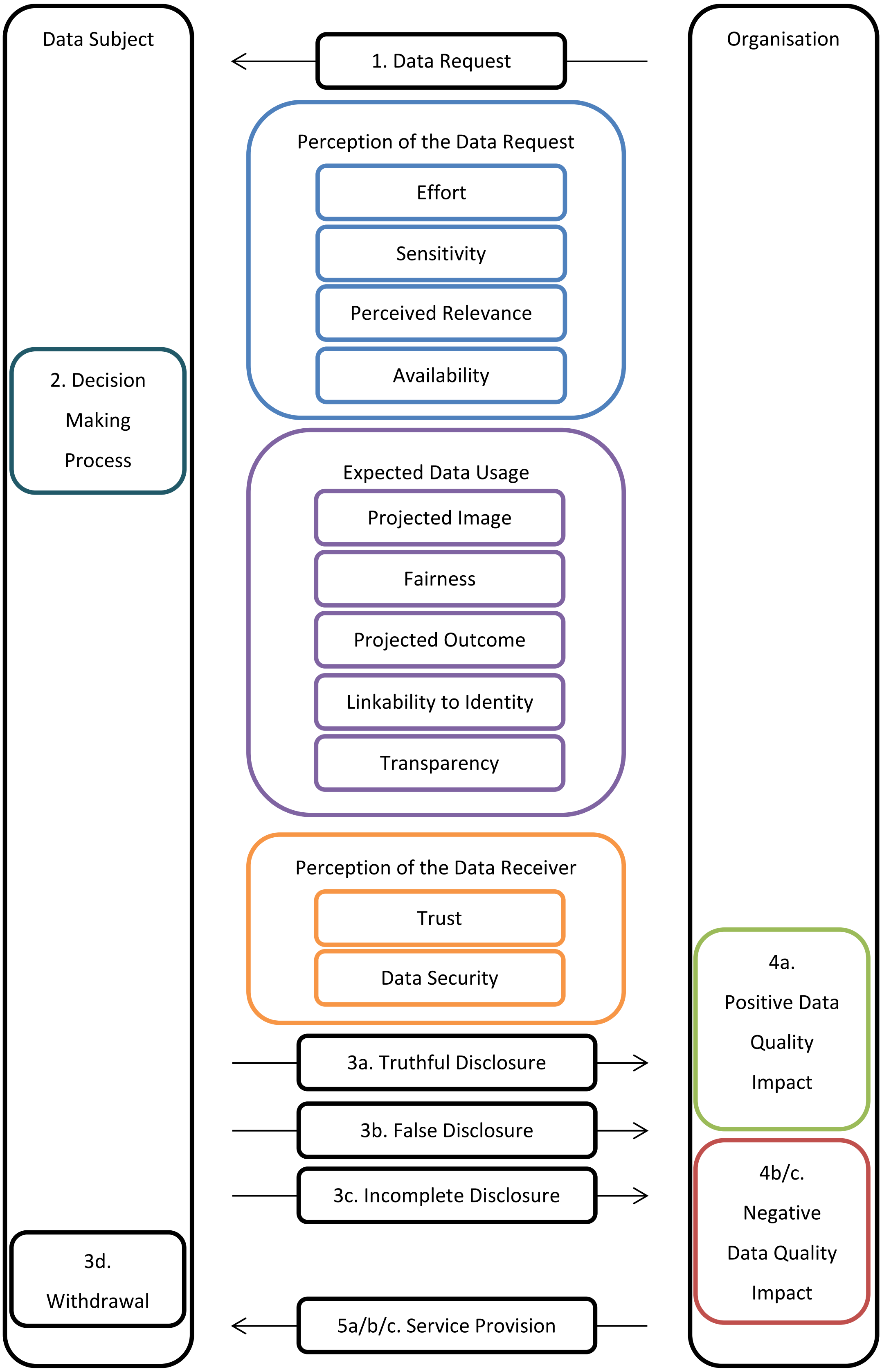


**Figure 8.1: A context-neutral model for individual disclosure behaviour**

| Model Factors | Thesis Section(s) | Meaning |
|---|---|---|
| **Perception of the Data Request** | | |
| Perceived Relevance | 4.3.3.4; 4.4.3.4; 4.6.3.1.1; 4.7.3.5.1; 6.2.3.1 | Is the question relevant? |
| Sensitivity | 4.4.3.1; 4.5.3.1; 4.7.3.5.4; 6.3.3.3; 6.2.3.4 | Am I comfortable answering? |
| Effort | 4.3.3.7; 4.6.3.1.2; 4.7.3.5.6; 6.2.3.3 | How much work is it answering? |
| Availability | 4.7.3.5.7 | Have I given this data before? |
| **Expected Data Usage** | | |
| Projected Image | 4.3.3.2; 4.4.3.2; 4.5.3.2; 4.6.3.1.3; 4.7.3.5.3; 5.2.3.1; 5.3.3.1; 5.4.3.2; 7.2.3.5; 6.2.3.6 | How will this make me look? |
| Projected Outcome | 4.3.3.2; 4.4.3.3; 4.4.3.2; 4.5.3.2; 4.6.3.1.4; 4.7.3.5.3; 5.2.3.1; 5.3.3.1; 5.4.3.6; 6.2.3.2 | What will happen if I answer? |
| Fairness | 4.7.3.5.2; 5.3.3.2; 5.4.3.3 | Will my data be used fairly? |
| Linkability to Identity | 5.3.3.3; 5.4.3.4 | Can I be identified from this? |
| Transparency | 7.2.3.4 | Where will my data go? |
| **Perception of Data Receiver** | | |
| Trust | 5.4.3.5.3 | Do I trust this organisation? |
| Security | 5.4.3.1 | How secure will my data be? |

**Table 8.1: Thesis support for model factors**

## 8.1 Perception of Data Request

Factors in this section are related to the immediate perception of the data request. They are more connected to the assessment of the question itself than with the medium and long-term consequences of disclosure.

### *8.1.1 Perceived Relevance*

Perceived relevance refers to the perception that the data item being requested is related to the current context and the communicated purpose of data collection. It also means that the data item is perceived as being necessary for the interaction to be completed successfully - i.e. individuals understand why it is being asked. Higher perceived relevance correspond to a more positive perception of the data request and willingness to disclose.

This factor was identified in Chapters 4 and 6. In the context of loan applications its significance is that applicants need to understand how the data item being requested is connected to creditworthiness. For example, financial details would generally be seen as relevant to determine likelihood of not repaying debts, but brand of car owned would not. In the context of the census relevant items are the ones with a clear link to the communicated goals of the census: planning health, education, and transport public services. As a result, questions about visitors, for example, which do not have an immediate connection to these goals, were perceived as less relevant.

The implication for organisations collecting data is that they should make clear to individuals why they need to collect each data item and how it is going to be used.

### 8.1.2 Sensitivity

Sensitivity refers to how personal the item is perceived to be and how comfortable the individual feels disclosing it. Sensitivity seems to be used as an umbrella term that may be decomposed into other factors, but in this model it is interpreted as the "baseline discomfort" with disclosure. The higher the sensitivity of a request, the more negative the perception and the lower the willingness to disclose.

Sensitivity emerged in studies in Chapters 4 and 6. In the context of loan applications, items that are commonly requested in forms, such as name or gender, were considered less sensitive than items related to personal finances or phone numbers. Within items that could realistically be used in future risk assessment processes but that are not currently used, history of bill payments were the least sensitive while indices of social capital, such as social network friends were the most sensitive. In the context of the census, items related to visitors were considered less comfortable to disclose than items about the individual filling in the form.

Sensitivity of a data item was linked to response rate of that item. The implication for organisations collecting data is that the higher the sensitivity of the items they attempt to collect the lower the quality of the data that they obtain. More targeted data collection efforts can actually end up providing higher value than widespread hoarding of personal data.

### 8.1.3 Effort

In this thesis, effort is associated with number of data requests, how difficult they are to answer, the level of detail required, and whether they require the individual to look for information or just "slot in" answers. The bigger the perceived effort involved in answering a data request the lower the willingness to answer it.

Effort emerged as a relevant factor in Chapters 4 and 6. In the context of loan applications, effort was associated with long forms with difficult questions. In the context of the census, visitor related questions were considered more troublesome because they required respondents to remember who was at their house on a specific day and possibly get in touch with that person to ask for their details.

Whenever possibly, organisations should minimise the number of data requests they make, keep these requests simple, and provide easy channels for individuals to respond.

### *8.1.4 Availability*

Availability refers to whether the individual believes s/he has disclosed this data item before or the data item is publicly available already. If the item is considered to be available the willingness to disclose will be higher as the associated privacy cost was already paid.

In Chapter 4, the fact that data was already publicly available anyway was mentioned as a justification for answering a data request that was considered unacceptable. Still, organisations should avoid collecting data items that may be perceived as unacceptable just because they have been already disclosed before. They should also avoid requesting the same item more than once, as this will increase the effort for individuals (see Section 8.1.3 on Effort). If the data item can be obtained without requesting it from the individual, it should still be made clear to him or her that the organisation has access to it (see Section 8.2.5 on Transparency).

## 8.2 Expected Data Usage

These factors are associated to how the individual expects the data disclosed to be used and generally refer to medium and long-term consequences of disclosure.

### *8.2.1 Projected Image*

This factor refers to how the individual expects the disclosure will make her/him look in front of others. Individuals want to disclose personal data that show them in a favourable light and avoid disclosures that make them look unfavourably.

This factor emerged in Chapters 4, 5, 6, and 7. When applying for a loan, individuals want to make disclosures that will make them look capable of repaying a debt while at the same time hiding details that may reveal they would have difficulty doing it. A similar phenomenon was identified in the serious-games studies, where individuals are concerned that performance data make them look incompetent. Respondents of the census also seemed wary that details about occupation or education could make them look bad. Finally, in the context of personalised advertising it was mentioned that individuals could infer private details about other people if they got a chance to see ads personalised for them.

Organisations should consider whether individuals will feel humiliated or that their reputation will be harmed as a result of answering a data request. If this is the case an alternative data item that fulfils the same purpose and that has not the same effect on the individual should be collected instead.

### 8.2.2 Projected Outcome

When individuals make a disclosure they assess the potential consequences, positive and negative, that may result from it. Disclosures that help them further their goals are seen positively. If a negative outcome is expected from answering a data request, individuals will be less willing to comply with it.

This factor was mentioned in Chapters 4, 5, and 6. In the context of loan applications the goal of applicants is to obtain the loan and, therefore, disclosure that bring them closer to that goal are perceived more positively. With regards to serious-games deployed in corporate environment, the main concern of players is not to suffer humiliation by peers or encounter careers obstacles as a result of playing the game. For census respondents, there is a risk that data collected for the census can actually be used for nefarious purposes such as social sorting.

As in Section 8.1.1, the implication for organisations collecting personal data is that they should not only clearly communicate the purpose for which they are collecting the data, but stick to that purpose. Moreover, all potential harmful consequences that can occur as a result of individuals answering should be explained.

### 8.2.3 Fairness

Fairness is an ethical consideration related to the perception that the data being collected will be used to draw reliable inferences about the individual and processed for the purposes communicated by the data receiver. Fair uses of data are associated with a more positive perception of the data practice and higher willingness to disclose.

In Chapter 4 fairness was mention in the context of lenders using certain types of data to discriminate applicants. Some data requests were considered unfair to use for the purpose of risk assessment, such as health related ones. In Chapter 5 the same factor emerged in relation to the automatic of assessment of the competence of serious-games players based on their performance in the game. Using a game to evaluate real-life skills was considered unfair.

The implication for organisations using items of personal data to make inferences about individuals is that they should be careful that those inferences are perceived as valid and ethically acceptable by those individuals. Individuals should not feel they are being disadvantaged by allowing their data to be processed in such a way.

### *8.2.4 Linkability to Identity*

This factor refers to how easy it is to identify the individual from the data item provided and whether the disclosures are made in a context where the individual can be identified. Disclosures less connected to the real identity of the individual are perceived more positively as the individual is less accountable.

This factor was mentioned in Chapter 6. When playing a serious-game deployed by their employer individuals feel they would be more relaxed playing if the data collected by the system was not associated to their real-life identity. One reason for this is that players could suffer negative consequences in the real world as a result of their performance in the game (see Section 8.2.2). The implication of this finding is that individuals are more willing to disclose data if that data is not connected to their identity. As a result, organisations should avoid identifying data subjects, unless that is absolutely required for the purposes of the data collection.

### *8.2.5 Transparency*

A transparent data flow implies that the individual disclosing the data knows when and what data is being collected and how it will be used. Not understanding how a data receiver obtained an item of personal data or with whom data being disclosed will be shared is disconcerting for individuals.

Transparency was mentioned in Chapter 7 in relation to the lack of transparency of targeted and personalised ads and cross-site advertising. It is fundamental that individuals clearly understand when their data is collected, who it is shared with, and how it can be used in the future. In particular, if the data is collected for the creation of profiles and to enable personalisation services it should made clear to individuals when they are offered those services how they were targeted at them.

## 8.3 Perception of Data Receiver

These factors are related to how the organisation requesting personal data is perceived and how they will keep the data collected.

### *8.3.1 Relationship & Trust*

The relationship individuals have with the data receiver and, in particular, how much they trust them, have an impact on how data requests are perceived. When individuals disclose personal data to a data receiver they are putting themselves in a vulnerable position. Trust refers to the expectation that the data receiver will not take advantage of this vulnerability. When data requests come from trusted organisations individuals have a more positive attitude towards the collection of personal data.

Relationship with and trust in the data receiver emerged as important concerns in Chapter 5. Individuals may not want to disclose personal data to individuals or organisations who have power over them (see section 8.2.2) and whom they do not trust. The implication for organisations is that they should attempt to collect personal data in the context of an existing and transparent relationship (see Section 8.2.5). Relationship building requires mutual selective disclosure and if organisations remain opaque while they ask individuals to surrender personal details then they will not be considered trustworthy.

### *8.3.2 Security*

This factor refers to how and where collected data is stored by data receivers and which security measures are in place to protect it. Individuals who are more confident in the security measures of the data receiver will be willing to comply with data requests.

This factor emerged in Chapter 5 with regard to the possibility of players' game related data being stored insecurely or being stored in an unknown overseas location. The implication is that individuals want to be reassured that their data will be secure and that its storage will not be outsourced to other countries.

This mode is partially validated in Chapter 9 and its overall implications are discussed in Chapter 10.

# Chapter 9: Validation

The model for individual disclosure behaviour proposed is founded on the findings from the studies presented in this thesis. While focused on understanding how individuals perceive the requests for their personal data and how those perceptions influence their disclosure behaviour, these studies employed different methods and were carried out in different contexts. The triangulation of both research method and research context supports the validity of the model, as several of the factors emerged repeatedly in different studies – e.g. *relevance.* Moreover, some of the factors had been identified in the literature before as having an impact on privacy perceptions and/or disclosure behaviour.

While triangulation lends validity to the model, it needs to be determined whether the factors presented actually impact individual disclosure behaviour and, consequently, the data quality if the organisation requesting or collecting the personal data. A final study was designed determine the impact of a subset of the model factors (perceived *fairness, relevance, sensitivity,* and *effort* of a data request) on actual disclosure decision. Not all factors were included in the study due to methodological, time, and budget limitations. Inquiring about all the factors would make the study too long for participants and, consequently, would require a large reward. The approach used to validate these factors can be replicated in future work to validate the rest of the model or even augmented versions of the model that include extra factors.

This study was conducted in collaboration with Dr. Sören Preibusch from Microsoft Research Cambridge. The study attempted to both validate part of the disclosure model presented in this thesis and answer some of Dr. Preibusch's research questions. Each researcher designed the part of the study that addressed his research goal. Only the author's part is reported here. Data was collected by Dr. Preibusch and analysed by the author. The complete study was published as (Malheiros et al., 2013).

## 9.1 Aims

This study aims to determine the effect of four different factors related to how individuals perceive data requests on (1) their decision to answer the request, and (2) the truthfulness of their answers. The four factors chosen are part of the individual disclosure behaviour model presented in this thesis and consist of perceived (1) fairness; (2) relevance; (3) effort; (4) sensitivity of a data request. All four have been shown in this thesis to be linked to privacy perceptions in different contexts and the studies' findings suggest they affect how likely individuals are to comply with data requests and whether they may engage in privacy protection behaviours. This study investigates whether these factors are also linked to actual disclosure behaviour and not only attitudes. This is an important contribution in privacy research since the literature is heavily skewed towards conclusions drawn from attitudinal data. Moreover, it has been shown that privacy attitudes can differ sharply from privacy behaviour.

### *9.1.1 Experimental Hypotheses*

Based on the findings of the studies presented in this thesis and the literature it is hypothesised that:

- **H1a**: Perceived effort of a request for a data item has a negative effect on decision to disclose that item.
- **H1b**: Perceived fairness of a request for a data item has a positive effect on decision to disclose that item.
- **H1c**: Perceived relevance of a request for a data item has a positive effect on decision to disclose that item.
- **H1d**: Perceived sensitivity of a request for a data item has a negative effect on decision to disclose that item.
- **H2a**: Perceived effort of a request for a data item has a negative effect on the truthfulness of the corresponding answer.
- **H2b**: Perceived fairness of a request for a data item has a positive effect on the truthfulness of the corresponding answer.
- **H2c**: Perceived relevance of a request for a data item has a positive effect on the truthfulness of the corresponding answer.
- **H2d**: Perceived sensitivity of a request for a data item has a negative effect on the truthfulness of the corresponding answer.

## 9.2 Method

### *9.2.1 Phase 1 of Experiment: Platixx Web Form*

The first phase of the experiment consisted of an online questionnaire for a fictitious credit card provider called Platixx. Participants were told that Platixx was a real company that planned to launch a new credit card: the Platixx Card. As part of their marketing studies, Platixx wanted participants to fill in a one page online survey. The survey page featured a professionally designed layout with a consistent colour scheme, website URL and company logo (see Figure 9.1).

While the study was advertised as a survey it is indeed a first phase of an experiment and not a questionnaire. The goal in this phase was to observe whether participants answered each question or not. This differs from most privacy research, which relies on self-reported measures of willingness to disclose personal data and not on observation of actual disclosure of personal data.

The study comprised 9 different treatments in a 3 x 4 triangular design varying on: total number of questions (5, 10, or 15) and the number of those which were mandatory (0, 5, 10, 15). All treatments also contained two mandatory check questions to determine whether participants were engaged with the exercise and were reading the questions properly. In the remaining of this chapter treatments are designated using the following notation: qXmY where X is the total number of questions and Y the number of those that are mandatory.

In treatments with mandatory questions these were always in the beginning of the form followed by any optional questions. Question order was constant. There was no graphical annotation, such as asterisks, to denote mandatory questions. Simply, the text at the top of the form explained which questions were mandatory – e.g. for treatment q10m10 the text said "Please provide some information about yourself. Questions 1 to 12 are mandatory. There is no bonus for this HIT." There was no input validation at any point in the form, even if a mandatory item had been left blank. All questions were open answer, i.e. no multiple choice questions.

There were different types of questions. Some were related to banking and personal finance, e.g. income, debt situation, spending, number of credit cards; others to demographic details, e.g. age, gender, marital status, health, education; and a final subset were questions that could be construed as uncommon and which served to avoid a flooring effect of sensitivity, e.g.: number of relatives who died during the childhood or the duration of the longest relationship. These uncommon items had been used in Study 3 of Chapter 4: (Section 4.5), as well.

2720 US participants were recruited using Amazon's crowdsourcing platform, Mechanical Turk (mTurk) in the beginning of 2013. Their reward depended on the treatment they were assigned to: 20 US cents for treatments q5; 40 US cents for treatments q10; and 60 US cents for treatments q15. Every participant was paid independently of having answered all mandatory questions or answering the check questions correctly. The samples for each treatment are independent as repeat participation was prevented.

### 9.2.2 *Phase 2 of Experiment: UCL Branded Questionnaire*

After submitting the Platixx web form participants were invited for a follow-up questionnaire. This questionnaire focused on their perceptions of the Platixx questions they had just been asked. To avoid socially desirability bias, the follow-up questionnaire was branded as a UCL research study and assured participants that their answers would not be shared with Platixx. Only participants who had completed the first phase could participate and reminders were sent if two days had passed since the participant had received the invitation. 79% of all who had participated in the first phase also submitted the follow-up questionnaire.

For each question in the Platixx web form, participants were asked to use a 4-level agreement scale (-2 = strongly disagree, -1 = disagree, +1 = agree, +2 = strongly agree) to rate the following statements:

- The question was hard;
- The question was fair;
- The question was relevant

Perceived sensitivity ratings were collected for a subset of 8 items. Participants were asked to use a 4-level scale to rate each of these 8 questions. Higher ratings corresponded to higher sensitivity: 1 = very happy to disclose, 2 = happy to disclose, 3 = unhappy to disclose, 4 = very unhappy to disclose. Reliability was good or high for these measures: Cronbach's α = 0.91 for effort, α = 0.88 for fairness, α = 0.84 for relevance, and α = 0.84 for sensitivity[12])

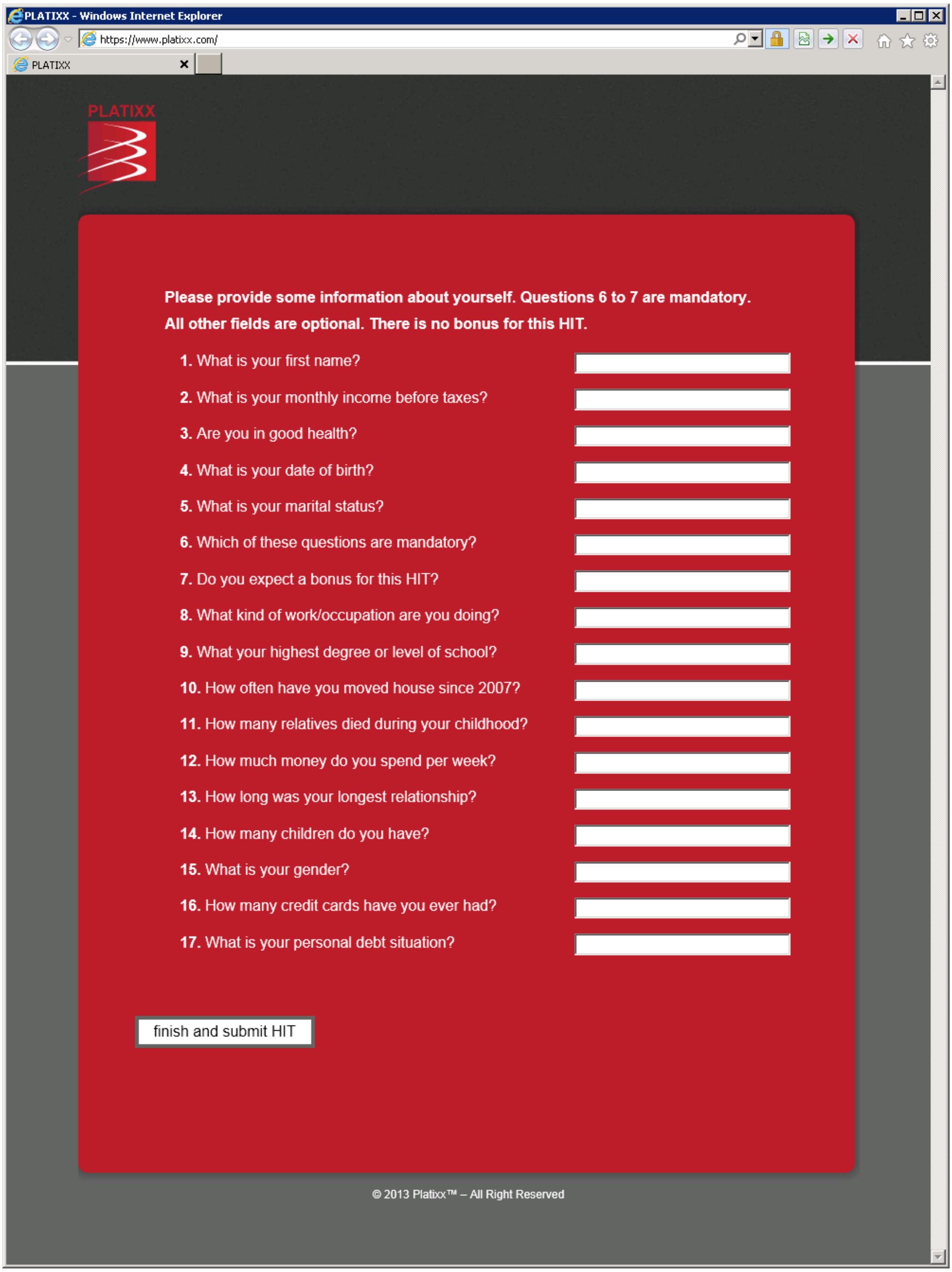
### 9.2.3 *Ethics Approval*

The study was approved for deployment after going through UCL Department of Computer Science’s ethics review process.

### 9.2.4 *Coding*

All answers were coded into three categories: answered, did not answer, and refused to answer. Refusals can either be explanations of why the participant doesn’t want to answer, such as “A lady doesn't reveal her age” or simply nonsensical text. Only data from participants who answered the two check questions correctly was considered in the analysis.

[12] Reliability for sensitivity took into account ratings for 36 different items, of which only 8 are discussed in this thesis.



**Please provide some information about yourself. Questions 6 to 7 are mandatory. All other fields are optional. There is no bonus for this HIT.**

**1.** What is your first name?

**2.** What is your monthly income before taxes?

**3.** Are you in good health?

**4.** What is your date of birth?

**5.** What is your marital status?

**6.** Which of these questions are mandatory?

**7.** Do you expect a bonus for this HIT?

**8.** What kind of work/occupation are you doing?

**9.** What your highest degree or level of school?

**10.** How often have you moved house since 2007?

**11.** How many relatives died during your childhood?

**12.** How much money do you spend per week?

**13.** How long was your longest relationship?

**14.** How many children do you have?

**15.** What is your gender?

**16.** How many credit cards have you ever had?

**17.** What is your personal debt situation?

© 2013 Platixx™ – All Right Reserved

**Figure 9.1: Platixx webform, treatment q15m0**

## 9.3 Results

Out of the 2360 valid participants who completed the first phase of the study, 1851 also completed the second phase. Sample sizes for each treatment are detailed in Table 9.1. Refusals to answer and omissions were grouped together as non-disclosure. Thus, for each question a participant was considered to either have answered or not answered. Some demographic data was collected in the follow-up questionnaire. Mean age was 30 years old and ranged from 17 to 80. 41% of participants were women, 59% men, and less than 1% refused to reveal their gender.

Table 9.1 shows that, in treatments with mandatory questions, disclosure rates are much higher and approach 100%. This suggests that saying that a question is mandatory has a strong effect on disclosure. While the differences between mandatory and optional data requests are important for disclosure research, they are outside the scope of this thesis. For this reason, when analysing the effect of different factors on disclosure, the focus is on treatment q15m0 (i.e. the treatment with 15 questions in total where all are optional), since it provides the broadest range of questions to analyse while avoiding the potentially overriding effect of mandatory questions. When analysing the effect of different factors on truthfulness all q15 treatments are used, as it is not expected that truthfulness is affected in the same way as disclosure by making questions mandatory. Data from all nine treatments is used when reporting descriptive statistics for perceived fairness, relevance, effort, and sensitivity.

| treatment | $N$ | $N_{\text{valid}}$ | first name | monthly income | good health | date of birth | marital status | occupation | education | times moved | childhood deaths | weekly spending | relationship max length | children count | gender | credit-card count | debt situation |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| q5m0 | 300 | 258 | 61.6 | 57.8 | 74.0 | 58.1 | 72.5 | | | | | | | | | | |
| q5m5 | 300 | 271 | **99.3** | **99.3** | **100.0** | **99.6** | **99.6** | | | | | | | | | | |
| q10m0 | 300 | 262 | 69.5 | 60.3 | 77.1 | 59.9 | 76.7 | 70.2 | 71.0 | 69.1 | 61.8 | 53.1 | | | | | |
| q10m5 | 300 | 254 | **99.2** | **98.8** | **100.0** | **100.0** | **100.0** | 64.6 | 66.5 | 62.6 | 57.9 | 53.5 | | | | | |
| q10m10 | 300 | 257 | **99.2** | **98.1** | **100.0** | **98.4** | **99.6** | **98.8** | **99.6** | **98.8** | **98.1** | **96.9** | | | | | |
| q15m0 | 320 | 279 | 64.5 | 64.9 | 75.3 | 57.0 | 74.2 | 67.0 | 71.0 | 67.0 | 60.2 | 54.5 | 61.3 | 67.4 | 72.4 | 65.9 | 56.6 |
| q15m5 | 300 | 253 | **99.2** | **98.0** | **99.2** | **98.8** | **99.2** | 69.2 | 70.4 | 67.2 | 62.1 | 51.4 | 61.3 | 66.0 | 67.6 | 63.2 | 53.4 |
| q15m10 | 300 | 258 | **98.4** | **99.2** | **100.0** | **100.0** | **100.0** | **100.0** | **100.0** | **100.0** | **99.6** | **95.0** | 71.3 | 77.5 | 78.3 | 76.7 | 66.7 |
| q15m15 | 300 | 268 | **97.0** | **98.5** | **100.0** | **99.6** | **100.0** | **99.3** | **99.6** | **99.3** | **99.6** | **95.1** | **93.3** | **99.3** | **98.9** | **97.8** | **95.9** |
| feedback | | | | | | | | | | | | | | | | | |
| *Effort* | | mean | −1.47 | −0.81 | −1.29 | −1.27 | −1.50 | −1.43 | −1.49 | −1.19 | −0.70 | −0.56 | −1.13 | −1.56 | −1.65 | −1.19 | −0.96 |
| | | $s$ | 0.99 | 1.29 | 1.06 | 1.18 | 0.91 | 0.97 | 0.93 | 1.17 | 1.46 | 1.43 | 1.26 | 0.90 | 0.82 | 1.23 | 1.37 |
| *Fairness* | | mean | 1.37 | 1.15 | 0.29 | 1.14 | 1.00 | 1.22 | 0.86 | 0.57 | −0.98 | 0.51 | −0.81 | 0.39 | 0.91 | 1.04 | 0.92 |
| | | $s$ | 0.93 | 1.02 | 1.44 | 1.09 | 1.16 | 0.99 | 1.23 | 1.34 | 1.31 | 1.35 | 1.42 | 1.43 | 1.35 | 1.19 | 1.28 |
| *Relevance* | | mean | 0.92 | 1.35 | −0.52 | 1.09 | 0.64 | 1.08 | 0.39 | −0.01 | −1.58 | 0.58 | −1.42 | 0.05 | 0.44 | 1.11 | 1.16 |
| | | $s$ | 1.35 | 0.92 | 1.42 | 1.14 | 1.35 | 1.13 | 1.41 | 1.44 | 0.94 | 1.39 | 1.08 | 1.50 | 1.55 | 1.20 | 1.18 |
| *Sensitivity* | | mean | 2.12 | 2.62 | 2.70 | 2.52 | 1.84 | 1.98 | 1.77 | | | | | | 1.63 | | |
| | | $s$ | 0.89 | 0.86 | 0.97 | 0.94 | 0.74 | 0.78 | 0.70 | | | | | | 0.66 | | |

**Table 9.1: Disclosure statistics per treatment and follow-up questionnaire ratings**

### 9.3.1 Perceived Effort, Fairness, Relevance, and Sensitivity of Data Requests

The bottom half of Table 9.1 shows the average ratings for each of the factors for each question across all treatments.

Average ratings for effort are negative for every question suggesting they were perceived by participants as easy to answer. The questions perceived as requiring the least amount of effort to answer were gender, children count, and marital status. Intuitively, the answers to these questions can be given immediately by most people: they do not require substantial calculations or recall effort. While still easy, weekly spending, childhood deaths, and monthly income were considered the most difficult to answer. Contrary to the previous group of questions, these three require participants to recall past events or make some calculations, possibly explaining why they were considered harder to answer.

Fairness ratings offer a broader range of answers, with some questions being considered unfair and others fair to ask. In particular, participants perceived childhood deaths, longest relationship, and health as the most unfair questions. Health related questions have been identified in the literature as a special case and individuals usually feel less comfortable answering this type of questions. Childhood deaths and longest relationship are uncommon questions in forms and it is unlikely that participants had seen them before. This may have contributed to them being perceived as unfair questions and it may have seemed difficult for participants to understand how they could be used by the data received in a fair way. Moreover, the most unfair items were also the ones considered the most irrelevant. It may have been difficult for participants to construct meaningful reasons for a credit card company to ask about childhood, relationships, or health for the purposes of a market study. First name, occupation, and monthly income were considered the fairest questions. First name and occupation are common questions in surveys and in some data collection efforts, income is also asked. It is possible participants were used to being asked these questions and saw them as fair. Furthermore, monthly income was also considered a very relevant question which may have contributed to it being seen as fair. Two other items perceived as relevant were debt situation and number of credit cards which are also financially related data items and thus consistent with the communicated purpose of the data collection.

Sensitivity ratings were only collected for eight of the 15 questions asked. Sensitivity has already been linked to both privacy perceptions and disclosure behaviour and so had lower interest for this study. Out of these, health (measured as *illnesses*) and income (measured as *annual income*) were considered the most sensitive items. This is consistent with the literature which states that medical and financial data are considered sensitive by individuals. The questions perceived as the least sensitive were gender and education. Both are common demographic questions and it is likely that participants were used to answering them and saw them as not sensitive.

### 9.3.2 Effect of Fairness, Relevance, Sensitivity, and Effort on Disclosure

The top half of Table 9.2 lists the binary logistic regression models for disclosure per item obtained by regressing effort, fairness, relevance, and sensitivity (where applicable) ratings on decision to disclose. These models explain between 7 and 20% of variability of the disclosure decision depending on the item. Nagelkerke's $R^2$ was used to assess model fit.

Perceived fairness has a significant effect on disclosure in 11 of the 15 models. Moreover, the coefficients are always positive, i.e. higher perceived fairness corresponds to larger odds of disclosure. The size of the fairness coefficients is also substantial in most items. For example, for the occupation data item, assuming all other factors remain constant, a unit change in perceived fairness – e.g.: from -2 to -1 – will make disclosure twice as likely (Exp(0.728) = 2.07). This supports hypothesis H1b. Fairness is an under-researched factor in privacy research and has never been linked to privacy decision making, but here it emerges as a promising predictor of disclosure behaviour as suggested in before in this thesis.

Sensitivity is significant for 3 of the 8 models it is part of, partially supporting H1d. The coefficients for these three items, first name, date of birth, and occupation are positive as expected and have a substantial size. For example, for date of birth, assuming all other factors remain constant, a unit change in perceived sensitivity – e.g.: from 1 to 2 – will make disclosure twice as likely (Exp(0.723) = 2.06).

Relevance also has a significant effect on the disclosure of 3 data items: first name, occupation, and times moved. However, unexpectedly, the coefficients are negative, indicating that higher perceived relevance leads to lower odds of disclosure. For example, for occupation, assuming all other factors remain constant, a unit change in perceived relevance – e.g.: from 1 to 2 – will make disclosure 0.6 times as likely (Exp(-0.448) = 0.64). H1c is rejected.

This result is difficult to articulate with previous qualitative results described in this thesis as well as established past research. One possibility is that relevance and fairness may be correlated resulting in multicollinearity. The model can then put most of the effect in one of the factors and the opposite signal in the other.

Effort was only significant for three data items: marital status, education, gender; but with negative coefficients contrary to what was expected. One possibility is that participants who did not answer a question rated it as having low effort because they did not answer it, while participants who went through the work of answering perceive a higher level of effort. H1a is rejected.

### *9.3.3 Effect of Fairness, Relevance, Sensitivity, and Effort on Truthfulness*

The lower half of Table 9.2 lists the linear regression models for disclosure truthfulness per item obtained by regressing effort, fairness, relevance, and sensitivity (where applicable) ratings on self-reported truthfulness ratings. The models explain between 10% and 26% of the variability of truthfulness.

As in the disclosure models, fairness is the best predictor here with a highly significant effect in the same 11 models. This supports H2b and the idea that perceived fairness is a strong predictor of personal data disclosure decision as well as likelihood of engaging in privacy protection behaviours such as lying. For example, for times moved, assuming all other factors remain constant, a unit change in perceived fairness – e.g.: from 1 to 2 – corresponds to a 0.58 units positive change in self-reported truthfulness (measured from -2, strongly disagree that my answer was truthful to +2 strongly agree that my answer was truthful).

Sensitivity is a significant predictor of truthfulness in 6 of the 8 items it applies to. The sensitivity coefficients are always negative indicating that higher perceived sensitivity of a data request contribute towards less truthful disclosure. This has also been observed in past research (Metzger, 2007). For example, for date of birth, assuming all other factors remain constant, a unit change in perceived sensitivity – e.g.: from 1 to 2 – corresponds to a 0.61 unit negative change in self-reported truthfulness. H2d is supported.

Perceived effort is only a significant predictor in two models: childhood deaths and weekly spending. The direction of its effect is negative, as expected. A unit change in effort, assuming all other factor remain constant, in the childhood deaths model, corresponds to a 0.15 decrease in truthfulness. H2a is only partially supported.

Relevance is only significant in four models and, unexpectedly, in two of them its coefficient is negative. H2c is not supported by the data. Again, possible multicollinearity between relevance and fairness may be the cause for this result and should be investigated further.

| Item | $R^2$ | Effort | Fairness | Relevance | Sensitivity | Constant |
|---|---|---|---|---|---|---|
| | | | item disclosure | | | |
| first name | 0.174 | 0.056 | $0.624^{**}$ | $-0.342^{*}$ | $-0.655^{***}$ | 1.407 |
| monthly income | 0.085 | 0.051 | 0.063 | 0.398 | −0.193 | 0.517 |
| good health | 0.069 | 0.188 | 0.217 | −0.132 | −0.331 | 1.736 |
| date of birth | 0.206 | −0.049 | $0.586^{*}$ | −0.304 | $-0.723^{***}$ | 1.896 |
| marital status | 0.101 | $0.330^{*}$ | $0.388^{*}$ | −0.032 | −0.103 | 0.510 |
| occupation | 0.149 | 0.129 | $0.728^{***}$ | $-0.448^{*}$ | $-0.597^{***}$ | 1.326 |
| education | 0.125 | $0.296^{*}$ | $0.484^{**}$ | −0.173 | −0.359 | 0.789 |
| times moved | 0.099 | 0.022 | $0.565^{***}$ | $-0.296^{*}$ | n/a | 0.317 |
| childhood deaths | 0.153 | −0.178 | $0.685^{***}$ | −0.312 | n/a | 0.750 |
| weekly spending | 0.108 | −0.154 | $0.381^{*}$ | 0.012 | n/a | 0.101 |
| relationship max length | 0.135 | −0.067 | $0.588^{***}$ | −0.060 | n/a | 1.090 |
| children count | 0.089 | 0.175 | $0.400^{*}$ | −0.071 | n/a | 0.403 |
| gender | 0.121 | $0.344^{*}$ | $0.497^{**}$ | −0.297 | −0.329 | 0.720 |
| credit-card count | 0.089 | 0.027 | 0.423 | 0.006 | n/a | 0.163 |
| debt situation | 0.063 | −0.047 | 0.375 | −0.028 | n/a | −0.008 |
| | | | item truthfulness | | | |
| first name | 0.096 | 0.005 | $0.384^{**}$ | $-0.189^{*}$ | $-0.355^{***}$ | 1.416 |
| monthly income | 0.097 | −0.082 | −0.082 | $0.475^{***}$ | −0.181 | 0.921 |
| good health | 0.096 | 0.013 | 0.098 | 0.124 | $-0.244^{**}$ | 1.817 |
| date of birth | 0.259 | −0.032 | $0.431^{***}$ | −0.048 | $-0.613^{***}$ | 1.910 |
| marital status | 0.153 | 0.118 | $0.361^{***}$ | 0.003 | −0.229 | 1.096 |
| occupation | 0.209 | −0.034 | $0.442^{***}$ | 0.077 | $-0.285^{**}$ | 1.192 |
| education | 0.149 | 0.020 | $0.339^{***}$ | −0.010 | $-0.301^{**}$ | 1.469 |
| times moved | 0.188 | 0.028 | $0.580^{***}$ | $-0.183^{*}$ | n/a | 0.636 |
| childhood deaths | 0.137 | $-0.146^{*}$ | $0.487^{***}$ | −0.188 | n/a | 1.030 |
| weekly spending | 0.140 | $-0.141^{*}$ | $0.285^{*}$ | 0.120 | n/a | 0.472 |
| relationship max length | 0.154 | −0.057 | $0.500^{***}$ | −0.065 | n/a | 1.215 |
| children count | 0.118 | 0.032 | $0.413^{***}$ | −0.074 | n/a | 0.885 |
| gender | 0.139 | 0.095 | $0.307^{***}$ | −0.013 | $-0.267^{*}$ | 1.335 |
| credit card count | 0.147 | −0.050 | 0.312 | 0.192 | n/a | 0.457 |
| debt situation | 0.105 | −0.032 | 0.066 | $0.368^{*}$ | n/a | 0.309 |

**Table 9.2: Item Disclosure and truthfulness regressed on perceived effort, fairness, relevance, and sensitivity. *=significant at p=0.05; **=significant at p=0.01; and ***=significant at p=0.005.**

## 9.4 Discussion

This study aimed to validate the effect of four different factors related to individuals' perception of data requests on their decision to comply with the request and decision to answer the request truthfully.

The results clearly support the hypothesis that the *perceived fairness* of a data request clearly impact the odds of individuals' answering the data request as well as the truthfulness of the answer. Thus, individuals who perceive the requests as unfair are less likely to answer them. Perceptions of unfairness will also lead to higher levels of falsification of answers. These findings validate the fairness construct in the disclosure model presented in this thesis not only as a factor of perceptions data requests but also disclosure behaviour decision-making.

Organisations that collect personal data, either explicitly or implicitly, should take into account how data practices perceived as unfair will lead to lower compliance by the data subjects and deteriorating data quality. Lower data quality can then undermine the ability of these organisations to make correct decisions and leverage the data to achieve their goals. Moreover, there may be reputational costs associated with the data practices. These, however, are not considered in this thesis.

The *perceived sensitivity* of a data request was also shown to impact both decision to disclose and the truthfulness of the disclosure albeit with lower support. It should also be noted that the effect of *perceive fairness* on disclosure behaviour holds regardless of the *perceived sensitivity* of the data item.

Surprisingly, little support was found for the effect of *perceived effort* and *relevance* on disclosure behaviour. The effort measure may have suffered from a flooring effect since all the items were rated, on average, as requiring low *effort* to answer. In any case, past research has identified a link between *effort* and disclosure behaviour (see Section 2.1.1.6). *Perceived relevance* was mentioned in several studies in this thesis as being linked to privacy perceptions and to how acceptable data requests are deemed to be by individuals. The data in this thesis suggests that higher *relevance* leads to a more positive perception of a data requests and, it was expected, to a higher level of compliance with it. Past research also suggests this (see Section 2.1.1.2). However, that effect was not verified in this study and actually higher *relevance*, in the models generated, was contributing to lower odds of disclosure and sometimes to lower levels of truthfulness. One potential explanation is multicollinearity between *relevance* and *fairness*.

A potential limitation of this validation study was the sample used. mTurk users come from various socio-economic background, but may be primed to disclosure and have less qualms about providing their personal data online. In any case, the results can be interpreted as an upper bound for disclosure behaviour.

Several factors in the model proposed in this thesis were not included in this study and, for some of them, it remains to be seen whether they are linked to actual disclosure behaviour and not just perceptions. While outside the scope of this thesis, future research can use a similar method to the one described in this study to verify the effect of new privacy factors on behaviour. Contexts other than financial services should also be investigated since different incentive structures may lead to different disclosure outcomes – e.g.: social-networking or e-commerce.

# Chapter 10: CONCLUSIONS

Privacy research in computer science had mostly been carried out in the disciplines of HCI and information security. HCI has focused on understanding how privacy perceptions are formed and how to design privacy sensitive systems, while researchers in information security have focused on developing techniques that help users to protect their privacy, such as access control, encryption, or anonymisation algorithms. This thesis takes the perspective that when faced with organisational efforts for massive collection of personal data it is difficult for individual users to manage the release of their personal data, and instead makes the argument that organisations should consider the negative reactions of individuals when assessing the value of collecting their personal data. This thesis aims to model how individuals perceive requests for their personal data or data collection efforts from organisations and in which circumstances these perceptions lead them to engage in privacy protections behaviours that harm the quality of the data provided. By linking perceptions of data collection to potential data quality impact this thesis makes the argument that minimising the invasiveness of organisational data practices can actually contribute to improving the quality of data they obtain from individuals while also reducing the privacy cost for those individuals.

Past research on disclosure behaviour has focused on a limited set of contexts, such as e-commerce. This thesis tackles this limitation by focusing on under-researched domains where personal data still plays a crucial part, such as loan applications, and by triangulating the results from these different domains. This allowed the thesis research to shed light on both privacy perceptions in these contexts of interaction, and to generalise some of the findings into a context-neutral model for disclosure behaviour. Another limitation in previous research addressed here is the overreliance on self-reported data, which has made it difficult to link perceptions of data practices to actual disclosure, omission and falsification rates. This thesis also makes use of self-reports extensively, but validates the identified themes with laboratory and field experiments. This triangulation of methods ads validity to the findings presented here.

This thesis investigated perceptions of organisational data practices in several domains. First, it investigated how individuals perceive requests for their personal data when applying for loans. While the lending industry is a big consumer of personal data - and relies on this data to control their exposure to the risk that borrowers do not pay back their loans – research on how individuals perceive their data practices has been scarce. This thesis then focuses on perceptions of serious-games and their collection and use of player data in the context of a corporate skills development programme. While previous research had been conducted on privacy perceptions of e-learning, it was overly data-centric and did not fully explore the tension between the use of a system aimed at learning, which requires risk-taking, while inserted in an environment that wants to assess individuals to make management decisions. Third, the thesis looked at how data requests in the UK Census of 2011 were perceived by citizens. Census efforts have been criticised for privacy reasons since they come to existence and substantial research on perceptions of the census has been conducted in the United States. However, little research has focused on the UK Census. Since the Census is the base for significant decisions made by the government with real impact in citizens lives, it was considered worthwhile to see how difference perception factors could lead to non-response on falsification of answers. The fourth domain investigated in this thesis, and the one where the collection of personal data and its use is less transparent to individuals, was targeted and personalised advertising. To avoid self-reported data, like most past research on the topic, and increase the validity of the findings, an experimental setup was used to investigate the perceived acceptability of personalised ads that used different types of personal data. Finally, an online field experiment was conducted to confirm whether a sub-set of the factors previously identified in the thesis had real impact on actual disclosure behaviour.

Section 10.1 discusses the theoretical, methodological, and empirical contributions of this thesis. Section 10.2 provides a roadmap for future research.

## 10.1 Contributions

### *10.1.1 Theoretical Contribution*

#### 10.1.1.1 A context-neutral model for individual disclosure behaviour

This thesis proposes a general model for individual disclosure behaviour that identifies a set of factors that influence how individuals perceive data requests from organisations, and how those perceptions can affect their response to the requests. This thesis posits that regardless of the context of interaction, data subjects will consider this subset of factors when assessing data requests. Based on that assessment individuals can comply with the request and answer truthfully, refuse to disclose data, or provide false data to the organisation.

This model is based on findings from all the studies conducted in this thesis. These studies focused on four very different domains and types of individual-organisation relationships, yet the identified factors emerged repeatedly throughout the thesis. The triangulation of methods, contexts, and findings supports the validity to the model. Moreover, some of the factors have been identified in past research on privacy perceptions, albeit mostly in the fields of e-commerce and marketing, which are not addressed in this thesis. This model breaks new ground by linking a subset of the factors to actual disclosure behaviour, and quantifying how changes in perception of these factors lead to a specific impact on data quality.

Practitioners that collect personal data can use this model to adjust their data practices to maximise data quality. In an initial phase, they can assess how individuals will perceive their data collection efforts according to each of the factors in a qualitative fashion and identify data requests that have a higher risk of non-compliance than the expected value for the organisation. In a second stage, short studies with a representative sample of individuals they are collecting data from can be carried out to quantify the perception of the data requests according to the model factors. These ratings could be used to estimate the likelihood of non-response and falsification of answer based on the research in this thesis. Practitioners could then make the necessary changes to the data collection process to minimise the occurrences of these privacy protection behaviours.

For fellow researchers this model provides a platform to generalise findings on privacy behaviour across contexts. Research on privacy perceptions and behaviour has usually focused on a subset of contexts. Because it is accepted that privacy perceptions and sensitivity of data varies a lot depending on the context in which the data practice occurs, attempts to generalise findings are rare. While this thesis agrees that privacy perceptions are context-depend, it argues that the process through which individuals perceive and respond to data collection efforts is not. It posits that a data request will always be assessed according to this model's core set of factors, even if the assessment itself will change depending on the situation. The model can also be used in the creation of privacy concern measures that have an actual link to behaviour. The model is not intended to be final and future research should focus on enriching it (see Section 10.2).

### *10.1.2 Methodological Contribution*

#### 10.1.2.1 Estimating likelihood of privacy protection behaviours

In both Study 5 of Chapter 4 (Section 4.7) and Chapter 9 experimental designs involving deception were employed where participants were confronted with actual requests for their personal data. This approach both addresses limitations of past privacy research and provides a first step to linking individual perceptions of data collection to data quality impact. With the exception of some recent research on privacy calculus, most privacy research has been based on participant self-reports and collected only measures of willingness to disclose personal data. Because privacy attitudes differ from behaviour (see Section 2.1.2), it is especially important to validate the link between perceptions and actual disclosure decision. By conducting experiments researchers can observe which items participants disclose and compare their disclosure decision with their perception of the question. While these perception measures are still self-reported and subject to post-hoc rationalisation, this approach is an improvement on methods that only capture attitudes towards disclosure. To further increase the realism of participants' disclosure behaviour compared to a laboratory experiment, in Chapter 9 a field experiment was conducted where participants were not told that they were part of a study.

By regressing measures of the model factors on answer and falsification rates, and validating the link between some of these factors and disclosure behaviour, this thesis provides a first step towards linking individuals' perceptions of data collection to data quality impact. This method can be used by practitioners to estimate how the quality of the data they collect can vary depending on the items they request from individuals. They can then decide whether the benefits outweigh the risks. This method can be repeated for specific organisational contexts and extended with additional factors.

### *10.1.3 Empirical Contributions*

#### 10.1.3.1 Research findings on loan applicants' perceptions of personal data collection and use by lenders

The studies in Chapter 4 identified that, in the context of loan applications, individuals want to make disclosures of personal data that make them appear creditworthy and, consequently make it more likely they are approved for a loan. Studies 2 and 3 (Sections 4.4 and 4.5) found that individuals were more comfortable disclosing items that they considered would increase their chances of obtaining a loan and less comfortable disclosing items that decreased their chances. The expectation of a positive outcome can also lead individuals to answer questions they previously considered unacceptable as was observed in Study 5 (Section 4.7). The implication of this finding for lenders is that they should attempt to collect data that participants feel will make them look good. Study 1 (Section 4.3), shows that this is something lenders are aware of and are already doing: they sometimes include questions in application forms that applicants enjoy answering (e.g. charity donations). However, this contributes to a bigger gap between the perceived use of applicants' data and its real use. This is in the interest of lenders who want to keep the risk assessment process obscure, but not in the interest of the applicants who do not fully understand how their data is being used.

The lack of transparency of the credit scoring process makes it difficult for applicants to understand the relevance of some questions. Studies 1, 2, 4, and 5 show that lower perceived relevance of a data request is associated with a more negative perception of that request. The implication of this finding for industry regulators is that improving the transparency of the risk assessment would contribute to applicants feeling more comfortable when providing personal data to lenders, possibly improving the quality of the data disclosed in the process. Study 5 investigated the impact of providing an explanation for each data request in a credit card application form, but found no effect on disclosure. Likely, more graphical ways of communicating the purpose of a data request will offer better results for researchers and designers. The challenge for industry and regulators is on how to combine transparency and predictive power.

Study 2 revealed that individuals are more comfortable disclosing items such as name and gender, which are commonly asked in forms. They are less comfortable disclosing financial data - which is consistent with past research - and phone numbers because they fear being contacted at awkward times. Study 5 also showed that items that are perceived as more sensitive are less likely to be disclosed, while less sensitive items are more likely to be disclosed. The implication for lenders is that the more sensitive the items requested the higher will item non-response be harming the data quality. Whenever possible, lenders should aim to collect low-sensitive items. While not collecting phone numbers may be feasible, it seems unlikely that the predictive power of the risk assessment process could be maintained without collecting financial data. One possible solution is to use alternative items that are also indicators of credit worthiness. Study 3 investigated the perceived sensitivity of such items and found that individuals are comfortable disclosing data items related to their bill payment history when applying for a loan, but not data related to their social networks. The implication for the industry is that individuals with thin credit histories or who feel uncomfortable disclosing other items could use past bill payments to show their ability to repay debts. Indices of social capital on the other hand were found to be very sensitive and it is not realistic that they can be used for credit scoring purposes without consumers reacting adversely.

Study 5 revealed that sensitive ratings of a nationally representative sample for one data item (collected in Study 2) were a predictor of the disclosure rate of the same item of a different sample in the same population (UK). This has a significant implication for privacy researchers since it suggests average data sensitive ratings have a better predictive power than the commonly used measures of privacy concern (see Section 2.1.1.8). This finding is also of relevance for any organisations that collects personal data. By measuring the perceived sensitivity of the data they collect for a sample representative of their data subjects they could estimate the probability of individuals not complying with data requests.

#### 10.1.3.2 Research findings on potential privacy issues of serious-games system deployed in organisational contexts

The studies in Chapter 5 identify the privacy implications of an employer deploying a serious-game platform aimed at supporting their employees' skill development needs. Studies 1, 2, and 3 (Sections 5.2, 5.3, 5.4) showed that the main privacy concern associated with such a system is that game performance could result in players looking bad in front of their peers and managers and the resulting negative consequences for career and reputation. This finding has serious implications for organisations that want to use technology-enhanced learning systems to address training needs. A successful learning experience requires learners to not be afraid to take risks, experiment with novel solutions for problems, and make mistakes. Thus, organisations deploying such systems must consider whether their main goal is to support learning or to collect performance data to assist in management decisions. This goal has to be communicated clearly to players so that they know how to approach the game.

This finding has also implications for serious-games developers who will have to design the system in such a way that it will not be considered invasive by its players. Keeping negative data from flowing outside the game would avoid some of the harmful outcomes identified in the studies, but would also undermine some of the benefits of serious games, such as the leveraging of competitive and social elements of games to improve knowledge transfer. One possible compromise is to allow players themselves to control the selective disclosure of their game data; another is to release aggregated data, such as at the team level.

Studies 2 and 3 revealed that another potential privacy risk is how identifiable players are. This is connected to the points already mentioned in this section. Anonymous play would allow more risk-taking and fewer privacy concerns. However, the lack of a stable identifier linked to a real person that could be held accountable for behaviour in the game would prevent the temporal, social and institutional embeddedness of players and decrease the ability to place trust well. One possible solution would be the use of pseudonyms, which make to link to an identity fuzzier, but are still stable across time and support trustworthiness. The implication for developers is that privacy mechanisms must be considered within the constraints of the goals of the system. The simple anonymisation of in-game actions would be detrimental for the learning experience in this case.

These findings have implications for privacy researchers in that they show that research on privacy risks of learning systems cannot be isolated from workplace privacy research. The system and context of deployment must be investigated together to identify risks resulting from their combination.

#### 10.1.3.3 Research findings on citizens' perceptions of personal data collection and use by the government

Studies in Chapter 6 showed that census respondents sometimes omit or answer incorrectly to census questions. Study 2 (Section 6.3) identified a link between perceived sensitivity of questions and likelihood of admitting to having engaged in these privacy protection behaviours. The obvious implication for census authorities is that the higher the sensitivity of the questions asked the lower the quality of the data they will obtain. The value that sensitive data items provide for decision making processes should be assessed to determine whether it is worth the risk of collecting sub-optimal data. Authorities can then focus on data items that provide the most value and maximise response rates. Study 1 (Section 6.2) showed that respondents do not always understand why certain data items are being asked and have concerns about how the data will be used. Census authorities should make an effort to clarify the link between the census data collection and real benefits that local communities have experienced as a result as, at the moment, this connection is too abstract.

Study 2 also revealed that the later respondents submitted the census the more likely it is that they engaged in privacy protection behaviours. As a result, researchers and decision-makers who make use of census data should consider that censuses submitted long after the deadline may provide lower quality data and put in place stronger validation processes than usual. It was also shown that racial minorities are more likely to omit and falsify data. While this phenomenon has been observed in the United States, it was the first time it was identified in the UK. This implies that certain communities in the UK may feel disenfranchised and, as a result, do not engage with the census. Again, census authorities would be advised to communicate better how census data may benefit these respondents.

Study 2 showed that average comfort with item disclosure has a significant effect on stated likelihood to engage in privacy protection behaviour. As in the case of Chapter 4: studies, sensitivity ratings (both sample averages for a single item and averages across items for one individual) seem to be better predictors of privacy attitudes and behaviour than classic privacy measures. In fact, the relationship between Westin's privacy concern measure and census attitudes was also investigated but no link was found. As past research has suggested, Westin's measure seems to be a poor predictor of privacy attitudes or behaviour and, as such, better measures of privacy concern should be investigated. A promising direction for future research seems to be to create such a measure around ratings for comfort with disclosure.

#### 10.1.3.4 Research findings on individuals' perceptions of rich-media personalised advertising

Chapter 7 shows that the type of personal data used to personalise an ad affects the users' perceptions of that ad, with discomfort increasing as ads become more personalised. In parallel, it was also shown that ads with that incorporate the user's name or photo are significantly more noticeable. The implication for advertisers is that they should aim to identify types of personalisation that result in ads that are noticeable, but comfortable at the same time. Focusing solely on whether ads catch attention would not be advisable as the advertised brands could face a significant consumer backlash as a result of users associating them with feelings of privacy invasion. It was also shown that a potential source of concern for users is the lack of transparency on how ads are personalised. Advertises should be careful to provide a simple channel (on the ad itself, for example) for users to learn why they are getting that ad. A consequence of the trend towards personalisation identified in Study 1 is that users sharing devices may infer private details about each other based on the personalised ads displayed. This is something that the industry must consider, as there is potential for significant privacy invasions.

This was the first study that investigated perceptions of rich media personalised ads and that compared different types of personalisation (including one that used the participant's photo) on noticeability, interest, and comfort. Moreover, to address limitations of past research on targeted advertising, which has for the most part relied on surveys, a lab experimental design was used and measures of attention captured to validate self-reports of noticeability. Future research should continue this trend for observation of actual reactions. As new and varied paradigms for the inclusion of personal data in advertisement emerge, it is crucial that researchers control exactly what type of ads participants are exposed to and do not capture only general perceptions of "personalised advertising." Meanwhile, commercial researchers who want to design more effective and acceptable ads should focus on personalisation that does not employ users' picture.

## 10.2 Future work

The disclosure model presented in this thesis provides a base from which to assess data collection efforts and estimate how they will be perceived and responded to by individuals, but further work is required to fully validate it. In particular, future research should focus on: (1) validating the remaining factors not covered in the validation study; (2) identifying additional factors that did not emerge in this thesis; (3) confirming if same factors are relevant in other contexts; and (4) exploring the relationship between factors.

The final study in this thesis (see Chapter 9) had the aim to partially validate the link between four of the factors in the disclosure model and actual disclosure behaviour, namely likelihood of response and likelihood of falsification. The study showed that two of the factors were significant predictors of disclosure decision: perceived fairness and sensitivity of data items; but no support was found for the other two factors. Additionally, most of the model items were not included in this study, for budget, time, and participant convenience reasons. Future work should address these limitations and investigate whether the remaining factors are predictors of disclosure decision using methods similar to this validation study where participants are not aware they are part of an experiment and the realism of their behaviour is maximised. These new studies could each pick a subset of factors to test or, if budget and time were not obstacles, test all the factors at the same time. This, however, does not seem feasible due to the burden it would put on participants and which could harm the internal validity of the results.

Another avenue for future research is to identify other sets of factors that were not covered in this thesis, but that are also linked to disclosure behaviour. This could mean further exploring factors related to the perception of data requests not mentioned here or augmenting the model with other types of factors considered outside the scope of this thesis, such as ones related to personality of personal background. For example, it seems likely that some measure of privacy concern, other than Westin's, may have an impact on disclosure and ethnicity has been connected to attitudes towards disclosure in the census in past research and also in this thesis.

New research can also focus on new contexts of interaction, industries, and types of individual-organisational relationships. Individuals are required to disclose personal data, both online and offline, in a multitude of situations every day. It would be important to understand whether the same factors emerge in these different situations. If that is the case, a general theory of privacy and disclosure could begin to be constructed. Moreover, other types of data relationships should be investigated. Individuals do not always get explicit requests for their personal data (see Chapter 5) or aware of how it was collected (see Chapter 7). It would be relevant to understand whether some factors are more important than others when mode of data collection varies.

The model presented in this thesis positions all the factors at the same level and makes no attempt to explain the relationships between them. Yet, there is clear indication in the thesis that some of the factors are related to each other. For instance, in Studies 2 and 3 of Chapter 4 (see Sections 4.4 and 4.5) it was shown that sensitivity and projected outcome were correlated, and in the validation study it seemed likely that perceived fairness and relevance were also correlated. These and other relationship between model factors must be investigated. It is possible some factors are antecedents of each other and if their links are clarified it might be possible to minimise the model while maintaining predictive power.

# REFERENCES

ACM, 1992. Association for Computing Machinery Code of Ethics and Professional Conduct. Available at: http://www.acm.org/about/code-of-ethics/

Ackerman, M.S., Cranor, L.F. & Reagle, J., 1999. Privacy in e-commerce: examining user scenarios and privacy preferences. In *Proceedings of the 1st ACM conference on Electronic commerce*. Denver, Colorado, United States: ACM, pp. 1–8.

Ackerman, M.S. & Mainwaring, S.D., 2005. Privacy Issues and Human-Computer Interaction. In *Security and Usability: Designing Secure Systems That People Can Use*. Sebastopol, CA: O'Reilly, pp. 381-399.

Ackoff, R.L. & Rovin, S., 2003. *Redesigning society*, Stanford University Press.

Acquisti, A., 2004. Privacy in electronic commerce and the economics of immediate gratification. In Proceedings of the 5th ACM conference on Electronic commerce. New York, NY, USA: ACM, pp. 21-29.

Acquisti, A., John, L.K. & Loewenstein, G. 2012. The impact of relative standards on the propensity to disclose. *Journal of Marketing Research*, 49(2), pp.160–174.

Adams, A., 2001. Users' Perceptions of Privacy In Multimedia Communications. PhD. University College London.

Adams, A. & Sasse, A., 2001. Privacy in Multimedia Communications: Protecting Users, Not Just Data. In A. Blandford, J. Vanderdonckt, & P. Gray, eds. *People and Computers XV - Interaction Without Frontiers: Joint Proceedings of HCI 2001 and IHM 2001.* London: Springer, pp. 49–64.

Anand, B. and Shachar, R., 2009. Targeted advertising as a signal. *Quantitative Marketing and Economics*, 7 (3), 237-266.

Andersen, B., Fradinho, M., Lefrere, P. & Niitamo, V., 2009. The Coming Revolution in Competence Development: Using Serious Games to Improve Cross-Cultural Skills. In *Online Communities and Social Computing*. pp. 413-422.

Annacker, D., Spiekermann, S. & Strobel, M., 2001. e-Privacy: Evaluating a New Search Cost in Online Environments. In *Proceedings of the 14th Bled Electronic Commerce Conference (BLED 2001)*. Bled, Slovenia, pp. 292–308.

Antón, A.I., Earp, J.B. & Reese, A., 2004. *An Analysis of Web Site Privacy Policy Evolution in the Presence of HIPAA*, North Carolina State University Computer Science Technical Report. Available at: http://theprivacyplace.org/blog/wp-content/uploads/2008/07/hipaa_7_24_submit.pdf [Accessed April 13, 2012].

Anwar, M.M., Greer, J. & Brooks, C.A., 2006. Privacy enhanced personalization in e-learning. In *Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services*. Markham, Ontario, Canada: ACM, pp. 1-4.

Agrawal, R. & Srikant, R., 2000. Privacy-preserving data mining. *SIGMOD Rec.*, 29(2), 439-450.

Agre, P.E. & Rotenberg, M., 1998. Technology and Privacy: The New Landscape, MIT Press.

Ariss, S.S., 2002. Computer monitoring: benefits and pitfalls facing management. *Information & Management*, 39(7), pp.553-558.

Aristotle, 1999. *Politics*, Kitchener: Batoche Books.

Barbaro, M. & Zeller, T., 2006. A Face Is Exposed for AOL Searcher No. 4417749. *New York Times*. Available at: http://query.nytimes.com/gst/fullpage.html?res=9E0CE3DD1F3FF93AA3575BC0A9609C8B63 [Accessed April 13, 2012].

Barkhuus, L. & Dey, A., 2003. Location-Based Services for Mobile Telephony: a study of users' privacy concerns. In *Proceedings of Interact 2003*. Zurich, Switzerland: ACM Press, pp. 709 - 712.

Batini, C. & Scannapieco, M., 2006. *Data Quality*, Springer.

Beales, H., 2010. The Value of Behavioral Targeting, Network Advertising Initiative, Washington, D.C..

Bellinger, G., Castro, D. & Mills, A., 2004. Data, Information, Knowledge, & Wisdom. Available at: http://www.systems-thinking.org/dikw/dikw.htm [Accessed April 13, 2012].

Berendt, B., Günther, O. & Spiekermann, S., 2005. Privacy in e-commerce: stated preferences vs. actual behavior. *Commun. ACM*, 48(4), 101-106.

Beresford, A.R., Kübler, D. & Preibusch, S., 2010. Unwillingness to Pay for Privacy: A Field Experiment ( No. 5017), Discussion Paper Series. Institute for the Study of Labor (IZA), Bonn, Germany.

Bodea, G., Huijboom, N., Oort, S. van, Ooms, M., Schoonhoven, B. van, Bakker, T., Teernstra, L., Finn, R.L., Bernard-Wills, D., Wright, D., Raab, C.D., 2013. PRISMS Deliverable 3.1: Draft analysis of privacy and security policy documents in the EU and US. Part II: A discourse analysis of selected privacy and security policy, PRISMS project. European Union 7th Framework Programme.

Bolger, N., Davis, A. & Rafaeli, E., 2003. Diary methods: capturing life as it is lived. *Annual Review of Psychology*, 54, 579-616.

Bowman, C. & Ambrosini, V., 2000. Value Creation Versus Value Capture: Towards a Coherent Definition of Value in Strategy. *British Journal of Management*, 11(1), 1-15.

Boyle, P. & Dorling, D., 2004. Guest editorial: the 2001 UK census: remarkable resource or bygone legacy of the “pencil and paper era”? Area, 36(2), pp.101–110.

Brostoff, S., 2009. Financial Exclusion Internal Report.

Braun, V. & Clarke, V., 2006. Using thematic analysis in psychology. Qualitative research in psychology, 3(2), pp.77–101.

Brunk, B., 2005. A User-Centric Privacy Space Framework. In *Security and Usability: Designing Secure Systems That People Can Use*. Sebastopol, CA: O'Reilly, pp. 401-420.

Bryman, A., 2006. Integrating quantitative and qualitative research: how is it done? *Qualitative Research* 6, 97–113.

Business Week/Harris Poll, 1998. *Online Insecurity*, Business Week/Harris Poll. Available at: http://www.businessweek.com/1998/11/b3569107.htm [Accessed April 13, 2012].

Charmaz, K., 2006. *Constructing grounded theory*, SAGE.

Chen, R. & Sanders, G.L., 2007. Electronic Monitoring in Workplace: Synthesis and Theorizing. In *AMCIS 2007 Proceedings*. AMCIS 2007.

Clarke, R., 1997. Privacy Introduction and Definitions. Available at: http://www.rogerclarke.com/DV/Intro.html#Priv [Accessed April 13, 2012].

Clarke, R., 2006. What's Privacy? Available at: http://www.rogerclarke.com/DV/Privacy.html [Accessed April 13, 2012].

Clifton, C. & Marks, D., 1996. Security and Privacy Implications of Data Mining. In *Proceedings of the 1996 ACM SIGMOD Workshop on Data Mining and Knowledge Discovery*.

Cohen, J., 1992. A Power Primer. *Psychological Bulletin*, 112(1), pp.155–159.

Collard, S. & Kempson, E., 2005. *Affordable credit*, Bristol, UK: The Policy Press.

comScore, 2008. U.S. Retail E-Commerce Growth Rates Soften In May and June. Available at: http://www.comscore.com/press/release.asp?press=2356 [Accessed April 13, 2012].

Consolvo, S., Smith, I.E., Matthews, T., LaMarca, A., Tabert, J., Powledge, P., 2005. Location disclosure to social relations: why, when, & what people want to share, in: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '05*. ACM, New York, NY, USA, pp. 81–90.

Cooper, J., Chalton, S.N.L., Gaskill, S., Walden, I.N., Inger, L., 1988. Encyclopedia of Data Protection and Privacy. Sweet & Maxwell.

Couper, M.P., Singer, E. & Kulka, R.A., 1998. Participation in the 1990 Decennial Census Politics, Privacy, Pressures. American Politics Research, 26(1), pp.59–80.

Cranor, L., Dobbs, B., Egelman, S., Hogben, G., Humphrey, J., Langheinrich, M., Marchiori, M., Presler-Marshall, M., Reagle, J., Schunter, M., Stampley, D.A., and Wenning, R., 2006. The Platform for Privacy Preferences 1.1 (P3P1.1) Specification. Available at: http://www.w3.org/TR/P3P11/ [Accessed 13 April 2012]

Cranor, L.F., Egelman, S., Sheng, S., McDonald, A.M., Chowdhury, A., 2008. P3P deployment on websites. Electronic Commerce Research and Applications 7, 274–293.

Culnan, M.J., 1993. "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. *MIS Quarterly*, 17(3), 341-363.

Culnan, M.J. & Armstrong, P.K., 1999. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, 10, pp.104–115.

Culnan, M. J. & Milne, G.R., 2001. The Culnan-Milne Survey on Consumers & Online Privacy Notices.

Cvrcek, D., Kumpost, M., Matyas, V. & Danezis, G., 2006. A study on the value of location privacy. In *Proceedings of the 5th ACM workshop on Privacy in electronic society*. Alexandria, Virginia, USA, pp. 109–118.

Davies, S., n.d.. New Techniques and Technologies of Surveillance in the Workplace. Available at: http://www.amicustheunion.org/pdf/surveillencetechniques.pdf [Accessed April 13, 2012].

Delo, C., 2013. Facebook Drops 'Sponsored Stories' As It Pares Down Ad Formats. AdAge, New York, NY, 2013. Available at: http://adage.com/article/digital/facebook-drops-sponsored-stories-cuts-ad-formats/241969/

Devlin, J.F., 2005. A Detailed Study of Financial Exclusion in the UK. *Journal of Consumer Policy*, 28(1), 75-108.

Denzin, N.K. & Lincoln, Y.S., 1998. Introduction: Entering the field of qualitative research. In *The Landscape of Qualitative Research*. Thousand Oaks, California: SAGE.

Dinev, T. & Hart, P., 2006. An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, 17(1), 61-80.

Drèze, X. and Hussherr, F.-X., 2003. Internet advertising: Is anybody watching? *Journal of Interactive Marketing*, 17 (4), 8-23.

Dworkin, G., 1973. The Younger Committee Report on Privacy. The Modern Law Review 36, 399–406.

Efferink, L. van, 2012. Matthew Hannah: Germany's census boycott, police tactics, oppression, biopolitics. Exploring Geopolitics. Available at: http://www.exploringgeopolitics.org/Interview_Hannah_Matthew_Germany_Census_Boycott_Police_Tactics_Oppression_Biopolitics_of_Populations_Nazi_Aggression_Rote_Armee_Fraktion_RAF.html [Accessed March 27, 2013].

Electronic Privacy Information Center, 2000. *Pretty Poor Privacy: An Assessment of P3P and Internet Privacy*, Electronic Privacy Information Center.

El-Khatib, K., Korba, L. & Lee, G., 2003. Privacy and security in E-learning. *International Journal of Distance Education Technologies*, 1(4), 1-19.

European Commission, 1995. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML [Accessed April 13, 2012].

Eurostat, 2012. Glossary:Equivalised disposable income. *Statistics Explained*. Available at: http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Glossary:Equivalised_disposable_income [Accessed October 16, 2013].

Experian, 2013. Mosaic UK - unique consumer classification based on in-depth demographic data. Available at: http://www.experian.co.uk/business-strategies/mosaic-uk.html [Accessed March 14, 2013].

Fairweather, N.B., 1999. Surveillance in Employment: The Case of Teleworking. *Journal of Business Ethics*, 22, pp.39-49.

Federal Trade Commission, 1998. *Privacy Online: A Report to Congress* , Federal Trade Commission.

Fiveash, K., 2012. Facebook facepalm: US judge tosses out “sponsored stories” deal. *The Register*. Available at: http://www.theregister.co.uk/2012/08/20/facebook_sponsored_stories_lawsuit/ [Accessed October 12, 2013].

Fried, C., 1967. Privacy. *Yale Law Journal*, 77, 475.

Friedman, B., Lin, P. & Miller, J.K., 2005. Informed Consent by Design. In *Security and Usability: Designing Secure Systems That People Can Use*. Sebastopol, CA: O'Reilly, pp. 495-521.

Gavison, R., 1979. Privacy and the Limits of Law. *Yale Law Journal*, 89, 421.

Grossklags, J. & Acquisti, A., 2007. When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information. In Workshop on Economics of Information Security.

Guba, E.G. & Lincoln, Y.S., 1998. Competing paradigms in qualitative research. In *The Landscape of Qualitative Research*. Thousand Oaks, California: SAGE.

Hackos, J.T. & Redish, J.C., 1998. *User and Task Analysis for Interface Design* 1st ed., Wiley.

Hann, I., Hui, K.-L., Lee, S.-Y.T. & Png, I.P.L., 2002a. Online information privacy: Measuring the cost-benefit trade-off, in: *Proceedings of the Twenty-Third International Conference on Information Systems*. L. Applegate, R. D. Galliers, and J. I. DeGross, Barcelona, pp. 1–10.

Hann, I., Hui, K., Lee, T.S. & Png, I.P.L., 2002b. The Value of Online Information Privacy: Evidence from the USA and Singapore. International Conference on Information Systems.

Harper, J. & Singleton, S., 2001. *With A Grain of Salt: What Consumer Privacy Surveys Don't Tell Us*, Washington, DC: Competitive Enterprise Institute.

Hastak, M. and Culnan, M.J., 2010. Future of Privacy Forum Online Behavioral Advertising “Icon” Study Summary of Key Results.

Heeney, C., 2012. Breaching the Contract? Privacy and the UK Census. The Information Society, 28(5), pp.316–328.

Hine C. & Eve J., 1998. Privacy in the Marketplace. *The Information Society*, 14, 253-262.

Holbrook, M.B., 1999. Consumer value: a framework for analysis and research, Psychology Press.

Hollis, N., 2005. Ten Years of Learning on How Online Advertising Builds Brands. *Journal of Advertising Research*, 45 (02), 255-268.

Hormozi, A.M. & Giles, S., 2004. Data Mining: A Competitive Weapon for Banking and Retail Industries. *Information Systems Management*, 21(2), 62.

Horne, D.R., Norberg, P.A. & Ekin, A.C., 2007. Exploring consumer lying in information-based exchanges. *Journal of Consumer Marketing*, 24(2), 90 - 99.

Hui, K., Teo, H.H. & Lee, S.T., 2007. The Value of Privacy Assurance: An Exploratory Field Experiment. *MIS Quarterly*, 31(1), 19-33.

Inness, J.C., 1992. *Privacy, intimacy and isolation*, Oxford University Press.

Jarrett, C. & Gaffney, G. 2009. *Forms that Work: Designing Web Forms for Usability*. Interactive Technologies. Elsevier Science.

Jennett, C., Brostoff, S., Malheiros, M., Sasse, M. A., 2010. Investigating loan applicants' perceptions of alternative data items and the effect of incentives on disclosure. *Privacy and Usability Methods Pow-wow (PUMP) 2010: Proceedings*. British Computer Society.

Jennett, C., Brostoff, S., Malheiros, M., Sasse, M. A., 2012a. Adding insult to injury: Consumer experiences of being denied credit. International Journal of Consumer Studies 36(5), 549-555 doi:10.1111/j.1470-6431.2012.01120.x.

Jennett, C., Malheiros, M., Brostoff, S. & Sasse, M. A., 2012b. Privacy for loan applicants versus predictive power: Is it possible to bridge the gap? In S. Gutwirth et al. (Eds.) *European Data Protection: In Good Health?* pp. 35-52. Springer Press.

Jerman-Blazic, B. & Klobucar, T., 2005. Privacy provision in e-learning standardized systems: status and improvements. Computer Standards & Interfaces, 27(6), 561-578.

Johnson, B., 2009. Older users becoming dominant on Facebook. *The Guardian*. Available at: http://www.guardian.co.uk/technology/blog/2009/jul/07/facebook-socialnetworking [Accessed April 13, 2012].

Joinson, A.N. & Paine, C.B. 2007. Self-Disclosure, Privacy and the Internet. In A.N Joinson, K.Y.A McKenna, T. Postmes and U-D. Reips (Eds). *Oxford Handbook of Internet Psychology* (pp. 237-252). Oxford University Press.

Jupiter Research, 2002. Security and Privacy Data. Available at: http://www.ftc.gov/bcp/workshops/security/020520leathern.pdf

Karat, C., Brodie, C. & Karat, J., 2005. Usability design and evaluation for privacy and security solutions. In *Security and Usability: Designing Secure Systems That People Can Use*. Sebastopol, CA: O'Reilly, pp. 381-399.

Kean, A. and Dautlich, M., 2009. A guide to online behavioural advertising, Internet Advertising Bureau, London.

Kelly, K.A., 2002. Private Family, Private Individual: John Locke's Distinction between Paternal and Political Power. *Social Theory and Practice*, Vol. 28, No.3, pp. 361-380.

Kent, W., 2000. *Data and Reality*, Authorhouse.

Kitzinger, J., 1995. Qualitative Research: Introducing focus groups. *BMJ*, 311(7000), 299-302.

Kling, R., 1996. *Computerization and Controversy* 2nd ed., Morgan Kaufmann.

Knowledge@Wharton., 2008. Privacy on the web: Is it a losing battle? Knowledge@Wharton Philadelphia, PA.

Kobsa, A. & Teltzrow, M. 2005. Contextualized communication of privacy practices and personalization benefits: Impacts on users’ data sharing and purchase behavior. *Privacy Enhancing Technologies*, pp. 329–343.

Kontio, J., Lehtola, L. & Bragge, J., 2004. Using the Focus Group Method in Software Engineering:
Obtaining Practitioner and User Experiences. In *Proceedings of the 2004 International Symposium on Empirical Software Engineering (ISESE’04)*.

Kourti, I., 2009. *Project FLAME Social Study Report*, Available at: http://tnc2009.terena.org/core/getfile2f59.pdf?file_id=350 [Accessed April 13, 2012].

Krol, K., Moroz, M., & Sasse, M. A., 2012. Don’t work. Can’t work? Why it’s time to rethink security warnings, in: 2012 7th International Conference on Risk and Security of Internet and Systems (CRiSIS). Presented at the 2012 7th International Conference on Risk and Security of Internet and Systems (CRiSIS), pp. 1–8.

Laufer, R. S., M. Wolfe. 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, 33(3), pp. 22–42.

Lederer, S., J. Mankoff, and A.K. Dey., 2003. Who Wants to Know What When? Privacy Preference Determinants in Ubiquitous Computing. In Proceedings of *Extended Abstracts of CHI 2003, ACM Conference on Human Factors in Computing Systems.* Fort Lauderdale, FL. pp. 724- 725.

Lederer, S., Hong, I., Dey, K., Landay, A., 2004. Personal privacy through understanding and action: five pitfalls for designers. *Personal Ubiquitous Comput.* 8, 440–454.

Lewis, P., 2009. Every step you take: UK underground centre that is spy capital of the world. *The Guardian*. Available at: http://www.guardian.co.uk/uk/2009/mar/02/westminster-cctv-system-privacy [Accessed April 13, 2012].

Leyshon, A., Signoretta, P., Knights, D., Alferoff, C., Burton, D., 2006. Walking with Moneylenders: The Ecology of the UK Home-collected Credit Industry. *Urban Stud*, 43(1), 161-186.

Lin, M., Prabhala, N.R. & Viswanathan, S., 2009. Judging Borrowers by the Company They Keep: Social Networks and Adverse Selection in Online Peer-to-Peer Lending. *SSRN eLibrary*. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1355679 [Accessed March 25, 2010].

Locke, J., 1823. Two Treatises of Government. In The works of John Locke. A new edition, corrected, in ten volumes. London.

Lwin, M.O. & Williams, J.D., 2003. A Model Integrating the Multidimensional Developmental Theory of Privacy and Theory of Planned Behavior to Examine Fabrication of Information Online. *Marketing Letters* 14(4), pp. 257–272.

Lyon, D., 2003. Surveillance As Social Sorting: Privacy, Risk, and Digital Discrimination, Psychology Press.

Malheiros, M., Preibusch, S. & Sasse, M.A., 2013. "Fairly Truthful": The Impact of Perceived Effort, Fairness, Relevance, and Sensitivity on Personal Data Disclosure. In M. Huth et al., eds. *Trust and Trustworthy Computing*. Lecture Notes in Computer Science. Springer Berlin Heidelberg, pp. 250–266.

Malheiros, M., Brostoff, S., Jennett, C. & Sasse, M.A., 2012a. Would You Sell Your Mother's Data? Personal Data Disclosure in a Simulated Credit Card Application. 11th Annual Workshop on the Economic of Information Security (WEIS 2012), Berlin, Germany, June 25-26, 2012

Malheiros, M., Jennett, C., Patel, S., Brostoff, S., Sasse, M. A., 2012b. Too close for comfort: A study of the effectiveness and acceptability of rich-media personalized advertising. Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems. ( pp.579-588). New York, NY, USA: ACM

Malheiros, M., Jennett, C., Seager, W. & Sasse, M.A., 2011. Trusting to Learn: Trust and Privacy Issues in Serious Games. In J. M. McCune et al., eds. *Trust and Trustworthy Computing*. Lecture Notes in Computer Science. Springer Berlin Heidelberg, pp. 116-130

Malhotra, N.K., Kim, S.S., & Agarwal, J. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale and a causal model. *Information Systems Research*, 15, 336–355.

McDonald, A.M. and Cranor, L.F., 2010. Beliefs and behaviors: Internet users‟ understanding of behavioural advertising. *Telecommunications Policy Research Conference*.

McKinlay, A. & McVittie, C., 2008. *Social Psychology and Discourse*, Wiley-Blackwell.

Metzger, M.J., 2007. Communication Privacy Management in Electronic Commerce. *Journal of Computer-Mediated Communication*, 12(2), pp.335–361.

Milberg, S.J., Smith, H.J. & Burke, S.J., 2000. Information Privacy: Corporate Management and National Regulation. *Organization Science*, 11(1), 35-57.

Mill, J.S., 1859. On Liberty.

Milne, G.R. & Gordon, M.E., 1993. Direct Mail Privacy-Efficiency Trade-offs within an Implied Social Contract Framework. *Journal of Public Policy & Marketing*, 12(2), 206-215.

Miltgen, C.L., 2007. Customers’ privacy concerns and responses toward a request for personal data on the internet: an experimental study ( No. 369). Université Paris Dauphine, DMSP, Paris, France.

Nejdl, W. & Wolpers, M., 2004. European E-Learning: Important Research Issues and Application Scenarios. In Proceedings of ED-MEDIA 2004, World Conference on Educational Multimedia, Hypermedia & Telecommunications. Lugano, Switzerland: Association for the Advancement of Computing in Education (AACE).

Nissenbaum, H., 2004. Privacy as Contextual Integrity. Washington Law Review, 79(1). Available at: http://papers.ssrn.com/abstract=534622 [Accessed October 3, 2012].

OFT., 2010. Online targeting of advertising and prices: A market study, Office of Fair Trading, London.

O'Hara, K. & Shadbolt, N., 2008. *The Spy in the Coffee Machine*, Oxford: Oneworld.

Olivero, N. & Lunt, P., 2004. Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology*, 25(2), pp.243-262.

ONS, 2013. Office for National Statistics. Available at: http://www.ons.gov.uk [Accessed March 14, 2013].

Paine, C., Reips, U.-D., Stieger, S., Joinson, A., Buchanan, T., 2006. Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of Human-Computer Studies*, 65(6), 526-536.

Pew Internet & American Life Project, 2000. *Trust and privacy online: Why Americans want to rewrite the rules*, The Pew Internet & American Life Project.

Phelps, J., Nowak, G. & Ferrell, E., 2000. Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, 19(1), pp. 27-41

Posner, R.A., 1978. The Right of Privacy. *Georgia Law Review*, 12(3), 393 - 422.

Posner, R.A., 1981. The Economics of Privacy. *The American Economic Review*, 71(2), 405-409.

Potter, J., Wetherell, M., 1987. "Unfolding discourse analysis", in Wetherell, M. et al., 2001. *Discourse theory and practice: a reader*, SAGE.

Potter, J., Wetherell, M., 1994. "Analyzing discourse", in Bryman, A., Burgess, B., (Eds), Analyzing Qualitative Data, London; Routledge

Potter, J., Wetherell, M., 1995. "Discourse analysis", in Smith, J., Harré, R., van Langenhove, R., (Eds), Rethinking Methods in Psychology, London; Sage

Potter, J., 1996. "Discourse analysis and constructionist approaches: theoretical background", in Richardson, J.T.E., 1996. Handbook of qualitative research methods for psychology and the social sciences, Wiley-Blackwell.

Preibusch, S., Kübler, D. & Beresford, A., 2013. Price versus privacy: an experiment into the competitive advantage of collecting less personal information. *Electronic Commerce Research*, pp.1–33.

Raab, C.D. & Bennett, C.J., 1998. The Distribution of Privacy Risks: Who Needs Protection? *The Information Society*, 14, 263-274.

Razavi, M.N. & Iverson, L., 2006. A grounded theory of information sharing behavior in a personal learning space. In *Proceedings of the 2006 20th anniversary conference on Computer supported cooperative work*. Banff, Alberta, Canada: ACM, pp. 459-468.

Redman, T.C., 1998. The impact of poor data quality on the typical enterprise. *Commun. ACM*, 41(2), pp.79-82.

Reiman, J.H., 1995. Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future. *Santa Clara Computer and High-Technology Law Journal* , 11, 27.

Riegelsberger, J., Sasse, M.A. & McCarthy, J.D., 2003. The researcher's dilemma: evaluating trust in computer-mediated communication. *International Journal of Human-Computer Studies*, 58(6), 759-781.

Riegelsberger, J., 2005. *Trust in Mediated Interactions*. PhD. University College London.

Rieman, J., 1996. A field study of exploratory learning strategies. *ACM Trans. Comput.-Hum. Interact.*, 3(3), 189-218.

Rimmer, J., Wakeman, I., Sheeran, L. and Sasse, M. A. 1999. Examining Users' Repertoire of Internet Applications. Proc. seventh IFIP Conference on Human-Computer Interaction - INTERACT '99, Edinburgh, UK.

Robson, C., 2002. *Real world research*, Wiley-Blackwell.

Ross, T., 2011. Census 2011: an army of enforcers. Telegraph.co.uk. Available at: http://www.telegraph.co.uk/news/uknews/8408003/Census-2011-an-army-of-enforcers.html [Accessed March 14, 2013].

Rudra, A. & Yeo, E., 1999. Key issues in achieving data quality and consistency in data warehousing among large organisations in Australia. In *Proceedings of the 32nd Annual Hawaii International Conference on*. *System Sciences, 1999. HICSS-32*..

Schneier, B., 2009. Privacy and the Fourth Amendment. Available at: http://www.schneier.com/blog/archives/2009/03/privacy_and_the_1.html [Accessed April 13, 2012].

Sheehan, K.B. & Hoy, M.G., 1999. Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns. *Journal of Advertising,* 28(3), pp. 37–51.

Sherman , E., 2008. Privacy Policies are Great -- for PhDs. *BNet*. Available at: http://www.cbsnews.com/8301-505124_162-43440282/privacy-policies-are-great----for-phds/ [Accessed April 13, 2012].

Simpson, L., 2003. Are the census outputs fit for purpose? In Census 2001 and Beyond Office for National Statistics and the Royal Statistical Society Conference. pp. 11–12. Available at: http://www.ccsr.ac.uk/staff/Ludi/documents/RSSONSNov03Simpson.pdf [Accessed March 11, 2013].

Singer, E., Bates, N. & Van Hoewyk, J., 2011. Concerns about privacy, trust in government, and willingness to use administrative records to improve the decennial census. In Annual Meeting of the American Association for Public Opinion Research, Phoenix Arizona. Available at: https://www.amstat.org/sections/srms/Proceedings/y2011/Files/400168.pdf [Accessed March 11, 2013].

Singer, E., Hoewyk, J.V. & Neugebauer, R.J., 2003. Attitudes and Behavior: The Impact of Privacy and Confidentiality Concerns on Participation in the 2000 Census. Public Opinion Quarterly, 67(3), pp.368–384.

Singer, E., Mathiowetz, N.A. & Couper, M.P., 1993. The Impact of Privacy and Confidentiality Concerns on Survey Participation the Case of the 1990 U.s. Census. Public Opinion Quarterly, 57(4), pp.465–482.

Smith, G.K. 1994. Privacy in the Information Age. De Montfort University. Available at: http://www.ccsr.cse.dmu.ac.uk/resources/privacy/privinfoage.html [Accessed October 3, 2013]

Smith, H.J., 1993. Privacy policies and practices: inside the organizational maze. Communications of the ACM, 36(12), 104-122.

Smith, H.J., Milberg, S.J. & Burke, S.J., 1996. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, 20(2), 167-196.

Snyder, J.L., 2010. E-Mail Privacy in the Workplace. Journal of Business Communication, 47(3), pp.266 -294.

Solove, D.J., 2007. 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Diego Law Review*, 44, 747.

Solove, D.J., 2008. *Understanding Privacy*, Cambridge, Massachusetts: Harvard University Press.

Spiekermann, S., Grossklags, J., Berendt, B., 2001. E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior, in: *Proceedings of the 3rd ACM Conference on Electronic Commerce*. ACM, Tampa, Florida, USA, pp. 38–47.

Stewart, K.A., & Segars, A.H. 2002. An empirical examination of the concern for information privacy instrument. Information Systems Research, 13, 36–49.

Stone, E.F., Gueutal, H.G., Gardner, D.G., McClure, S., 1983. A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations. *Journal of Applied Psychology*, 68(3), 459-468.

Stone, E.F. and Stone, D.L., 1990. Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms in Research in *Personnel and Human Resources Management* (8), K. M. Rowland and G. R. Ferris (eds.), JAI Press, Greenwich, CT, pp. 349-411.

Strauss, A.L. & Corbin, J.M., 1998. *Basics of qualitative research*, Thousand Oaks, California: SAGE.

Strong, D.M., Lee, Y.W. & Wang, R.Y., 1997. Data quality in context. *Commun. ACM*, 40(5), 103-110.

The Sydney Morning Herald, 1851. The Census of a Century Ago. The Sydney Morning Herald.

Syverson, P., 2003. The paradoxical value of privacy. *In Proc. of 2nd Annual Workshop on Economics and Inform. Sec. (WEIS 2003)*.

Tolchinsky, P.D., McCuddy, M.K., Adams, J., Ganster, D.C., Woodman, R.W. &, Fromkin, H.L., 1981. Employee perceptions of invasion of privacy: A field simulation experiment. *Journal of Applied Psychology,* 66(3), pp. 308–313.

TRUSTe, 2011. 2011 Consumer Research Results: Privacy and Online Behavioral Advertising.

Tullis, T. & Albert, W., 2008. *Measuring the user experience*, Morgan Kaufmann.

Turow, J., King, J., Hoofnagle, C.J., Bleakley, A. and Hennessy, M., 2009. Americans Reject Tailored Advertising and Three Activities that Enable It. SSRN.

UK Data Protection Act 1998 (c.29) Available at:
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1 [Accessed April 13, 2012].

US Secretary's Advisory Committee, 1983. *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*. Available at: http://epic.org/privacy/hew1973report/ [Accessed October 3, 2013].

Vasalou, A., Gill, A., Mazanderani, F., Papoutsi, C. and Joinson, A., 2011. Privacy Dictionary: A New Resource for the Automated Content Analysis of Privacy. *Journal of the American Society for Information Science and Technology*, 62, 11, 2095-2105.

Verykios, V.S., Bertino, E., Fovino, I.N., Provenza, L.P., Saygin, Y., Theodoridis, Y., 2004. State-of-the-art in privacy preserving data mining. *SIGMOD Rec.*, 33(1), 50-57.

Warren, S.D. & Brandeis, L.D., 1890. The Right to Privacy. *Harvard Law Review*, (4), 193-220.

Weirich, D., 2006. Persuasive Password Security. PhD. University College London.

Westin, A.F., 2003. Social and Political Dimensions of Privacy. *Journal of Social Issues*, 59(2), 431--453.

White, T., Zahay, D., Thorbjørnsen, H. and Shavitt, S., 2008. Getting too personal: Reactance to highly personalized email solicitations. *Marketing Letters*, 19 (1), 39-50.

Williams, C., 2007. Information Commissioner pokes kids on social networking privacy. *The Register*. Available at: http://www.theregister.co.uk/2007/11/23/ico_social_networking_kids/ [Accessed April 13, 2012].

Williams, C., 2008. BT and Phorm secretly tracked 18,000 customers in 2006. *The Register*. Available at: http://www.theregister.co.uk/2008/04/01/bt_phorm_2006_trial/ [Accessed April 13, 2012].

Woodman, R.W., Ganster, D.C., Adams, J., McCuddy, M.K., Tolchinsky, P.D. & Fromkin, H., 1982. A Survey of Employee Perceptions of Information Privacy in Organizations. *The Academy of Management Journal,* 25(3), pp. 647–663.

Xu, H., Nord, J.H., Brown, N., Nord, G.D., 2002. Data quality issues in implementing an ERP. *Industrial Management & Data Systems*, 102(1), 47 - 58.

Yan, J., Liu, N., Wang, G., Zhang, W., Jiang, Y. and Chen, Z., 2009. How much can behavioral targeting help online advertising? *Proceedings of the 18th international conference on World Wide Web*, ACM, Madrid, Spain, 2009, 261-270.