LEABHARLANN CHOLÁISTE NA TRÍONÓIDE, BAILE ÁTHA CLIATH | TRINITY COLLEGE LIBRARY DUBLIN
Ollscoil Átha Cliath | The University of Dublin

Terms and Conditions of Use of Digitised Theses from Trinity College Library Dublin

Copyright statement

All material supplied by Trinity College Library is protected by copyright (under the Copyright and Related Rights Act, 2000 as amended) and other relevant Intellectual Property Rights. By accessing and using a Digitised Thesis from Trinity College Library you acknowledge that all Intellectual Property Rights in any Works supplied are the sole and exclusive property of the copyright and/or other IPR holder. Specific copyright holders may not be explicitly identified. Use of materials from other sources within a thesis should not be construed as a claim over them.

A non-exclusive, non-transferable licence is hereby granted to those using or reproducing, in whole or in part, the material for valid purposes, providing the copyright owners are acknowledged using the normal conventions. Where specific permission to use material is required, this is identified and such permission must be sought from the copyright holder or agency cited.

Liability statement

By using a Digitised Thesis, I accept that Trinity College Dublin bears no legal responsibility for the accuracy, legality or comprehensiveness of materials contained within the thesis, and that Trinity College Dublin accepts no liability for indirect, consequential, or incidental, damages or losses arising from use of the thesis for whatever reason. Information located in a thesis may be subject to specific use constraints, details of which may not be explicitly described. It is the responsibility of potential and actual users to be aware of such constraints and to abide by them. By making use of material from a digitised thesis, you accept these copyright and disclaimer provisions. Where it is brought to the attention of Trinity College Library that there may be a breach of copyright or other restraint, it is the policy to withdraw or take down access to a thesis while the issue is being resolved.

Access Agreement

By using a Digitised Thesis from Trinity College Library you are bound by the following Terms & Conditions. Please read them carefully.

I have read and I understand the following statement: All material supplied via a Digitised Thesis from Trinity College Library is protected by copyright and other intellectual property rights, and duplication or sale of all or part of any of a thesis is not permitted, except that material may be duplicated by you for your research use or for educational purposes in electronic or print form providing the copyright owners are acknowledged using the normal conventions. You must obtain permission for any other use. Electronic or print copies may not be offered, whether for sale or otherwise to anyone. This copy has been supplied on the understanding that it is copyright material and that no quotation from the thesis may be published without proper acknowledgement.

A Case Study of Action Design Research for Privacy Risk Management Engineering

A Thesis submitted to the University of Dublin in fulfilment of the requirements for the degree of Doctor of Philosophy (Information Systems)

August, 2013

Maria Moloney

Declaration

I, the undersigned, declare that this thesis has not been submitted as an exercise for a degree at this or any other university.

This dissertation is entirely my own work.

I agree to deposit this thesis in the University's open access institutional repository

Or

I agree to allow the library to do so on my behalf, subject to Irish Copyright Legislation and Trinity College Library conditions of use and acknowledgement.

TRINITY COLLEGE
0 9 JUN 2014
LIBRARY DUBLIN

Maria Moloney

28/03/2014

Maria Moloney

Date

Thesis 10410

Acknowledgements

I need to thank my family first and foremost. I'd like to thank Valerio, my husband for all the support and encouragement he has given me, especially in these last 14 months of rework. I know this dissertation would not exist without him.

I need to thank my children, Matthew (8) and Marco (7). I know I have been absent lately but I hope to dedicate myself to being the best mum I can possibly be very soon. Thank you guys for not complaining (much) about the missed weekends and days out, even the missed Christmas. I *will* make it up to you.

I would like to thank my boss, Liam Church. He gave me the creative freedom to seek out my research interests and to find innovative ways of combining them with my work at Escher Group.

I also need to thank my supervisor, Dr Frank Bannister for sticking with me and helping me in every manner possible. I gratefully acknowledge the Irish Research Council for Science, Engineering and Technology who initially funded me. I would also like to thank all participants of the online questionnaire, the semi-structured interviews and the focus groups carried out for this work.

Last but definitely not least, I would like to thank my parents for constantly telling their girls that dreams can come true.

Summary

This dissertation presents a case study concerning the application of the Action Design Research (ADR) methodology to the development of a privacy-enhanced electronic postal system. As part of the ADR project, a model of privacy-related decision making and privacy risk handling behaviour is developed and validated and it is applied to guide the development of the privacy-related features of the electronic postal system.

In doing so, the thesis makes three contributions to the IS literature on online privacy. The first contribution is methodological in that the dissertation describes the application of the recently formulated design science research methodology, namely ADR, in a novel setting, namely new software product development (NSPD) concerning IS for extra-organisational use. The second main contribution is theoretical in nature, in that, by considering heuristic biases and bounded rationality, we redefine the privacy calculus (PC) model, as described in the IS literature, in a manner that more closely fits the decision making process of individuals when dealing with electronic information disclosure in uncertain or ambiguous situations. Finally, the third main contribution is applied in nature in that we provide preliminary privacy design principles to guide the development of privacy risk management systems for electronic postal systems and other IS.

Contents

1 INTRODUCTION AND OVERVIEW 1

1.1 Background to the Research: The RiposteTrEx Project 3
1.2 The Research Project 5
1.2.1 First Stage (Exploratory) 8
1.2.2 Second Stage (Formalized ADR) 9
1.3 Outline of the Dissertation 14
1.4 Conclusions 18

2 INFORMATIONAL PRIVACY LITERATURE REVIEW 19

2.1 Informational Privacy Definitions 19
2.2 Theories of Privacy 21
2.2.1 Sociological Theories of Privacy 22
2.2.2 Privacy Theories Applied to Digital Contexts 26
2.3 Informational Privacy and Privacy Concerns 31
2.3.1 Antecedents to Privacy Concerns 35
2.4 Informational Privacy Control Models and Legislation 42
2.4.1 European Data Protection Legislation 43
2.4.2 Safe Harbor 45
2.4.3 Fair Information Practices (FIPs) 46
2.5 Approaches to Engineering Informational Privacy Protections 48
2.5.1 Privacy by Design (PbD) 49
2.5.2 Privacy Enhancing Technologies (PETs) 53
2.6 Conclusions 62

3 PRIVACY-RELATED DECISION MAKING UNDER UNCERTAINTY 63

3.1 Theories of Decision Making under Uncertainty 64
3.1.1 Rational Decision Making and Expected Utility Theory (EUT) 64
3.1.2 Bounded Rationality 66
3.1.3 The Broader Behavioural Economics Critique of the Rational Paradigm 67
3.1.4 Knightian Uncertainty 70
3.1.5 Risk and Risk Perception 71
3.2 Privacy-Related Decision Making 75
3.2.1 Privacy as a Commodity and the Privacy Calculus 76
3.2.2 The Privacy Calculus (PC) and EUT 85
3.2.3 Behavioural Economics Insights on the PC 87
3.2.3.1 Privacy Risk Taking under Bounded Rationality 90
3.2.3.2 Privacy Risk Taking and Knightian Uncertainty 93
3.2.3.3 Soft Paternalism or Nudging in Informational Privacy Protection 96
3.3 A Synthesis of the Privacy Calculus (PC) Model and Behavioural Economics Insights: the Revised Privacy Calculus (RPC) Model 100
3.3.1 The Hypotheses 109
3.3.2 Privacy as an Absolute and the Revised Privacy Calculus (RPC) Model 112
3.4 Conclusions 113

4 RESEARCH METHODOLOGY 116

4.1 The Research Process under Alternative Epistemologies 116
4.1.1 Positivism in Information Systems Research 119
4.1.2 Interpretivism in Information Systems 122
4.2 Qualitative Research Methods and Methodologies 126
4.2.1 Semi-structured Interviews 126
4.2.2 Focus Groups 128
4.2.3 Hypothetical Scenarios 130
4.2.4 Action Research 131

4.2.5 Case Study *132*
4.2.6 Ethnography *134*
4.2.7 Grounded Theory *135*
4.3 Quantitative Research Methods 136
4.3.1 Survey Research *136*
4.3.2 Experiments *138*
4.3.3 Quasi Experimental Design *140*
4.4 Design Science Approach to Research in IS 141
4.5 The Action Design Research (ADR) Methodology 146
4.5.1 ADR Stage 1: Problem Formulation *151*
4.5.2 ADR Stage 2: The Building, Intervention and Evaluation (BIE) Stage *153*
4.5.3 ADR Stage 3: Reflection and Learning *154*
4.5.4 ADR Stage 4: Learning Formalisation *155*
4.6 The Methodological Framework for This Research: A Mixed Methods Approach 156
4.6.1 Methodological Steps *156*
4.6.2 Qualitative and Quantitative Research Methods Combined *160*
4.6.3 Ethical Considerations in the Project *162*
4.7 Conclusion 163

5 THE SURVEY: THE QUESTIONNAIRE AND SEMI-STRUCTURED INTERVIEWS 165

5.1 The Questionnaire 166
5.1.1 Preliminary Steps: The Pilot Survey and Follow-up interviews *168*
5.1.2 Mapping between Survey Questions and Constructs *170*
5.1.3 The Distribution of the Online Questionnaire *188*
5.1.4 Regression Analysis of Questionnaire Results *191*
5.1.5 Summary of Main Findings from the Questionnaire *205*
5.2 The 20 Semi-structured Interviews 206
5.2.1 The Demographics of the Respondents *207*
5.2.2 Analysis Method *212*
5.2.3 Results *215*
5.2.4 Summary of Findings from the Interviews *233*
5.3 Summary and Implications of Overall Findings of the Survey 235
5.4 Conclusions 237

6 ADR IN NEW SOFTWARE PRODUCT DEVELOPMENT (NSPD) 239

6.1 Choosing ADR for New Software Product Development (NSPD) 239
6.1.1 ADR Stage 1: Problem Formulation *243*
6.1.2 ADR Stage 2: Building, Intervention, and Evaluation (BIE) *245*
6.1.3 ADR Stage 3: Reflection and Learning *248*
6.1.4 ADR Stage 4: Learning Formalisation *248*
6.2 Conclusion 250

7 ENGINEERING AND TESTING THE REVISED PRIVACY CALCULUS (RPC) MODEL 250

7.1 Defining the System Requirements for RiposteTrEx 252
7.1.1 Alignment of the complexity of privacy risk management options to users' rationality *257*
7.1.2 Building users' trust *259*
7.1.3 Increasing (actual and perceived) control *261*
7.1.4 Ambiguity (actual and perceived) reduction *262*
7.1.5 Nudging *263*
7.1.6 Data protection legislation alignment *266*
7.2 Description of the Focus Groups 267
7.3.1 Effectiveness of the RPC Model as a Theoretical Basis for the System *276*
7.3.1.1 Evidence of Cognitive Bias *280*
7.3.1.2 A Hypothetical Scenario *281*

8 CONCLUSIONS, CONTRIBUTIONS AND FUTURE WORK 296

8.1 The Main Results Restated 296
8.1.1 Methodological Contribution: Using the ADR methodology for Engaged Scholarship 297
8.1.2 Contribution to Theory: A Revised Privacy Calculus Model 300
8.1.3 Applied Contribution: Preliminary Privacy Design Principles and Features 301
8.2 Limitations and Future Research 305
8.2.1 Implications of the Methodological Constraints within the Dissertation 311
8.2.2 Future Related Research Projects and Collaborations 315
8.2.3 Related R&D Prospects: Pilots and Applications of RiposteTrEx 317
8.3 Conclusion and Final Remarks 319

9 BIBLIOGRAPHY 321

10 APPENDICES 340

10.1 Appendix A: Informational Privacy Concerns and their Antecedents 340
10.1.1 Perceived Control 340
10.1.2 Online Trust 344
10.1.3 Demographics 351
10.2 Appendix B: Immediate and Mediated Antecedents to Privacy Concerns 353
10.3 Appendix C: Sources for the Questions of the Survey 356
10.3.1 Willingness to disclose 357
10.3.2 Perceived benefit 357
10.3.3 Online Privacy Concern (perceived risk) 358
10.3.4 Online Control preference 360
10.3.5 Awareness of Privacy Practices (Ambiguity aversion) 361
10.3.6 Trust Propensity 361
10.3.7 Risk Handling Behaviour 362
10.4 Appendix D: Instrument for Deriving a Typology of Internet Users and Online Privacy Concerns 364
10.5 Appendix E: The Questions asked of the Participants of the Semi-Structured Interviews 366
10.5.1 Introduction to the interview 366
10.5.2 Interview Questions 366
10.5.3 Concluding the Interview 367
10.6 Appendix F: Paradoxical Answers to the same Question: Online Privacy to me is... 368
10.7 Appendix G: The Research Project's Code of Ethics 371
10.7.1 Research Background 371
10.7.2 Participation in this Research is Voluntary. 371
10.7.3 Duration of the Questionnaire/Interview/Focus Group 372
10.7.4 Debriefing Opportunities 372
10.7.5 Anonymity of Participants and Resulting Data 372
10.7.6 Recording of the Interview/Focus Groups 373
10.8 Appendix H: Privacy Protection Functionalities 374
10.9 Appendix I: Technical Design Principles 380
10.10 Appendix J: Other System Features 386
10.11 Appendix K: Research Papers from this Dissertation 392

List of Tables

TABLE 1.1 EVOLUTION OF THE INFORMATION PRIVACY CONCEPT (SMITH ET AL., 2011) .. 2
TABLE 1.2 THE RIPOSTETREX ADR PROJECT 12
TABLE 2.1 A REVIEW OF EXISTING PRIVACY THEORIES 29
TABLE 2.2 SUMMARY OF SURVEY FINDINGS ON PRIVACY CONCERNS 35
TABLE 2.3 ANTECEDENTS TO INFORMATIONAL PRIVACY CONCERNS 41
TABLE 2.4 PETS CLASSIFICATION, (META GROUP, 2005) 57
TABLE 2.5 PETS FOR PRIVACY PROTECTION (LONDON ECONOMICS, 2010) 58
TABLE 5.1 QUESTIONNAIRE CONSTRUCTS AND ASSOCIATED PROXY VARIABLE 181
TABLE 5.2 SUMMARY STATISTICS 185
TABLE 5.3 CORRELATION MATRIX 186
TABLE 5.4 GLM REGRESSIONS (DEPENDENT VARIABLE: *WILLINGNESS*) 202
TABLE 5.5 GLM REGRESSIONS (DEPENDENT VARIABLE: *RISKHAND*) 203
TABLE 5.6 GLM REGRESSIONS (DEPENDENT VARIABLE: *DRISKHAND*) 204
TABLE 5.7 A BREAKDOWN OF PRIVACY RISK HANDLING BEHAVIOUR AMONG INTERVIEWEES 218
TABLE 5.8 FACTORS INFLUENCING INTERVIEWEES DECISION-MAKING PROCESSES 226
TABLE 5.9 BREAKDOWN OF HEURISTIC BIASES AMONG INTERVIEWEES 235
TABLE 6.1 BREAKDOWN OF ADR METHODOLOGY FOR THE RIPOSTETREX DEVELOPMENT CYCLE 242
TABLE 7.1 MAPPING THE RPC MODEL IMPLICATIONS TO SYSTEM REQUIREMENTS (STAGE 1) 254
TABLE 7.2 FINAL LIST OF QUESTIONS 269
TABLE 7.3 THE DEMOGRAPHICS OF THE FOCUS GROUP PARTICIPANTS 271
TABLE 7.4 THE MAPPING PROCESS FOR HOW THE ORGANISING (PRIVACY) DESIGN PRINCIPLES FOR PRIVACY RISK MANAGEMENT INFORMATION SYSTEMS WERE DERIVED 294
TABLE A1 PERCEIVED CHARACTERISTICS OF TRUSTWORTHINESS 349
TABLE F1 COMPARISON OF QUESTION 1 AND QUESTION 14 FROM THE ONLINE QUESTIONNAIRE 369

List of Figures

FIGURE 1.1 LOGIN PAGE FOR THE RIPOSTETREX SYSTEM 4
FIGURE 1.2 STAGES AND PRINCIPLES OF THE ADR METHODOLOGY (SEIN ET AL, 2011) 7
FIGURE 1.3 TIMELINE FOR THE RIPOSTETREX RESEARCH AND DEVELOPMENT PROJECT 14
FIGURE 2.1 ONLINE PRIVACY CONCERN MULTI-LEVEL FRAMEWORK (BÈLANGER AND CROSSLER, 2011) 32
FIGURE 3.1 PARADIGMS IN RISK PERCEPTION RESEARCH (ADAPTED FROM RENN (2005), TAYLOR-GOOBY & ZINN (2006) AND LUPTON (1999). 75
FIGURE 3.2 THE PRIVACY CALCULUS MODEL (PC) 82
FIGURE 3.3 THE PC MODEL UNDER EUT-RATIONAL DECISION MAKING 87
FIGURE 3.4 THE REVISED PRIVACY CALCULUS (RPC) MODEL 108
FIGURE 4.1 CIRCUMSTANCES FOR A QUESTION IS TO BE VALID AND RELIABLE (FRODDY, 1994) 137
FIGURE 4.2 THE COMPLEMENTARY NATURE OF DESIGN SCIENCE AND BEHAVIOURAL SCIENCE RESEARCH (HEVNER AND CHATTERJEE, 2010) 144
FIGURE 4.3 ENGAGED SCHOLARSHIP FOR PROBLEM SOLVING (VAN DE VEN, 2007) 150
FIGURE 5.1 WILLINGNESS TO DISCLOSE PERSONAL INFORMATION 172
FIGURE 5.2 PRIVACY RISK HANDLING BEHAVIOUR 175
FIGURE 5.3 PROPENSITY TO TRUST 178
FIGURE 5.4 THE SPREAD OF AGE GROUPS THAT PARTICIPATED IN THE ONLINE PRIVACY QUESTIONNAIRE 190
FIGURE 5.5 BREAKDOWN OF AGES FOR THE SEMI-STRUCTURED INTERVIEWS 208
FIGURE 5.6 A BREAKDOWN OF INTERVIEWEES ACCORDING TO SHEEHAN'S (2002) PRIVACY CLASSIFICATION 209
FIGURE 5.7 A BREAKDOWN OF INTERVIEWEES WHO HAVE EXPERIENCED A PRIVACY BREACH IN THE PAST 210
FIGURE 5.8 A BREAKDOWN OF INTERVIEWEES ACCORDING TO AGE AND PRIVACY RISK PERCEPTION 211
FIGURE 5.9 THE CONSTANT COMPARATIVE METHOD 214
FIGURE 6.1 TIMELINE FOR THE RIPOSTETREX ADR PROJECT 249
FIGURE 7.1 THE MAPPING OF GENERAL SYSTEM REQUIREMENTS ONTO SYSTEM FEATURES, FUNCTIONALITIES AND TECHNICAL DESIGN PRINCIPLES (STAGE 2) 257
FIGURE 7.2 INFORMATIONAL PRIVACY SETTING WINDOW FOR RIPOSTETREX 259
FIGURE 7.3 PRIVACY POLICY OF RIPOSTETREX 266
FIGURE 7.4 COOKIE POLICY POP-UP FOR RIPOSTETREX 266
FIGURE 7.5 RESPONSES TO THE QUESTION: DOES THIS SYSTEM HELP REDUCE THE RISK OF YOUR PERSONAL INFORMATION BEING COMPROMISED OR ABUSED? 277
FIGURE 7.6 EFFECTIVENESS OF IMPLEMENTATION OF SYSTEM REQUIREMENTS (AMBIGUITY REDUCTION AND DATA PROTECTION LEGISLATION ALIGNMENT SCORING LOWEST) 284
FIGURE 8.1 RUGGEDISED IPADS LOCATED IN 3 LOCAL LIBRARIES AND IN A LOCAL MOSQUE 318
FIGURE J.1 "OPT-IN" TO MARKETING FROM COMPANIES WITHIN THE RIPOSTETREX NETWORK 388
FIGURE J.2 A SHORT SURVEY ON EMPLOYMENT ISSUES IN THE LONDON BOROUGH OF TOWER HAMLETS 389

Abbreviations

ADR	Action design research
AR	Action research
BIE	Building, intervention and evaluation
DSR	Design science research
EUT	Expected utility theory
FIPs	Fair information practices
ICT	Information communication technology
IS	Information systems
NPO	National postal operator
NSPD	New software product development
PC	Privacy calculus
PbD	Privacy by design
PETs	Privacy enhancing technologies
RPC	Revised privacy calculus

1 Introduction and Overview

Today, in the 21st century, Information Systems (IS) surround us. They can be found in our cars, our phones and even in the clothes we wear. Information drives these new technologies. Meglena Kuneva, the European Consumer Commissioner, said in 2009 that personal information was the new oil of the Internet and the new currency of the digital world (Kuneva, 2009). Challenges exist, however, and a central one in the information age is the extent to which an individuals' personal information is protected from unauthorised use. Indeed, informational privacy protection has become a sensitive topic in many areas of 21st century life (Whitley, 2009). Concern among users of information technologies regarding the protection of their personal information is considerable (Dinev, Hart and Mullen, 2008; Federal Trade Commission, 2010; Privacy Rights Clearinghouse, 2005; Tsai et al., 2011). Substantial efforts, especially in recent years, have been made by a number of governments to address these concerns. Westin (2003) describes a four stage progression that any contentious social innovation goes through before it is transformed and adapted to a degree that is acceptable to mainstream society:

- Early alarms;
- Empirical studies;
- Alternative policy formulations;
- First-generation legal and organizational actions.

Smith et al. (2011) reconsider Westin's four stage progression and claim that the recent evolution of the concept of privacy in general, and informational privacy in particular, follows the evolution of information technology itself. Table 1.1 outlines this evolution.

Table 1.1 Evolution of the Information Privacy Concept (Smith et al., 2011)

Period	Characteristics
Privacy Baseline 1945-1960	Limited information technology developments, high public trust in government and business sector, and general comfort with the information collection.
First Era of Contemporary Privacy Concept Development 1961-1979	Rise of information privacy as an explicit social, political, and legal issue. Early recognition of potential dark sides to the new technologies (Brenton 1964), formulation of the Fair Information Practices (FIPs) Framework and establishment of government regulatory mechanisms such as the Privacy Act of 1974.
Second Era of Privacy Concept Development 1980-1989	Rise of computer and network systems, database capabilities, federal legislation designed to channel the new technologies into FIP, including the Privacy Protection Act of 1984. European nations move to national data protection laws for both the private and public sectors.
Third Era of Privacy Concept Development 1990-present	Rise of the Internet, Web 2.0 and the terrorist attack of 9/11/2001 dramatically changed the landscape of information exchange. Reported privacy concerns rose to new highs.

Regardless of its evolution in the twentieth century, the concept of privacy is not new. Provisions broadly concerning privacy have been codified even since before the birth of common law in the twelfth century (Holt, 1973). Initially, the provisions of the law on privacy simply covered physical interference with life or property (Warren and Brandeis, 1890). Over the centuries, the law started to cover not only the right to life but also the right to enjoy life. Accordingly, the right to privacy began to be viewed as encompassing "the right to be let alone" (Warren and Brandeis, 1890) and to exercise extensive civil privileges. Concurrently, the right to private property grew to encompass not only tangible assets, but also intangible assets such as intellectual property rights (Warren and Brandeis, 1890).

There is also evidence throughout history that the notion of privacy existed long before contemporary legal and philosophical conceptualisations of the last few centuries. The dichotomy between the public and private realm dates back to the time of Aristotle. Aristotle saw the polis, the Greek term for city-state, as a public sphere where politics were developed. The polis was strictly separate from the sphere of the oikos which was the private sphere where each individual was in his own dominion (Decew, 1997). Likewise, the Romans saw privacy as an essential element of humanity. They saw the private space of hearth and home as a place where the individual felt sheltered from the world. They even went as far as to declare that to have no private place of one's own was to be no longer human (Arendt, 1998). Locke notes this same separation of public and private in his Second Treatise on Civil Government (Locke, 2007). According to Locke, the original state of nature is a state of perfect freedom, "we must consider, what state all men are naturally in, and that is, a state of perfect freedom to order their actions, and dispose of their possessions and persons, as they think fit, within the bounds of the law of nature, without asking leave, or depending upon the will of any other man." (Locke, 1690, Chapter 2, Section 4). According to Locke everyone has property rights to his own person and can extend these rights through sweat and labour. Therefore, what belongs to and is acquired by the self is private property and is distinctly separate from what is owned publicly.

1.1 Background to the Research: The RiposteTrEx Project

The research undertaken for this dissertation has its origins, to a considerable extent, in an investigation carried out to understand how to engineer informational privacy risk

management functionality into an electronic postal system that is being developed by a company called Escher Group (IRL) Ltd. for An Post, the Irish National Postal Operator (NPO). The electronic postal system under development is currently called RiposteTrEx, although this may change once it is sold to An Post. The RiposteTrEx system was built using the infrastructure of a product entitled Riposte. The Riposte product has been used in post offices for over twenty years in the electronic transfer of funds across the globe (Escher Group, 2013). The Riposte system is currently in use in 34 NPOs globally, including the United States Postal Service (USPS). The new RiposteTrEx system leverages this infrastructure with the aim to support the transfer of personal information through trusted exchanges (whence, the "TrEx" element of the name) over the secure Riposte network (Escher Group, 2013). It is being developed for the Irish NPO to provide private electronic messaging and to facilitate the private electronic transfer and storage of (sensitive) personal information. Figure 1.1 shows the log-in page for RiposteTrEx.

Figure 1.1 Login Page for the RiposteTrEx system

1.2 The Research Project

The research underlying this dissertation was integrated with the development process of RiposteTrEx (henceforth, the product), a commercial software product, which made available a unique setting and resources for conducting the investigation that would not have been otherwise available. The study was conducted on the premises of Escher Group's headquarters on St Stephen's Green in Dublin. During this time, the Author (i.e., the author of this thesis) was head of research at Escher Group and, as such, she was embedded in the company throughout almost the entire development lifecycle of the first release of the product. She joined the company at the early stages of the product development lifecycle, i.e. during the product conceptualisation stage (which involved close collaborative interaction between Escher Group and An Post), and from the outset one of her key tasks was to bring to the product development project insight from research on privacy.

Integral to the product development for RiposteTrEx are two interrelated research questions, which are also at the heart of this dissertation: how do individuals make informational privacy-related decisions and how can such knowledge be used in the design and engineering of privacy-management systems? In turn, these two questions can be broken down further as follows:

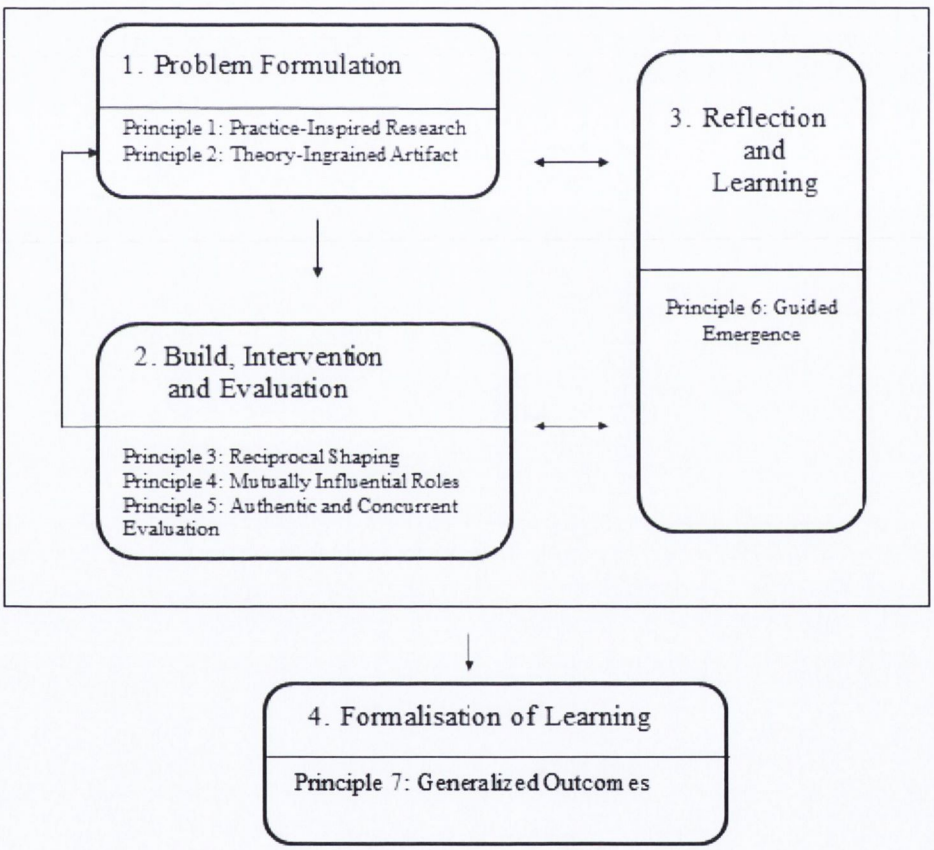
- How does uncertainty over the outcome of online interactions influence an individual's decision to disclose his/her personal information online? How is on-line behavior influenced by perceived uncertainty and what are the strategies (risk handling behavior) deployed by individuals in the presence of such uncertainty? Does the possibility or otherwise of deploying risk-handling

strategies influence an individual's decision to disclose his/her personal information online?

- Since disciplines such as economics and, more recently, branches of the IS literature (e.g., Acquisti (2004)) distinguish between quantifiable and unquantifiable uncertainty, depending on the nature of the risks involved, is there evidence that an individual's decisions to disclose his/her personal information online in the presence of the former are qualitatively or quantitatively different from such decisions that occur in the presence of the latter type of uncertainty (also known as "ambiguity", Acquisti (2004))?
- Is there evidence of cognitive error and/or bias in the assessment of privacy risk and, if so, how does this affect the "privacy calculus" (Chellappa and Sin, 2005; Culnan, 1993; Dinev et al., 2006; Hann, Hui and Lee, 2008; Hui, Teo and Lee, 2007; Milne and Gordon, 1993; Milne and Rohm, 2000; Xu et al., 2009) performed by individuals in their decision-making processes?
- Are there circumstances that exacerbate or mitigate the impact of cognitive error and bias and to what extent are such circumstances under the control of either providers of ICTs or public agencies/regulators?
- Is there a way of usefully mapping the implications of a privacy-related decision making model, such as one describing the "privacy calculus" in a way that takes possible cognitive error and biases into account, onto the specifications of a software product design, given a set of product requirements deemed desirable?
- If this is possible, can the implications of such a privacy-related decision making model be mapped into a set of principles which may guide the design of entire classes of artifacts characterized by specific product requirements?

We[1] sought to answer these questions by conducting an Action Design Research (ADR) project, adapting to a new software development setting a methodology which was recently proposed by Sein et al (2011) in the context of organizational IS development. Figure 1.2 shows the different stages and principles involved in the ADR methodology, which will be discussed at length in chapter 2 and then revised, to better adapt the methodology to the needs of this research, in chapter 6.

Figure 1.2 Stages and principles of the ADR methodology (Sein et al, 2011)



Initially, the methodology we used in the project to answer the research questions was a mixture of Action Research (AR) and Design Science Research (DSR). In the

[1] This dissertation uses the first person plural to explain the research undertaken by the author. When the first persona plural is used for any other reason than this it is specifically outlined in the text.

meantime, we became aware of the seminal article on Action Design Research (ADR) that had just been published by Sein et al (2011). Due to the project already relying heavily on the DSR and AR methodologies, ADR was seen as a natural progression and therefore, after the first year of the project, it was decided to follow this methodology as a more systematic alternative to the informal and somewhat ad-hoc combination of DSR and AR that we had followed until then. In our research, as shall become clearer later, ADR came to play the role of an overarching methodological framework, effectively a sort of meta-methodology, within which, at different stages, we used methods prescribed by other methodologies, i.e. regression analysis of survey results, semi-structured interviews and focus groups, to carry out the learning required by the ADR methodology. In retrospect, we may divide the ADR project underlying this dissertation in two stages, i.e. an exploratory one and a more formalized one.

1.2.1 First Stage (Exploratory)

During the first stage, i.e. the exploratory one, we had not fully conceptualized the project as ADR. In fact, while the Author was using her research to offer insight on the design of privacy-related features of the product and was using experience gained through her involvement in the product development to reflect on issues directly related to her research, neither she nor the product development team at Escher Group had realized the Author's research and the development project were becoming intertwined so as to merge into a learning endeavour that could be naturally and more effectively conceptualized, to the mutual benefit of the Author's research and the company development project, first as AR and subsequently as an ADR project.

During this stage, we sought to investigate, as part of both the Author's doctoral research and of the product development efforts, individuals' privacy concerns and how individuals make informational privacy decisions when faced with the option of submitting their personal information *electronically*. This was done by undertaking a review of the literature on privacy, through a questionnaire and semi-structured interviews and by engaging with stakeholders of the project, mainly the management of An Post, public bodies involved in the regulation of NPOs and the management of Escher Group. Since this early stage of the research, our focus has been on the privacy-related issues that arise specifically in the context of *electronic* submission of personal information, because of a concern that individuals are faced with uncertain and ambiguous situations when submitting their information in this way, essentially due to the fact that, typically more so than in off-line settings, they do not have access to the full set of information regarding how their personal data will be handled once they submit it electronically (Varian, 1997).

1.2.2 Second Stage (Formalized ADR)

The onset of the second stage of the research, to which we referred to above as the more formalized one, occurred six months before the submission of the first version of this dissertation and was accelerated by the reflection triggered by the feedback obtained during and after the Viva Voce examination. We conceptualized the project first as an instance of AR and subsequently, after realizing that the engineering of the product could be formalized as an instance of DSR and after coming across Sein et al (2011) seminal article on ADR, as an instance of the latter. During this stage, with a view to focusing on IS users' decisions concerning online interaction in the face of privacy risk

and determinants of risk handling behaviour, we examined the privacy calculus (henceforth, PC) model (Klopfer and Rubenstein, 1977; Laufer and Wolfe, 1977; Dinev et al., 2006) and extended it to account for the possible influence of heuristic driven cognitive biases, along the lines of the seminal work of Kahneman and Tversky (1979), and ambiguity (Acquisti and Grossklags (2004)), leading to a *revised privacy calculus* (henceforth, RPC) model. We first tested this model using regression analysis of the survey data gathered during the first stage and semi-structured interviews conducted with a sub-sample of survey participants.

We then used the model to guide the engineering of the RiposteTrEx system. In order to achieve this, we examined existing design science literature surrounding privacy-enhancing technologies (Burkert, 1997; Agre and Rotenberg, 1997; Levy, 2001; Brunt, 2006; London Economics, 2010), software engineering and the Privacy by Design (PbD) principles (Cavoukian, 1998; Cavoukian, 2006; Kuner, 2007; Gurses, Rizk and Gunther, 2010; Gurses, Troncoso and Diaz, 2011; Van Lieshout et al., 2011). The RiposteTrEx system was then subject to tests (via focus groups[2]) to assess the extent of user satisfaction with and, more generally, user reaction to its features. The results of these tests are then used to make inferences on the privacy design principles that guided the development of the privacy management information system and therefore, indirectly, to test our RPC model (which is used to guide the derivation of the design principles in the first place). The direct input of research-driven theorizing into the product and the testing of the theory permitted by the users' feedback constitute, from

[2] Two sets of eight focus groups were conducted during the RiposteTrEx project, the first in Jan-March 2011, during the exploratory stage of the project, and the second set a year and a half later in August and September 2012. The second set of eight focus groups are analysed in this thesis as they are the set that tests for evidence of ambiguity aversion and heuristic bias among the participants.

an epistemological point of view, the essential ingredients that establish this research as one of the first applications of the ADR methodology and, to our knowledge, the very first one in the context of new software product development (NSPD). Table 1.2 shows how the RiposteTrEx project followed the structure of an ADR project.

The first and second columns of the table outline the stages of the RiposteTrEx project and the methods that were employed during each stage of the project. The third column outlines the various stages and principles of the ADR methodology as outlined by Sein et al (2011).

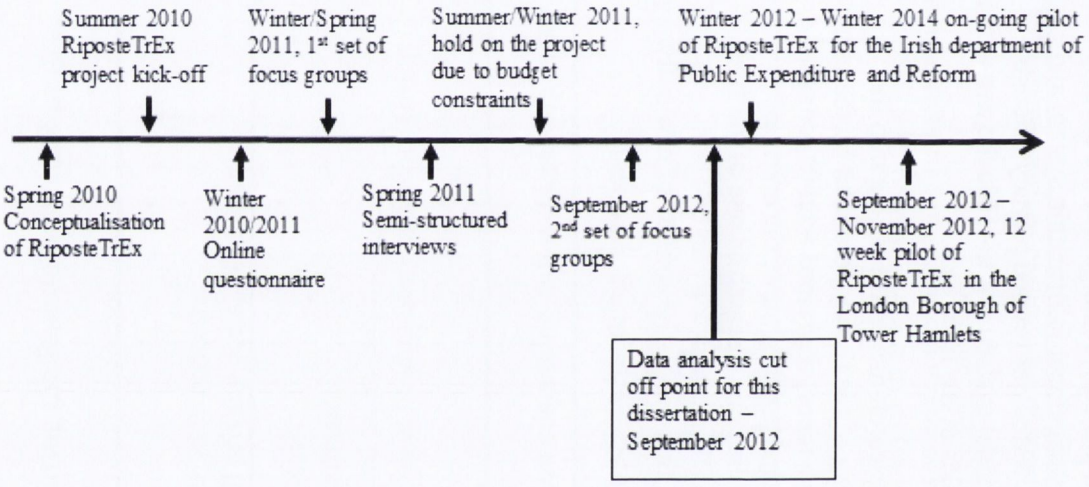
Table 1.2 The RiposteTrEx ADR Project

Stages of the RiposteTrEx ADR project	Work conducted during the RiposteTrEx ADR project	ADR Method: stages and principles (Sein et. al, 2011)
Stage 1, the exploratory stage of the research project	Investigated: 1. Individuals privacy concerns; 2. Informational privacy decision making.	1. Problem formulation Principle 1: practice inspired research; Principle 2: theory ingrained practice.
Stage 1, methods used The result of the first stage of the first stage of the project is a revised privacy calculus model.	1. Literature review; 2. Online questionnaire; 3. Semi-structured interviews; 4. Action research at headquarters of Escher Group (IRL) Ltd.	3. Reflection and learning (stage 1) Principle 6: guided emergence of the RPC model
Stage 2, the formal stage of the ADR research project	Investigated: 1. Users' decision concerning online interaction in the face of privacy risk; 2. Determinants of risk handling behaviour; 3. Privacy calculus (pc) model; 4. Design science research; 5. Software engineering methods. 6. Privacy by design principles.	2. Building, intervention and evaluation Principle 3: reciprocal shaping of the RPC model and the artefact Principle 4: mutually influential roles Principle 5: authentic and concurrent evaluation 3. Reflection and learning (stage 2) Principle 6: guided emergence 4. Formalisation of learning Principle 7: generalized outcomes
Stage 2, methods used	1. Literature review; 2. Regression analysis; 3. Qualitative analysis of semi-structured interviews; 4. Focus groups to assess the extent of user satisfaction with the RiposteTrEx product.	
Outcome of the project	The analysis of the focus groups is used to make inferences	

The ADR methodology guides the emergence of both the product and the theory. The result of the second stage of the project is a set of design principles for privacy risk management information systems.	on the privacy design principles that guided the development of the privacy risk management information system and therefore, indirectly, tested our revised privacy calculus (RPC) model. The model is also used to guide the derivation of the design principles in the first place. The direct input of research-driven theorizing into the product and the testing of the theory permitted by the users' feedback (producing a theory ingrained artefact) constitute, from an epistemological point of view, the essential ingredients that establish this research as one of the first applications of the ADR methodology and, to our knowledge, the very first one in the context of new software product development (NSPD).

The timeline for the RiposteTrEx project spans three years. Figure 1.3 shows the timeline of the RiposteTrEx project. Due to time and space constraints, not all work outlined in the timeline below is examined in this thesis. The cut-off point for analysis of work included in this thesis was September of 2012. This thesis includes analysis of only the second set of focus groups for the RiposteTrEx project which were carried out in August and September of 2012, which tested the effectiveness of the privacy design principles derived for RiposteTrEx and thus indirectly tested the validity of the RPC Model. The first set of focus groups were conducted in 2011.

Figure 1.3 Timeline for the RiposteTrEx research and development project



1.3 Outline of the Dissertation

In this section we offer a succinct overview of the structure of this dissertation.

In chapter 1, we provide some background to the dissertation and outline the motivations for undertaking the research. We describe the new software product development project (NSDP) within which the research itself was embedded. In chapter

2, a review of the informational privacy literature is provided. As part of this literature review, we look at existing definitions of informational privacy and, in order to provide a better understanding of the research that has already been conducted in this field and to provide further motivation for the research that underpins this dissertation, we review theories on privacy from the IS, with special emphasis on the so called PC model, and the sociology literatures. In chapter 2, we also examine the current trends in informational privacy engineering. We focus, in particular, on the societal and policy landscape surrounding the issue of informational privacy protection, i.e. the software engineering, political and legal landscapes. We examine the data protection laws and the privacy by design methodology, which was designed to guide developers and designers of privacy enhancing technologies in how to implement legal and political informational privacy requirements into technology. We continue, in chapter 3, with a review of the literature, conceptualizing privacy-related decision making as an instance of decision making under uncertainty and focussing on insight from both neoclassical economics, with its emphasis on rational decision making, and behavioural economics, which allows for biased decision making and less than fully rational behaviour, and eventually we seek to offer a synthesis of the PC model, developed within the IS literature, and insight from behavioural economics.

Chapter 4 consists of a review of the main research philosophies and methodologies in the Information Systems domain as well as relevant qualitative and quantitative research methods. A particular emphasis is placed on action research, semi-structured interviews, focus groups and the survey method because they are the methods used in the dissertation. This is followed by a review of Design Science Research (DSR) and of the recently developed ADR approach.

At the end of chapter 4, an overview of the methodological framework for this research, i.e., a mixed methods approach is provided. It outlines how in this research project the ADR methodology plays the role of an overarching methodological framework, effectively a sort of meta-methodology, within which, at different stages, we use methods prescribed by other methodologies, i.e. a questionnaire, semi-structured interviews and focus groups, to carry out the learning required by the ADR approach. From within the overarching framework in which the ADR methodology plays the organizing role, this research employs a combination of both qualitative and quantitative research methods. We outline and motivate the steps of such a multi-method approach, with a greater emphasis on those which occurred during the more advanced stage of the project, i.e. the 'Formalized ADR' stage.

Chapter 5 describes the gathering of data through an online questionnaire and semi-structured interviews, as well as the analysis of the data. The latter includes parametric tests of the hypothesis of the RPC model based on estimates of implications of the model itself obtained within a multiple linear regression framework, specified as a generalized linear model (GLM), as well as an analysis and discussion of the semi-structured interviews. The findings generally support the hypotheses put forth in chapter 3.

In chapter 6, we look in more detail at the ADR methodology and its novel application to a new environment, i.e. new software product development (NSPD). In this chapter, in describing how this recent design methodology was applied to the environment in

question, we outline the challenges that were faced by the NSPD team in applying the ADR methodology to the NSPD project.

Chapter 6 is placed strategically between the chapters that analyse the online questionnaire and the semi-structured interviews and the engineering and testing of the RPC Model. This was done to emphasise the two stage approach, i.e. the exploratory stage and the formalised stage, which was undertaken for this research.

In chapter 7, we use the RPC Model to offer guidance to the engineering of privacy risk management functionalities into RiposteTrEx and similar information systems. To do so, we first derive requirements for such systems. We then report on eight focus groups that were conducted before the first pilot of the product went live, in September 2012, to ascertain users' satisfaction with the system requirements and how effectively they have been implemented in the product. The results of the focus groups were mixed, offering some degree of empirical validation to the RPC model but warranting further research to further understand the basis of privacy-related decision making and (self-reported) privacy risk handling behaviour.

Finally, chapter 8 concludes and discusses the contributions and limitations of the research undertaken in this dissertation. It also outlines the future work to be conducted for the on-going RiposteTrEx project.

1.4 Conclusions

In this chapter, we introduced the concept of informational privacy and briefly outlined the background to the concept. This was done in order to explain the importance of privacy not just throughout history but also in modern day life. We then went on to outline the motivations for conducting the research project as well as its methodological framework and the methodological steps undertaken as part of the study. Such steps will be described and discussed in detail in later chapters. We delineated the research questions tackled by this research, namely what are the variables that play a role in the decision to interact online in the presence of privacy risk, how they influence privacy risk handling behaviour and how such knowledge can be used as a guide when engineering and developing a privacy-enhanced information system. We also gave a brief outline of the project at the centre of this research, i.e. the new software product development project for a software system entitled RiposteTrEx. Finally, we outlined what is to come in the rest of the dissertation by outlining the overall structure of the dissertation and briefly discussing the content of each chapter.

2 Informational Privacy Literature Review

This chapter examines the concept of informational privacy from different perspectives. We first present and discuss a number of existing privacy theories, prevalently drawn from the Information Systems literature and the legal and sociology literature. We then examine several surveys on informational privacy concerns of IS and ICT users. In the final part of the chapter, we review legislation and policies on informational privacy protection and examine trends in informational privacy engineering, with special emphasis on the privacy by design methodology, which was conceived to guide developers and designers of information systems in implementing legal and political informational privacy requirements into technology. The chapter concludes with an examination of how existing privacy enhancing technologies are contributing to informational privacy management within organizations.

2.1 Informational Privacy Definitions

Informational privacy is a specialized and situation-specific version of the general concept of privacy. Like the latter, informational privacy is defined in various ways across different disciplines. Agre and Rotenberg (1997) point out that the only constant in the evolution of the concept of privacy is the difficult task of defining it. Stone et al. (1983) refer to informational privacy as control over how one's personal information is acquired. Along similar lines, Pavlov (2011) defines it as the ability to maintain control over one's personal information. According to Whitley (2009), however, privacy has

come to be seen as having no inherent definition, rather different social groups and disciplines have developed different meanings and interpretations of the concept. It has been lamented that this difficulty in pinning down the concept of privacy, combined with the lack of transparency of some current methods for transferring personal data, give the topic of informational privacy protection a nebulous character (Gurses, Troncoso and Diaz, 2011). The diversity of interpretations of the meaning of privacy reflects its complexity and subjectivity. Most people have opinions regarding the meaning of privacy as it is a subjective notion and affects everyone differently. One such subjective definition of informational privacy is "*the seclusion and freedom from unauthorized intrusion*" (Dhillon and Moores, 2001: 2). The key word in this definition, according to Dhillon and Moores, is 'unauthorized'. They believe that although individuals may not like the fact that information regarding their purchases and habits are monitored and stored in databases around the world, they are at least usually aware that it is happening. They argue that an unauthorized intrusion to collect personal data marks the beginning of privacy infringement. Westin (2003) defines informational privacy more broadly as:

> *"the claim of an individual to determine what information about himself or herself should be known to others...This also involves when such information will be obtained and what uses will be made of it by others" (Westin, 2003, p431).*

DeCew (1997) sees Internet privacy within the U.S. as an area of the privacy domain that is addressed by tort law and the Fourth Amendment to the United States constitution. These laws help to control access to information about an individual and ensure personal information is not available for public perusal. Individuals have the

right to expect that Information provided to others for explicit and agreed purposes (e.g. financial, medical, educational) should not be passed on to third parties without the permission of the person to whom the data refers. Bennett (2008) sees privacy as an elusive and multidimensional concept whose meaning is culturally and historically contingent. He argues that it is the concept that tends to define policy issues in advanced industrial societies, and it is still the concept around which challenges to excessive surveillance gets framed. He goes on to define privacy as "*the extent to which individuals have control over the circulation of their personal information*" (Bennet, 2008, p xi). This parallels developments in the IS discipline that show a growing recognition that an individual's understanding of what constitutes the modern concept of privacy includes having control over their personal data (Whitley, 2009; Introna, 1997; Van Dyke, Midha and Nemati, 2007). Whitley (2009) goes a step further and argues that "*the understanding of...control that frequently emerges is an impoverished version based on earlier understandings of technology*" (p.3). He argues that the notions of consent and the revocation of given consent form the basis for a new understanding of "*user-centric*" control of personal data. This perspective of user centric control of personal data is also prevalent in the literature of the European Union's Internet strategy for the next decade (European Commission, 2010). As a result, a number of EU funded projects are looking into the idea of giving control of personal information to the users that create that information (ABC4Trust Project, 2009; PICOS, 2007; Primelife, 2008).

2.2 Theories of Privacy

In this section, we illustrate theories of privacy drawn from sociology, or at least that rely heavily on concepts and constructs developed in the sociological literature, and we

subsequently discuss the influence of these theories on the IS literature and how IS researchers' of online privacy have interpreted these theories for online privacy-related decisions and behaviour, including the decision to engage in possibly risky interactions in digital contexts, e.g. online or in other ICT-mediated interactions.

2.2.1 Sociological Theories of Privacy

Westin (1970) describes ways in which people protect their privacy by temporarily limiting access to themselves by others. In his view, privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about themselves is communicated to others. When viewing privacy in relation to individuals and their social interactions, he sees it as the voluntary and temporary withdrawal of a person from the society through physical or psychological means, either via a state of solitude or small group intimacy or, when among large groups, in a condition of anonymity or reserve. Westin believes we need privacy, among other things, to help us adjust emotionally to everyday life. He claims that his theory of privacy is applicable to western democracies because it is consistent with the socio-political values widely held in such societies. For Westin, privacy is a means of achieving the overall end of self-realisation (Margulis, 2003).

Another influential sociologist is Irwin Altman. Altman defined privacy as "*the selective control of access to the self*" (Altman, 1975). He sees selective control as intrinsic to privacy because people try to control their openness or reserve to others by being open and available to others sometimes and at other times being closed and

unavailable (Altman and Chemers, 1980). In Altman's work, the crucial idea is that privacy provides a bridge between personal space, territory and other realms of social behaviour. He describes privacy as "*an interpersonal boundary regulation process by which a person or group regulates interaction with others*" (Altman and Chemers, 1980, P75). Privacy, according to Altman, allows people to be open or closed to interaction with other people depending on the situation, which implies that privacy is a changing process whereby people continuously attempt to regulate their interaction with others (Altman and Chemers, 1980). Personal space, territory, verbal and nonverbal responses and cultural practices operate as behavioural mechanisms to facilitate privacy regulation. People establish a desired level of privacy in their minds and then set in motion a series of behavioural mechanisms to implement their momentary desired level of interaction. Sometimes these behaviours work as expected and the outcome or achieved privacy is equal to the desired privacy. Other times, the achieved privacy is less (crowded) or more (isolated) than the desired privacy.

Laufer and Wolfe (1977) present a socio-psychological theory of privacy. They point out that there is an historic dialectic between the views of privacy from the standpoint of the state and from the standpoint of the individual. The individualistic tradition, in their view, is based on Greek, protestant and common-law views, while the Roman Catholic tradition emphasises the priority of the state's right of intrusion upon a group or individual for the common good. Laufer and Wolfe argue that the same dialectic is evident not only in the political-legal history of privacy but also in the behavioural science literature of privacy. Some social scientists approach the privacy issue from a perspective of individual experience, while others are primarily concerned with the

social and cultural rules of privacy and privacy invasion. In their analysis, the subjective and normative aspects of privacy are interdependent. According to Laufer and Wolfe (1977), time provides the dynamic basis for this interdependence. The individual experiences time as growing or aging, while within the socio-cultural system, time is manifest as historical and technological development. They, therefore, present a developmental theory of privacy that relates the individual's understanding, and experience of privacy and invasion of privacy in relation to his/her growth and life within a particular socio-historical environment. Laufer and Wolfe describe the elements of any given situation (environmental, interpersonal and self-ego) that must be taken into account to understand the individual's perception and experience of privacy and invasion of privacy. Laufer and Wolfe (1977) also discuss the issue of control/choice, which they believe is relevant to any conceptualisation of privacy. The general experience of control/choice has played a decisive role in the development of autonomy in western societies. We describe this development of autonomy as the single most important expression of the evolution of a sense of self. In turn, the control/choice an individual believes he/she has and actually does have in a given situation is a function of the contemporary cultural and historical interpretation of personal dignity (Laufer and Wolfe, 1977).

In contrast, Moor (1997) discusses privacy in the context of moral human values. He explains the difference between instrumental values, intrinsic values and core values. Instrumental values are values which are good because they lead to something good. Intrinsic values are values which are good in themselves and core values are values that are shared and fundamental to human evaluation. Core values are found in all human

cultures. Moor agrees with the notion that privacy has instrumental value. Privacy offers us protection against harm. For example, in some cases if a person's medical condition were publicly known, then that person may, depending on their medical condition, be at risk of discrimination in, for example, purchasing health insurance. Privacy in this case protects the individual from such discrimination. However, he also argues that privacy has intrinsic value because it is an expression of the security value which is a core value. "*Without protection species and cultures do not survive and flourish. As societies become larger, highly interactive, but less intimate, privacy becomes a natural expression of the need for security. We seek protection from strangers who may have goals antithetical to our own. In particular, in a large, highly computerized culture in which lots of personal information is greased it is almost inevitable that privacy will emerge as an expression of the core value, security*" (Moor, 1997, P29).

An advocate of Moor's views on privacy is Taviani (2007). He divides existing privacy theories into four categories, non-intrusion such as the theory put forth by Samuel Warren and Louis Brandeis (1890), seclusion which was advocated by Gavison (1980) and Westin (1970), control as expounded by Fried (1990), Miller (1971) and Rachels (1975) and limitation which can be found in the writings of Parent (1983). He finds all of these theories wanting. He argues that privacy has evolved from a notion of seclusion put forth initially by theorists such as Westin and Altman to a notion of controlling the flow of personal information. As a result of this, modern privacy theorists tend to analyse the notion of privacy in terms of controlling this flow of personal information and have coined the phrase "informational privacy" to express this new concept. Taviani argues that limiting privacy to the control of personal information again

restricts privacy to a specific area of an individual's life and ignores other important aspects (Tavani, 2007). Zhao (2006) argues that individuals exert their right to privacy while interacting with others online in a similar way as they do offline. They may be willing to be intimate with close friends or acquaintances or remain reserved while interacting with strangers online. Non-social or solitary activities such as web surfing and news reading, do not involve direct contact with others and allow individuals to be separated from the group in a state of solitude or anonymity (Zhao, 2006).

2.2.2 Privacy Theories Applied to Digital Contexts

Similar to Westin's view, Fried (1968) sees privacy not simply as an absence of information about a person in the minds of others, but rather as the control that a person has over information about themselves. Informational privacy concerns can, according to Floridi (2005), be reduced or increased according to how people develop the "infosphere" or digital world. ICTs can change the nature of the digital world or "infosphere" and either reduce or increase informational privacy concerns as a result. Floridi calls this ability to change the nature of ICTs, a re-ontologisation of ICTs. He argues that ICTs can alter the very nature of informational privacy and as a result our understanding of informational privacy.

Additionally, Floridi (2005) sees personal information as the digital representation of the "self" in the digital world. Thus, he argues, a breach of one's personal information is a form of aggression towards the person and their digital identity. He calls for what he understands as "*a radical change in the nature of ICT*" or a redrawing rather than an

erasing of the boundaries of informational privacy. According to Floridi, digital ICTs exacerbate old problems concerning informational privacy because of the dramatic increase in their data processing capacities, in the pace at which they can process data, and in the quantity and quality of data that they can collect record and manage.

Somewhat similar to Floridi's view, Rule (2007) believes that blaming technology or other non-human agencies for the pressure that is currently being placed on informational privacy is futile. Technologies that are being used for privacy-eroding activities could just as well support privacy-friendly practices. In fact, he argues that the technological problems of protecting personal information is easy compared to counteracting the sophisticated measures devoted to creating, collecting, transmitting, and using personal information that is being driven by the need to get value from personal information for commercial gain. He argues that mass surveillance and concomitant pressures on privacy are driven by a mass desire for efficient processing of personal information. Nearly all systems of mass surveillance can rely on significant support from the public however anxious individuals may be concerned about demands made on their own personal information. Rule argues that privacy-eroding activities could just as well support privacy-friendly practices, if only those in charge approved, i.e. those in charge of the technologies that gather personal information. However, he believes that it is not just those in charge that are to blame for the pressure on informational privacy, individuals themselves drive this issue, to a degree, with their obsession with efficiency. He argues that on the one hand, modern "developed" societies wish to be as efficient as possible, but they also want to retain traditional values such as privacy and protecting their personal information. Rule argues that a common ground needs to be found between these two conflicting interests, that of

efficiency in business and protecting informational privacy. Table 2.1 below summarises the literature discussed in this chapter up to this point.

Table 2.1 A Review of existing privacy theories

Theories of Privacy	Core Constructs	Definitions	Comment
Westin's Regulated Theory of Privacy (Westin, 1970)	Four states of privacy which convey how humans achieve privacy. Four functions of privacy in society which outline the reasons why humans need privacy	Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about themselves is communicated to others.	This theory has not been applied to the online environment.
Altman's Regulated Theory of Privacy (Altman, 1975)	Privacy is a dynamic process whereby people vary in the degree to which they make themselves accessible to others. Privacy is an interpersonal boundary regulation process by which a person or group regulates interaction with others. Privacy is a changing process whereby people continuously attempt to regulate their interaction with others	Privacy is the selective control of access to the self.	
Social Psychological Theory of Privacy (Laufer and Wolfe, 1977)	Individuals' concepts of privacy are tied to concrete situations in everyday life. These situations are described in terms of three dimensions: Self-ego; Environmental; Interpersonal; These combined with the dynamic of time aids in understanding individual perceptions of privacy.	The ability to exercise choice is experienced in any privacy situation as the ability to choose how, under what circumstances, and to what degree the individual is to relate to others or separate themselves from others.	This theory bases the concept of privacy on situational and temporal factors which influence an individual's view of their privacy

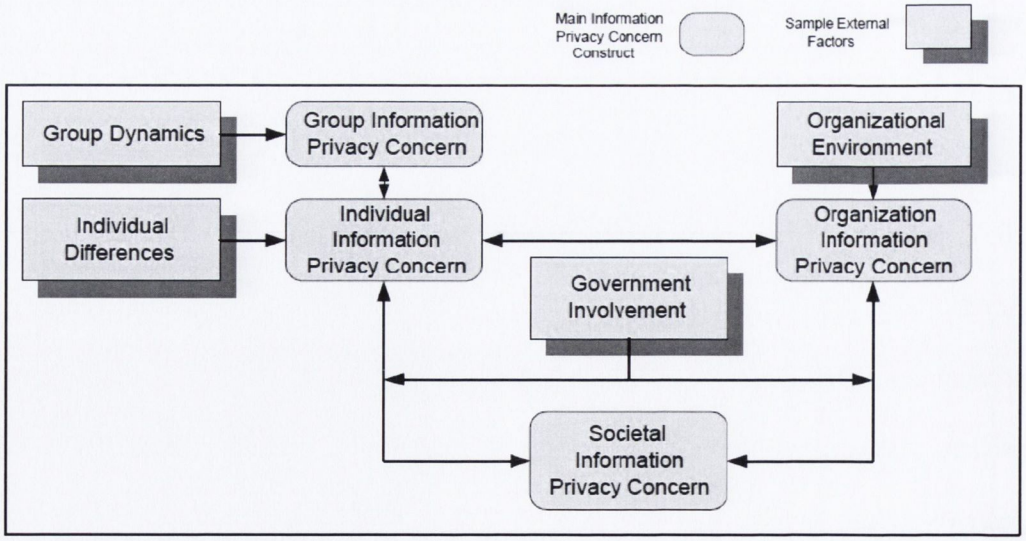
Control/Restricted Access Theory (Moor, 1997)	It is important to make sure the right people have access to relevant information at the right time. This theory allows different levels of access for different kinds of information at different times.	Privacy is a complex of situations in which information is authorized to flow to specific people, at specific times.	This theory allows different levels of access for different kinds of information at different times. This approach likens privacy to access control of personal information.
Control Theory of Privacy (Fried, 1968)	Individuals control access to their personal data.	Privacy is not simply an absence of information about a person in the minds of others, rather it is the control that a person has over information about themselves.	This theory gives the impression that privacy is simply a form of access control to personal information, similar to Moor (1997) in approach.
Ontological Theory of Informational Privacy (Floridi, 2005a)	Informational privacy concerns can be reduced or increased according to how the infosphere develops. ICTs can change the nature of the infosphere and thus change the very nature of informational privacy. By changing the nature of informational privacy, ICTs can change our understanding of informational privacy.	Informational privacy is a function of the ontological friction of the infosphere.	Privacy can be shaped by actors to either improve informational privacy or invade it.
A theory of informational privacy (Rule, 2007)	People are responsible for privacy invasions, not ICTs. Therefore, ICTs can be used to protect privacy.	Privacy is an authentic option to withhold information on one's self.	Rule limits his privacy theory to information about one's self.

2.3 Informational Privacy and Privacy Concerns

Informational privacy is difficult to measure (Belanger and Crossler, 2011). Almost all empirical privacy research in the social sciences relies on measurement of a privacy-related construct of some sort (Smith, Dinev and Xu, 2011). Examples of such constructs are beliefs, attitudes, and perceptions concerning privacy. Over time, however, especially within IS research, there has been a movement toward a focus on privacy concerns as the key measurable construct, thereby switching the focus of measurement efforts from privacy itself to the extent to which a subject cares about it. Surveys have consistently indicated that individuals are concerned with the ways businesses use their personal information. Such concerns prevent some consumers from making online purchases (Tsai et al., 2011). Privacy and American Business (2005) found that concerns about the (mis)use of personal information deterred 64% of respondents from purchasing from an online company at least once in the past, whereas 67% of respondents declined to register, at least once, at a website or shop online because they found the stated privacy policy to be too complicated or unclear. A number of e-commerce studies empirically verified the negative effect of perceived risk on intentions to conduct transactions (Budnitz, 1998; Jarvenpaa and Leidner, 1999; Jarvenpaa and Tiller, 1999; Jarvenpaa, Tractinsky and Vitale, 2000; Norberg and Horne, 2007; Norberg, Horne and Horne, 2007; Pavlou, 2003; Pavlou and Gefen, 2004). Additionally, previous studies generally supported the positive impact of privacy risk on privacy concerns (Dinev et al. 2006; Dinev and Hart 2004), and the negative impact of privacy risk on willingness to disclose personal information (Malhotra, Kim and Agarwal, 2004; Xu, Teo and Tan, 2005).

Smith et al. (1996) developed the concern for information privacy (CFIP) scale. They identify four data related dimensions of privacy concerns (collection, errors, secondary use, and unauthorized access to information). The meaningfulness of these dimensions was later confirmed by Stewart and Segars (2002) and have since served as some of the most reliable scales for measuring individuals' concerns about organizational privacy practices (Smith, Dinev and Xu, 2011). More recently, Malhotra et al. (2004) operationalized a multidimensional scale of Internet users' information privacy concerns (IUIPC), which adapted the CFIP into the Internet context (Smith et al., 2011). Bèlanger and Crossler (2011) contend that online privacy concern is a multi-level concept. They illustrate this by way of a framework depicting the expected interrelationships between levels of analysis for informational privacy concern (Figure 2.1). This multi-level framework suggests that group online privacy concerns are influenced by external factors as well as individual members' concerns for online privacy.

Figure 2.1 Online Privacy Concern Multi-level Framework (Bèlanger and Crossler, 2011)



Examples of external factors are *group dynamics*, *organizational concerns* and *societal concerns*. *Group dynamics* factors include a number of variables such as group cohesion, group centrality (level of centralized communications in the group), group distribution (level of collocation of team members), or group characteristics such as group size or duration of group existence (Bèlanger and Crossler, 2011). *Organizational* privacy concerns reflect the overall concern that organizational leaders have regarding the privacy of the information the organization possesses and to which it has access. *Societal* information privacy concern refers to the overall concerns citizens in societies taken as a whole have for the privacy of the information about them.

In an endeavour to assess the level of privacy concern within the Internet community, various academic and commercial surveys have been conducted over the last thirty or so years. Examples of such surveys are Dhillon and Moores (2001), Harris Interactive (2002), Hart and Dinev (2004), Earp et al. (2005), (Hui, Teo and Lee, 2007), Antón, Earp and Young (2010) and Tsai et al., (2011). Dhillon and Moores (2001) identified four central Internet privacy concerns and eighteen means to alleviate these concerns. Examples of these means were to enact stronger laws to protect consumer privacy and to use encryption in email communications (Dhillon and Moores, 2001). Milberg et al. (1995) conducted a survey of 900 members of the Information Systems Audit and Control Association (ISA&CA) in 30 countries and found that while the overall level of privacy concern for personal information varies across countries, the relative importance of four underlying dimensions of informational privacy concern (collection, secondary use, errors, and improper access) did not vary. Earp, et al. (2005) found that

information transfer, notice/awareness, and information storage were the top online privacy concerns of Internet users. In 2008, given the speed, according to Earp et al (2008), at which the privacy debate and the Internet environment was evolving, they were prompted to rerun the survey, to examine how events in the interim may have affected Internet users' online privacy concerns. The latter survey showed that U.S. Internet users' top three privacy concerns had not changed since 2002 (Earp et al, 2008). We report in the Table below a synopsis of informational privacy concerns identified by surveys conducted by the extant literature.

Table 2.2 Summary of survey findings on privacy concerns

Privacy Concern	Source
Collection of personal information	Smith et al. (1996) Milberg et al. (1995) Ackerman et al. (1999b) Harris Interactive (2002) Earp, et al.(2005) Antón, Earp and Young (2010)
Unauthorized secondary use of personal information	Smith et al. (1996) Dhillon and Moores (2001) Milberg et al. (1995) Ackerman et al. (1999b) Harris Interactive (2002), Earp, et al.(2005) Antón, Earp and Young (2010)
Improper access to personal information	Smith et al. (1996) Dhillon and Moores (2001) Milberg et al. (1995) Harris Interactive (2002)
Errors within stored personal information	Smith et al. (1996) Milberg et al. (1995) Earp, et al.(2005) Antón, Earp and Young (2010)
Identification theft through personal information once it has been collected;	Dhillon and Moores (2001)
Receiving unsolicited email	Dhillon and Moores (2001)
Being ask to provide personal information for free (people would be more willing to provide personal information if they were paid to do so)	Hui et al. (2007b)
Excessive request for information (the more information requested, the less likely the subjects were willing to disclose it)	Hui et al. (2007b)

2.3.1 Antecedents to Privacy Concerns

The IS literature on privacy has devoted considerable attention to the identification of *antecedents* to privacy concerns, i.e. observable determinants of privacy concerns. Their

identification rests on a combination of theory and empirical analysis. Typically, the researcher identifies variables deemed to influence privacy concerns, according to some theory or intuition, and then tests whether the candidate antecedent explains or predicts the level of privacy concerns by observing some measure of statistical association or causation. For example, Dinev and Hart (2004) and Harris Interactive (2002) found that the lack of trust in a company's ability to adequately safeguard personal information and the lack of knowledge regarding a company's use of such information are both antecedents to informational privacy concerns. Dinev and Hart (2004) suggest that the privacy concerns of individuals who use the Internet are driven by two antecedents:

- Perceived vulnerability;
- Perceived ability to control information.

The results of their investigation, which are based on a regression analysis of variables constructed from survey results, provide strong support for the relationship between perceived vulnerability and privacy concerns, but only moderate support for the relationship between perceived ability to control information and privacy concerns, perhaps suggesting that the relationship among the proposed antecedents and privacy concerns are more complex than the authors anticipated. The authors concede that other antecedents to privacy concerns, which are not captured in their theoretical model, may exist and may play an important role. An example of such an antecedent could be trust (Dinev and Hart, 2004). Ackerman et al. (1999) found that individuals cared about the (perceived) trustworthiness of companies that collect their information, and the purpose of the information collection and the company's policies with regard to redistributing it. These findings suggest that the following are two further plausible privacy concern antecedents:

- Lack of trustworthiness of companies that collect personal information
- Lack of clarity over the purpose of the information collection and the company's policies with regard to its use

They argue that proposed solutions to protecting privacy need to address each of these topics. They concluded that, in the absence of clear explanations about why the information is being collected, individuals produce their own versions of the company's motivations, which are usually not favourable. Clear and readily available explanations of intended information use might alleviate some concerns. The Harris Interactive survey (2002) also found that providing individuals with explanations of how their information will be used is one way of addressing many informational privacy concerns, thereby alleviating them.

Other U.S. based studies investigate the relationship between informational privacy concerns and other factors such as gender, age, income level and education (Dommeyer and Gross, 2003; O'Neil, 2000; Phelps, Nowak and Ferrell, 2000; Sheehan, 1999; Sheehan, 2002). There are some contradictory findings in these studies. For example, Sheehan (2002) and Phelps et al (2000) find that individuals with higher income levels are more concerned about informational privacy than those with lower income levels whereas O'Neill (2000) finds that individuals with higher income levels are *less* concerned about their informational privacy than those with lower income levels. O'Neill also finds no difference between individuals with high education levels and those with low education levels in terms of privacy concern. Both O'Neill (2000) and Sheehan (1999) find that women have more informational privacy concerns than men. Drommeyer and Gross (2003) find that males and young people were more likely to be

aware of privacy-protection strategies than their counterparts. O'Neill (2000) finds that the level of informational privacy concern also varies with race. Ethnic groups such as Latin Americans, Aboriginals, and African Americans, are more concerned about their privacy than Caucasians.

Castañeda and Montoro (2007) identify an extensive set of variables as the antecedents to privacy concerns for individuals on the Internet. The variables are divided into 4 categories:

- Customer-intrinsic characteristics, examples of such are socio-demographic factors or the amount of Internet experience individuals possess.
- Perceptions, beliefs and attitudes of the online customer in relation to factors such as direct marketing, trust, and the knowledge and perception of information control mechanisms, as well as to data collecting processes.
- Website-related variables, such as the publication of a fair and coherent privacy policy.
- Situational variables, such as the type of information requested, the benefits and risks perceived in providing such data over the Internet.

The same study also examined concerns about disclosing personal information on the Internet by looking at how consumer behaviour is influenced by:

- their familiarity with the website;
- the level of control the customer has over their personal information;
- the sensitivity of the information requested

Their results show the need for online companies to justify requests for information. Furthermore, increased sensitivity of the information requested has a negative influence on the intention of individuals to provide it (Castañeda and Montoro, 2007b). Phelps et al. (2000) find that the level of information control consumers feel that they possess and the type of information requested by marketing companies both have a significant influence on the purchase intentions of consumers. Sheehan and Hoy (1999) report that, as privacy concern increases, an individual is more likely to exhibit the following behaviour:

- Provide incomplete information to websites;
- Notify Internet Service Providers about unsolicited email;
- Request removal from mailing lists;
- Complain to online entities about unsolicited e-mail.

Unsurprisingly, it was found that, as privacy concerns increase, individuals are less likely to register on websites that request personal information. A survey of 1,017 Internet users by the Pew Internet and American Life Project found that about 25% of US Internet users have provided false information to a website and about 20% have used a secondary e-mail address to avoid giving websites real information (Rainie et al., 2000). George (2002) also examines the relationship between beliefs about privacy and Internet trustworthiness, intention and purchasing behaviour. He finds that beliefs about privacy and Internet trustworthiness help to determine attitudes towards the Internet, which in turn affects purchasing intentions (George, 2002). In a more recent study, George (2004) investigates whether customers' beliefs about privacy and trustworthiness over the Internet, influence their purchasing behaviour. He finds that

individuals' beliefs about trust have positive effects on their attitudes toward buying online, which in turn positively affects their purchasing behaviour (George, 2004).

Synopsis of Antecedents

Table 2.3 on the next page shows a summary of the results from the studies examined in this section. Both panels in the table report privacy concerns antecedents and the authors that draw attention to them. Panel A refers to the studies that have used the term "antecedent to privacy concerns" whereas Panel B refers to studies that have used the term "causes of privacy concerns" to refer to constructs that play essentially the same role in characterizing attitudes to privacy. Out of all the antecedents considered in the table, those broadly concerning online trust, perceived control over personal information and demographics of users that have received greatest attention in the empirical literature and the relevant literature is reviewed and discussed further in Appendix A, whereas the sensitivity of the personal information that the IS user is required to submit and the complexity of the circumstances surrounding the interaction have received the least support and attention, most likely due to the difficult to measure these constructs in the context of the surveys typically used to measure privacy concerns and their antecedents (as lamented by Smith et al. (2011), all such surveys focus on attitudes and a-situational intentions, rather than situation-specific circumstances, such as the sensitivity of the information that the IS user must supply in a given set of circumstances and the complexity of the latter).

Table 2.3 Antecedents to Informational Privacy Concerns

Panel A
(Constructs defined by the Authors as "antecedents" to informational privacy concerns)

Construct	Researcher(s)
Lack of trust in a company's ability to adequately safeguard personal information	(Ackerman et al., 1999b, Dinev and Hart, 2004, George, 2004, Harris Interactive, 2002)
The lack of knowledge regarding a company's use of such information including collection and redistribution	(Ackerman et al., 1999b, Castañeda and Montoro, 2007b, Dinev and Hart, 2004, Harris Interactive, 2002, Phelps et al., 2001)
The lack of informational control individuals feel once they have imparted their personal information.	(Castañeda and Montoro, 2007b, Milne and Boza, 1999, Phelps et al., 2000)
The sensitivity of the information that is being requested	(Castañeda and Montoro, 2007b, Milne and Boza, 1999, Phelps et al., 2000)

Panel B
(Constructs defined by the Authors as "causes" of informational privacy concerns)

Construct	Researcher(s)
Not having sufficient control over personal information once submitted online	(Phelps et al., 2001, Culnan, 1993)
Not knowing how their personal information is being used by businesses.	(Privacy and American Business, 2005)
The complexity of privacy policies	(Privacy and American Business, 2005; Ackermann, 1999)

2.4 Informational Privacy Control Models and Legislation

Solove (2008) argues that the misuse of personal information is frequently viewed by policy-makers as a technology problem, but he argues technology is not the root cause of many abuses of personal information. The shift to a digital environment certainly facilitates information misuse, but he believes the problem stems from a set of business and government practices. He argues that the problem is caused in significant part by the law, which has allowed the construction and use of digital dossiers without adequately regulating the practices by which companies keep them secure. For example, despite taking elaborate technological measures to protect their data systems, companies readily disseminate the personal information they have collected to a host of other entities and sometimes even to anyone willing to pay a small fee (Solove, 2008). This situation calls to mind what has come to be known as the unofficial slogan of the National Rifle Association in the US, "guns don't kill people, people do". Similarly, Solove (2008) argues that information systems do not breach online privacy, the people designing and controlling information systems do.

Rule (2009) notes that regardless of the limitations of the law, virtually every democracy in the world has some national privacy code. Some of the most recent countries to adopt such codes are Argentina, India and Taiwan. The majority of these countries have adopted regulation closer to the European model rather than the US model, which establishes broad rights, i.e. non situation specific rights, for holding personal information in various institutional settings (Rule, 2009).

Having recognised that information and communication technologies (ICTs) will play a pivotal role in the future success of Europe, the EU are investing millions into research and development in the pursuit of a trustworthy platform for safe online transactions to take place across Europe (The eSENS Project, 2013). Both the researcher and Escher Group (IRL) Ltd are participating in this EU project. Equally, the Federal Trade Commission (FTC) in the United States is working towards achieving similar results. The FTC published a report in late 2010 that proposes a framework to balance the privacy interests of consumers with innovation reliant on consumer information for developing beneficial new products and services (Federal Trade Commission, 2010).

In the next subsections, we look at existing regulations and policies that are already in place for protecting individuals' personal privacy at a national and governmental level.

2.4.1 European Data Protection Legislation

The European Union Data Protection Directive of (1995) was established to provide a regulatory framework to guarantee secure and free movement of personal data across the national borders of the EU member countries, in addition to setting a baseline for the security surrounding personal information wherever it is stored, transmitted or processed (European Commission, 1995).

The Directive contains 33 articles in 8 chapters and it came into effect in October, 1998. At a high level, the six basic principles of the Directive are as follows:

1. Notice: An individual has the right to know that the collection of personal data will happen. Personal data must be "*collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes*" (Section 1, article 6).
2. Choice: An individual has the right to choose not to have their personal data collected.
3. Use: An individual has the right to know how personal data will be used and to restrict its use. Personal data may only be used for "legitimate processing" as described by the Directive details.
4. Security: An individual has the right to know the extent to which the personal data will be protected. Organizations must "*implement appropriate technical and organizational measures to protect personal data.*" The measures must be "*appropriate to the risks represented by the processing and the nature of the data to be protected*" (Section 8, article 17)
5. Correction: An individual has the right to challenge the accuracy of the data and to provide corrected information. Personal data collected and maintained by organizations must be up to date and reasonable steps must be taken to ensure that inaccurate or incomplete data is corrected.
6. Enforcement: An individual has the right to seek legal relief through appropriate channels to protect privacy rights (The European Commission, 1995).

The personal data that the directive covers includes information relating to 'an identifiable person'. This includes information about a natural person directly identified by an identification number or indirectly with one or more facts that relate to his 'physical, physiological, mental, economic, cultural, or social identity'. Sensitive data is an important subset of personal data. Sensitive data is that which reveals racial or ethnic

origin, political opinions, religious beliefs, trade union membership, and health or sex life details. This information is regarded as sensitive because it could expose the data subject to discrimination as well as infringe on the fundamentals of privacy. Health information as defined by this research would include past or present information on physical or mental state as well as any abuse of drugs or alcohol (Herold, 2002).

The Directive on Privacy and Electronic Communications (2002) is an EU directive on data protection and privacy in the digital age. It builds on the Data Protection Directive of 1995 and applies to all matters which are not specifically covered by the Data Protection Directive. It deals with the regulation of a number of important issues such as confidentiality of information, treatment of traffic data, spam and cookies (European Commission, 2002). Since its enactment, it has also been amended by Directive 2009/136, which introduces changes specifically concerning cookies and unsolicited email or other messages (European Commission, 2009).

2.4.2 Safe Harbor

The EU Data Protection directive mandates that the personal data of consumers and employees cannot be transferred by multi-nationals operating in the EU to their home country unless that country has "adequate" data protection regulations in place. In the late nineties, this mandate nearly resulted in a 'trade war' between the US and Europe over the issue of privacy (Rule, 2007). In 1995, America stood out for its lack of a comprehensive legislation regulating private sector uses of personal information (Rule, 2007). By the end of the 1990s, it became apparent that the business-friendly Clinton administration had no intention of taking steps to make its privacy legislation adequate

by European standards. The consequence of such a stance, under the EU data Directive, was to block flow of personal information collected in Europe to the US. In response, Clinton administration officials threatened that any such action would trigger economic retaliation from the US side (Rule, 2007). In the end, over objections of the European Parliament, the European Commission agreed to a compromise that met American requirements in almost all respects (Rule, 2007). The agreement is called Safe Harbor.

The Safe Harbor provides a privacy compliance framework and a way for American organizations to avoid experiencing interruptions in their business dealings with the EU, or facing prosecution by the European authorities under European privacy laws. Certifying an American organization to the Safe Harbor requirements was intended to assure EU entities that the organization provides "adequate" privacy protection as required by the EU Directive (Rule, 2007). It was intended that the Safe Harbor framework would provide a simpler and cheaper means of complying with the privacy adequacy requirements of the EU Directive, and would also significantly benefit small and medium organizations. Due to the fact that Safe Harbor permits American corporations to self-certify the practices that they follow regarding personal information, most organisations importing personal information into the US from Europe frequently disregard the measure (Rule, 2007).

2.4.3 Fair Information Practices (FIPs)

Various guidelines have been set out as codes of practice for the Internet community to follow regarding informational privacy protection. Most existing privacy guidelines and

indeed privacy laws have their foundations in the Fair Information Practices (FIPs) principles which were first formulated by the Advisory Committee on Automated Personal Data Systems. This advisory committee was appointed by the U.S. Department of Health, Education and Welfare to assess the impact of computer-based record keeping on private and public matters and to recommend safeguards against its potentially adverse effects (Weinberger, 1973). There are five FIPs principles:

- Notice/Awareness;
- Choice/Consent;
- Access/Participation;
- Integrity/Security;
- Enforcement/Redress.

Examples of other privacy guidelines can be found in the Platform for Privacy Preferences Project (P3P) (World Wide Web Consortium, 1994) and the OECD Privacy Guidelines (OECD, 1980). There are also a number of privacy theories and conceptual models in the research domain that have been proposed as solutions to bridging the social-technical gap (DePaolo, C. Wetzel and Wilson, 2003; Milberg, Smith and Burke, 2000; Moor, 1997; Taviani, 2007). Van Lieshout et al. (2011) argue that the drafters and adopters of FIPs had large mainframe computers and centralized databases in mind for these principles and that they could not have foreseen how revolutions in sensors, bandwidth, storage, and processing power would converge into a hyper-connected "Web 2.0" networked world of ubiquitous data availability. They argue that the scale and complexity of current data systems, networks and practices require a new and updated set of universally-accepted privacy design and practice principles that are

robust, comprehensive, and capable of assuring privacy and trust amid the new global realities.

In 2008, the Privacy Office at the Department of Homeland Security offered its own version of privacy principles for systems engineering. They are also modelled on the FIPs and are called Fair Information Practice Principles (FIPPs) (Teufel III, 2009). These FIPPs build on the original FIPs to protect informational privacy in a more complex information age. The principles are:

1. Transparency;
2. Individual Participation;
3. Purpose Specification;
4. Data Minimization;
5. Use Limitation;
6. Data Quality and Integrity;
7. Security;
8. Accountability and Auditing.

2.5 Approaches to Engineering Informational Privacy Protections

There has been much debate across many disciplines over the last few decades about how to reduce privacy concerns and how to enforce the right of the individual to control and protect their personal information once submitted online. It has been unclear at times how such privacy rights should be given effective expression through technology. Gurses et al. (2011) argue that there is a disconnect between policy makers and

engineers when it comes to what it means to comply technically with data protection regulations. Policy makers often make recommendations about how personal information should be protected but fail to give explicit directions to organisations and systems developers on how exactly the systems should be developed to ensure such levels of protection. In the IS literature, Smith et al (2011) call for more research that applies the theoretical developments made in the IS privacy literature to studies which produce empirical results. Gurses, Troncoso and Diaz (2011) argue that building privacy into IS technologies and operations must be done in a systematic way, with reference to time-honoured privacy principles, standards and other relevant guidance. In this section, we look at existing approaches to building privacy into IS technologies. Firstly, we look at the Privacy by Design (PbD) principles. These were developed to guide IS designers on how to build privacy into systems. Secondly, we review existing privacy-enhancing technologies and categorise them according to their privacy enhancing capabilities.

2.5.1 Privacy by Design (PbD)

The concept of Privacy by Design (PbD), first introduced by Ann Cavoukian in the late 90s, builds on the Fair Information Practices outlined by the Organization for Economic Cooperation and Development (OECD) in 1980 (Gellman, 2012). The concept of PbD is straightforward: build privacy in early and thoroughly into your data management systems, and reap the many rewards that will result from enhanced trust (Cavoukian 2010). The PbD principles for reducing privacy concerns of individuals are as follows:

1 Data minimization;

2 User participation;

3 Safeguards;

4 Accountability;

5 Proactive not reactive;

6 Privacy embedded into design;

7 Positive-sum not zero-sum.

These seven principles must be applied from the onset of systems development to mitigate privacy concerns and achieve data protection compliance. The use of PbD to engineer privacy into ICT systems is still rather underexplored and requires substantial conceptual and empirical work to be done to ensure it is designed and engineered effectively (Van Lieshout et al. 2011). Van Lieshout et al. (2011) believe a holistic PbD approach to implementing privacy into the design of an artefact can offer increased privacy protection without foregoing functional requirements. However, they warn that the implementation of PbD is not easily realized (Van Lieshout et al. 2011).

Engineering systems with privacy in mind requires integrating privacy requirements into the typical systems engineering activities of a product development project. This requires the elicitation and analysis of 1) the concept of privacy, 2) the functional requirements of the system being developed; and 3) the development of designs that fulfil those requirements. It also includes implementing those designs, and testing that functional and privacy requirements are fulfilled by such implementations. Since most privacy requirements rely on the application of basic security principles, i.e. confidentiality, integrity, and availability, security engineering activities like risk and threat analysis ought to also accompany the process. However, research on designing systems with privacy in mind is limited, and even such research is typically inaccessible to policy makers who discuss the principles of PbD (Gurses, Troncoso, and Diaz 2011).

Cavoukian's (2010) concept of PbD not only applies to IT Systems, it also considers how informational privacy should be protected in business practices, and the physical design and networked infrastructure of an organisation. Practical implementation of this concept demands a holistic organisational approach to informational privacy protection. Gurses et al. (2011), however, argue that, despite its "comprehensiveness", it is not clear how the PbD concept should be translated into engineering practices. Most of the principles include the term Privacy by Design in the explanation of the principle itself. For example, the definition of Principle number 3, (Privacy Embedded into Design), states that PbD is "*embedded into the design and architecture of IT systems [...]. It is not bolted as an add-on after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system without diminishing functionality*" (Cavoukian, 2006: 3). This circular definition communicates to the reader that something needs to be done about privacy from the beginning of systems development, but it is not clear what exactly this privacy matter is nor how it can be translated into design (Gurses, Troncoso, and Diaz 2011).

This vagueness is not unique and can also be found in the various principles expressed in the articles of the Data Protection Directive 1995 (The European Commission, 1995). The Directive states that data collection should be limited. As Kuner (2007) explains the EU data protection law requires that personal data processing be strictly limited to the purpose originally notified to the data subject. For instance, Article 6(1)(b) of the General Directive provides, in part, that personal data must be `collected for specified, explicit and legitimate purposes' and must be `adequate, relevant and not excessive in

relation to the purposes for which they are collected and/or further processed' (The European Commission, 1995).

Even though Kuner (2007) argues that the first principle, data minimization, can be interpreted as meaning that processing of personal data must be restricted to the minimum amount necessary, it is not explicitly stated in the Directive. This oversight has serious consequences in practice (Gurses, Troncoso and Diaz, 2011). The absence of an explicit and precise data minimization principle makes the proportionality clause susceptible to a reversal of its intended effect. Data collectors can articulate the purpose specification to include any data they wish (Gurses, Rizk and Gunther, 2010), eliminating the need to consider data minimization. Moreover, the interpretation of the Data Protection Directive (or FIPs) to collect all data of interest is acquiesced as long as individuals are provided with control over the collected information, e.g., informed consent and subject access rights (Gurses, Rizk and Gunther, 2010).

This control can be translated in systems as policy selection and negotiation, privacy settings, and other solutions that allow individuals to access and amend their personal data. Although providing control can be a powerful tool, even when all the aforementioned protection measures are in place, the scope of control over personal data may be limited. By shrinking the scope of the definition of what counts as personal data, companies can limit the reach of solutions that provide users with control over their collections of data (Gurses, Rizk and Gunther, 2010). By applying simple anonymisation over aggregated personal data, data processing activities are taken outside of the scope of data protection and slip further away from the control of the users (Gurses, Troncoso and Diaz, 2011).

2.5.2 Privacy Enhancing Technologies (PETs)

Implementing stronger governmental models and privacy policies for safeguarding personal information over the Internet may be seen by some as a positive step toward solving the problem of informational privacy protection. However, as seen in the previous section, the law has its limitations and there are many difficulties associated with policing and enforcing regulation, not to mention the difficulty in defining what is meant by privacy. The question then arises as to whether there are other, more effective ways to limit the powers of government and private companies in collecting personal information from individuals and using this information for their (the government or private company) own purposes.

Goold (2009) questions whether society can move from a regulatory framework that is reactive to one that is proactive. Considering this line of thought, he questions whether it is possible to establish a system of checks and safeguards that does not rely solely on the co-operation of law enforcement agencies, or the vigilance of individuals and civil liberties groups. One such solution would be to shift the underlying basis of regulation away from one focused on reactive legal measures to one that seeks to limit the powers of private companies and government to collect personal data. This could be achieved in two ways. The first would be through the establishment of a set of general, legally enforceable principles that seek to clearly define the limits of personal information collection and the conditions that must exist before any such collection can take place. One example of such a principle would be data minimisation. This principle states that personal information should only be collected if it is directly relevant and necessary to accomplish a specified purpose, and that it should only be retained for as long as it is

necessary to fulfil that purpose (The Privacy Office, 2007). Gurses et al (2011) argue that different kinds of data minimization are possible, and each system requires careful crafting of data minimization best suited for its purpose. They argue that decentralisation of personal information is key to minimising access to personal data.

The second way would be through the principle of minimal retention (Goold, 2009). This requires that records containing personal information be destroyed once the specific purpose of collecting that personal information has been satisfied and its retention is no longer needed to achieve that purpose. The adoption of such a principle would mark a significant break with traditional principles of data retention, which either have unlimited retention or lengthy time limits. The problem with the principle of minimal retention approach is that it is inevitably very general. A second approach, which is more subjective and contextual, will usually be needed. Goold argues that mechanisms need to be put in place, which limit the amount of human agency and discretion associated with collection of personal information. These mechanisms need to be capable of being adjusted according to the context in which personal information collection takes place and the legitimate purposes for which that information is being used (Goold, 2009).

An alternative way of achieving this type of restraint is through the use of what have come to be known as Privacy Enhancing Technologies or PETs. This term encompasses a wide spectrum of both new and well established technologies which protect private data from unauthorised exposure in the information society. Unfortunately, the term does not have a widely accepted definition, and the scope of PETs is often context-

dependant (META Group, 2005). According to Burkert (1997) the concept of PETs refers to technical and organisational concepts that aim to protect personal identity. These concepts usually involve encryption of some form such as digital signatures. Agre and Rotenberg (1997) view PETs as one of the most significant technical innovations of the previous thirty years. They argue that since the publication of the first public-key cryptographic methods in the 1970s, mathematicians have constructed formidable methods for communicating and transacting over the Internet while at the same time managing to control access to sensitive information. Levy (2001) gives a detailed account of these developments from the time before the first public key cryptographic methods were published in the 1970's up until more recent developments in PETs technology at the beginning of the 21st Century. Brunt (2006) takes a wider approach to the definition of PETs in a technical note for the Information Commissioner's Office of the UK. He sees PETs as not being limited to tools that provide a degree of anonymity for individuals, but rather any technology that exists to protect or enhance an individual's privacy. Goold (2009) summarises PETs as:

1. Technologies that automatically anonymise personal information and make it difficult for third parties to determine the origin of that information;
2. Encryption tools, which aim to prevent hacking of information transmitted over the Internet;
3. Cookie-cutters, which prevent third parties from placing cookies on an individual's computer in order to make it perform certain tasks without the user being aware of them;
4. Platform for Privacy Preferences (P3P) services, which allow Internet users to analyse the privacy policies of websites and compare them with their preferences as to the information they wish to release.

Regardless of how they are defined, most researchers agree that the concept of privacy-enhancing technologies (PETs) is a complex one (London Economics, 2010). It comprises a broad range of various technologies at different levels of maturity. PETs are constantly evolving, often in response to ever more sophisticated threats. Data minimisation and consent mechanism are an important part of the PETs concept. Many PETs combine various technologies, including data protection tools such as encryption and data minimisation tools to form integrated PET systems of varying complexity (London Economics, 2010).

A variety of different classifications of PETs has been proposed, primarily based on technological characteristics. Any useful classification of PETs recognises that disparate technologies exist, and at different stages of development. These range from cutting edge concepts, not yet commercially available, to long established technologies. Several classifications for PETs have been developed. None, thus far, have gained universal acceptance (London Economics, 2010). This perhaps is a result of different underlying assumptions about the use of PETs, their definition and their purpose i.e. for legal, business or medical purposes etc. Typically, the classification systems follow a functional paradigm.

Wang and Kobsa (2009) propose three paradigms:

- Protection of identity: this type of privacy protection aims to prevent users' true identities from being revealed (i.e., who they are).
- Seclusion: this type of privacy protection attempts to prevent users from being bothered by unwanted contact or solicitation (e.g., spam emails).

- Control over data: this type of privacy protection allows users to have control over their data, e.g. regarding what data can be collected or disclosed for what purpose, how the data will be used, and with whom the data may be shared or to whom it may be transferred.

The META Group (2005) classification contains a more specific breakdown of PETs, further classifying PETs in terms of aim (curative or informative) and function (unobservability, unlinkability and anonymity). A high level overview of the META classification is shown in the table below:

Table 2.4 PETs Classification, (Meta Group, 2005)

Privacy Protection	Pseudonymiser Tools
	Anonymiser Products and Services
	Encryption Tools
	Filters and Blockers
	Track and evidence erasers
Privacy Management	Informational tools
	Administrative Tools

The European Commission Director General (DG) Justice, Freedom and Security, Mr Jonathan Faull, commissioned the consultancy firm 'London Economics' to undertake a study on the economic benefits of PETs for organisations and institutions using and holding personal data. The study covered 12 EU member states that were selected after consultation with DG Justice, Freedom and Security. Table 2.5 below summarises the current PETs solutions that the report found available to both individuals and enterprise within the 12 EU member states.

Table 2.5 PETs for privacy protection (London Economics, 2010)

Stand-alone technologies	**Examples**
Technologies for protecting of the identities of senders/receivers of email	Remailers, types 0-III.
Technologies for protecting of identity when accessing interactive Internet services	PipeNet, Anonymizer.com, Onion Routing, The Freedom Network, Java Anon Proxy, Tor
Technologies for protecting of the content of Internet conversations	PGP and Compatible Systems, SSL and TLS, Off-the-Record Messaging
Technologies for enabling private payments	None (according to Goldberg, referring to electronic cash).
Technologies for proof of authorisation without revealing privet information (privacy credentials)	eID, OIX, U-prove
Technologies for offline information systems	Van Blarkom's hospital information system
Privacy technologies for RFID systems	Out-of-tag mechanisms, Tags with cryptographic circuits
Concepts, processes and systems	Examples
Cryptographic obfuscation	N/A
Random data perturbation	Privacy Integrated Queries (PINQ)
Privacy friendly pay-as-you-drive insurance	PriPAYD
PETs for privacy management	
Standalone technologies	Examples
Technologies for preventing phishing attacks	eBay's Account Guard, Google's Safe Browsing toolbar, Cloudmark Anti-Fraud Toolbar, Numerous others.
Technology for transparency of prior transactions	PRIME Data Track
Concepts processes and systems	Examples
Privacy metrics	Uncertainty measures, Indistinguishability measures.
Languages for writing enterprise privacy	EPAL

policies	
Enterprise privacy policies	EPAL policies
HCI technology for privacy-enhancing identity management	PRIME HCI technologies, Role-centred paradigm, Relationship-centred paradigm, TownMap-based paradigm.

PETs can assist companies in complying with the principles that protect an individual's privacy. Such technology can empower individuals by providing easier access to, and control over, their information and allow them to decide how and when to disclose it as well as when it can be used by third parties (Brunt, 2006). PETs have their critics. Taviani (2007) argues that technology-based solutions such as PETs do not provide systematic or comprehensive approaches to resolving the broader dimensions of privacy issues affecting online activities. He contends that they provide solutions that are narrow and *ad hoc*, in that they focus on concerns that are specific concerns such as data-mining, as opposed to broader concerns about online privacy in general (Taviani, 2007). Levy (2001) notes that there are many threats to even the most sophisticated modern encryption systems. Because of Moore's Law (Moore, 1965), brute force attacks on renowned encryption systems, attacks that seemed impossible only a few years ago, may now be possible. Additionally, an even greater threat to the world of encryption is the development of quantum computers, machines which take advantage of subatomic physics to run much faster than current computers. Levy uses an amusing analogy to describe this difference in the speed of quantum computers to current models: "*Think of the speed differential between turtles and laser beams*" (Levy, 2001, P275).

Goold (2009) believes that it is important that PETs are at the centre of any governmental legal model and makes their development and adoption mandatory. Information systems developers should be required by law to build in certain key privacy enhancing features that government agencies and private companies would be both required to use and prohibited from disabling. Companies developing new technologies should be required to design privacy and limiting mechanisms into their systems in order for their products to be licensed for sale. This technologically enhanced approach to online privacy regulation has three important advantages. Primarily, it does not focus solely on modifying the behaviour of those collecting personal information. Instead it explicitly recognises that there is a need to restrict what the technology can do and make it more difficult for private companies and governmental agencies to engage in unlawful or overly intrusive behaviour. The second advantage of this approach is that it is proactive and preventative, rather than reactive and punitive. As it focuses on preventing unwanted forms of collection and on limiting what companies can do and in principle, it should also reduce the number of abuses and the need for costly complaints procedures. The third advantage is that it forces both producers and users of technology to regard the collection of personal information and the legality of doing this as inseparable, and therefore encourages them to regard privacy enhancements as a positive aspect of the technology (Gurses, Troncoso and Diaz, 2011). At present, producers of data mining software have no incentive to think about privacy matters or about the ways in which their products might be used. By making it a legal requirement for any such devices to have privacy enhancing technologies built in, such companies are forced to confront these issues and to negotiate them with their potential customers. Thus, PETs should be part of a mosaic of solutions in combination with stronger governmental privacy models, laws and policies.

Conceptual models from the academic domain also have a role to play in such a solution.

2.6 Conclusions

This chapter examined the concept of Informational privacy from various perspectives, with a special emphasis on views held within the law, sociology and IS disciplines, of theories within which such definitions arise and, more generally, of how such definitions inform extant theories of informational privacy. We also reviewed the empirical literature on informational privacy concerns, both in online and offline settings, the main policies and regulations concerning the protection of informational privacy, and methodologies considered by the literature for engineering privacy protection mechanisms into technology. We placed special emphasis on the Fair Information Practices (FIPs) developed in the early seventies and the principles of PbD that were introduced in the late nineties by Cavoukian (1998). These sets of privacy protection practices and design principles are especially useful in NSPD and, along with the European Data Protection legislation, were used during the RiposteTrEx project to provide guidance to the designers and developers of the system on matters concerning the engineering of data protection mechanisms into RiposteTrEx. In order to understand what has already been achieved in the engineering domain with regard to privacy enhancing technologies (PETs), existing PETs and their usefulness in protecting informational privacy were also considered in the final part of this chapter.

3 Privacy-Related Decision Making Under Uncertainty

The decision to interact online in a manner that might put privacy at risk and the strategies that IS users may elect to deploy to handle such risk are instances of decisions made under conditions of uncertainty. The economics literature has devoted considerable effort, over many decades, to modelling and understanding the problem of decision making under uncertainty. Acquisti & Grossklags (2008) argue that the understanding of decision making problems in the IS domain has not yet fully benefited from progress made by economists in modelling and understating these type of problems, due to a somewhat limited interaction between these two disciplines (Acquisti & Grossklags, 2008).

In this chapter, we will first review the main contributions made by the economics literature to the understanding of decision making under uncertainty. We will group these contributions in two broad paradigms, one in which the decision maker is assumed to be fully rational and well informed and the other one in which this assumption is, to different degrees, relaxed. We will then review studies that have made use of such contributions to shed light on decision making problems in the IS domain, with special emphasis on those considering privacy and privacy-related problems, and, more broadly, we will seek to trace and discuss the influences that insights offered by the economics literature have had on the IS literature and on the understanding of privacy risk, privacy risk taking and privacy risk handling behaviour. The final section of the chapter will summarize the main insights with special regard to those that will prove

more useful in the analysis that will follow and, in particular, in the development of the stylized model of privacy risk taking and risk handling behaviour that will be put forth in later chapters.

3.1 Theories of Decision Making under Uncertainty

There are at least two broad paradigms in the economics literature with respect to goal-driven decision making under uncertainty. One such paradigm, which can be labelled as *neo-classical* or as including theories of '*rational decision making*', revolves around the assumption that the decision-maker is both fully rational, in the sense of being able to formulate an exhaustive ranking of all available alternatives and make coherent choices among all available alternatives, and endowed with a large amount of information. The other paradigm, which we may label as *behavioural,* or as including theories of '*imperfectly rational decision making*', allows for less than full rationality on the part of economic agents, i.e. the decision makers, and/or limited information available to them. It consisted initially of theories based on '*bounded rationality*' (Simon, 1957) and later developed into the broader *behavioural economics* critique of the rational decision making paradigm (Kahneman and Tversky, 1979). We shall now illustrate first the neoclassical rational decision making paradigm and subsequently the theory of bounded rationality and other models belonging to the behavioural paradigm.

3.1.1 Rational Decision Making and Expected Utility Theory (EUT)

A crucial role in models of rational decision making under uncertainty is played by Expected Utility Theory (EUT), as formulated in the seminal work of von Neumann and

Morgenstern (1947). In EUT, decision-makers are fully rational in that they use a well-defined mathematical object known as a utility function to rank alternatives, have a well-defined goal represented by the maximization of the *expectation* of this function and make coherent decisions by choosing the course of action or alternative that, ex-ante, achieve such goal. Implicitly or explicitly, it is also assumed that they have enough information to find it worthwhile to adopt such a structured approach to decision making, which entails considerable 'computational' requirements (Anand, 2002).

As for the requirement that the decision-maker be endowed with a large amount of information, which also plays a central role in theories of rational decision making, a relatively strong version thereof is the so called rational expectation hypothesis, which has been influential in economics discipline (Muth, 1961). Under this hypothesis, the information available to the decision maker includes the full knowledge, up to a random error term, of the stochastic process that generates the possible outcomes. It implies that the weights assigned to possible outcomes in calculating expected utility, i.e. the decision making goal under EUT, correspond to the true probability of such outcomes.

EUT, often under the companion assumption of rational expectations, has usually been applied in the discipline of economics but it has also had considerable influence in many of the behavioural and social sciences and in related policy fields such as law and medicine (Mongin, 1997). The theory implies, for example, that the rational actor will follow the elementary rules of probability when calculating, say, the likelihood of a given candidate winning an election or the odds of surviving a surgical intervention. Calculations of probability and multi-attribute utility can be rather formidable judgments to make, but the EUT assumes that people make them and make them well

(Gilovich, Griffin and Kahneman, 2002). Advocates of the theory do not argue that people never make mistakes in these calculations, but they do insist that the mistakes are unsystematic (Gilovich, Griffin and Kahneman, 2002).

3.1.2 Bounded Rationality

The paradigm that revolves around the concept of 'bounded rationality' assumes that, in the presence of limited information and/or limited information processing capacity on the part of the decision maker, the latter either replaces or complements expected utility maximization with other less demanding decision making rules, for example heuristics and rules based on adaptive learning. Bounded rationality has become the workhorse of a school of thought about decision making under uncertainty that developed from dissatisfaction with comprehensively rational economic decision theory models, represented by EUT and its variants. Like EUT, bounded rationality theory assumes that actors are goal-oriented, but bounded rationality takes into account the cognitive limitations of decision makers in attempting to achieve those goals. Its scientific-epistemological approach is different to EUT in that, rather than making assumptions about decision making and modelling the implications mathematically for aggregate behaviour (as in markets or legislatures), advocates of bounded rationality typically adopt an explicitly behavioural stance deeming that the behaviour of decision makers must be examined, whether in the laboratory or in the field (Jones, 1999), rather than deducted from first principles and axioms of (rational) choice.

Herbert Simon (1957) was among the first to argue that the "full" rationality implied by the rational choice model was an unrealistic standard for human judgment and to

propose a systematic alternative to EUT that did not suffer from this shortcoming. He proposed a more limited criterion for actual performance, which has already been discussed namely bounded rationality. Bounded rationality theory acknowledges the inherent processing limitations of the human mind. Simon (1957) argued that people reason and choose rationally, but only within the constraints imposed by their limited search and computational capacities. He also discussed the simplifying heuristics that people could employ to cope effectively with these limitations.

3.1.3 The Broader Behavioural Economics Critique of the Rational Paradigm

Later, psychologists Kahneman and Tversky (1972) developed their own outlook on bounded rationality, laying the foundations for a comprehensive reappraisal of decision making under uncertainty within the economics literature. They were convinced that the processes of intuitive judgment were not merely simpler than rational models assumed, but were categorically different in kind. Kahneman and Tversky described three general-purpose heuristics, "availability", "representativeness" and "anchoring and adjustment," that underlie many intuitive judgments under uncertainty. These heuristics, it was suggested, were simple and efficient because they piggybacked on basic computations that the mind had evolved to make (Gilowich et al. 2002). For instance, many people rely on media for information about deaths by homicide and strokes. If the media tends to report type A cause of death more than type B, people who rely on availability heuristics recall instances related to type A more readily than type B and as a result believe type A is the main cause of death between the two. The availability of information about type A cause of death leads them to conclude it is the main cause of death. Thus media coverage biases a rule based on recall (Sheffrin, 2002).

Representativeness is "the degree to which [an event] 1) is similar in essential characteristics to its parent population, and 2) reflects the salient features of the process by which it is generated" (Kahneman and Tversky, 1972, p. 431). Representativeness, when used to form the basis for judgement, gives rise to a cognitive bias to the extent that an individual categorizes a situation based on a pattern of previous experiences or consolidated beliefs about that situation. Representativeness, as a principle on the basis of which beliefs are formed, is about reliance on stereotypes. The simplest example of using such a principle in forming beliefs is to predict that university GPA will be the same as high school GPA. Thus, a student with a high GPA in school is seen as representative of a good student. This does not necessarily predict their performance at university (Sheffrin, 2002).

The anchoring bias emerges when individuals need to reach some judgment, let us say the exchange they are willing to make when disclosing personal information to an online entity in return for some benefit. Initially they form a preliminary judgment from some simple feature (anchor) and then adjust this estimate to form a final judgment. The adjustment, however, is usually conservative, and hence the final judgment is usually biased towards the initial anchor. Thus, if an individual primarily perceives (or anchors) the online entity to be risky, for any number of reasons, then the final judgement (adjustment) is likely to be biased toward the initial anchor and hence towards the initial assessment that the entity is risky, even after additional information (previously possibly neglected) suggests otherwise. This is of particular relevance for entities that have experienced bad press with regard to informational privacy breaches.

The work of Kahneman and Tversky (1972) played a key role in the development of behavioural economics, which examines how individual, social, cognitive and emotional biases influence economic decisions. The research in the behavioural economics discipline is predominantly based on neoclassical models of economic behaviour, in many ways similar to those employed by advocates of the rational decision making paradigm, but it aims to integrate rational choice theory with features supported by evidence from individual, cognitive, and social psychology (Sheffrin, 2002). Behavioural economic models abandon some of the tenets of rational choice theory, i.e. that agents possess consistent preferences between alternatives, choose the utility maximizing option, discount future events consistently, and act upon complete information or known probability distributions for all possible events (Acquisti and Grossklags, 2008). This way, behavioural economics can in principle account for empirical phenomena which would be impossible or difficult to reconcile with the rational paradigm and EUT (Sheffrin, 2002).

In doing so, behavioural theories of decision making under uncertainty allow for judgement error and incoherent decision making, such as how our innate bounded rationality limits our ability to exhaustively search for the best alternative; how the framing of a scenario or a question may influence an individual's reaction to it; how heuristics often replace rational searches for the best possible alternative; and how biases and other anomalies, themselves generated by reliance on biased heuristics, affect the way we compare alternatives, perceive risks, or discount values over time (Camerer & Lowenstein, 2003; Sheffrin, 2002). Heuristic biases are cognitive errors, that is, they are errors that stem from the way people think. Unlike models that adopt the perspective of the rational decision making paradigm, models in the behavioural economics

literature typically allow for the systematic occurrence of such biases (Camerer and Lowenstein, 2003). As summarized by Sheffrin (2002), heuristic-driven bias affecting decision making is the end result of the following four sets of circumstances:

- People develop general principles as they find things out for themselves;
- They rely on heuristics, rules of thumb, to draw inferences from the information at their disposal;
- People are susceptible to particular errors because the heuristics they use are imperfect;
- People actually commit errors in particular situations, and in some of those situations they do so in a systematic fashion.

Sheffrin (2002) suggests that most of these biases involve a combination of emotion and cognition. He also argues that both emotion and cognition involve mental processing and they may be physiologically linked, as opposed to being separate from each other. For example, as shown in the psychology literature, evidence exists that emotion plays a role in the way people remember occurrences and especially the different ways in which they remember pleasant and unpleasant occurrences (Sheffrin, 2002).

3.1.4 Knightian Uncertainty

Knight (1921) proposed to distinguish situations characterized by risk, in which the possible random outcomes of a certain event have known associated probabilities, from those characterized by uncertainty or ambiguity, in which the randomness cannot be expressed in terms of mathematical probabilities, and the probabilities themselves are unknown or unknowable. This definition of uncertainty has come to be known as Knightian uncertainty.

In decision theory and economics, ambiguity aversion, also known as (Knightian) uncertainty aversion, plays an important role in models of decision making under uncertainty. There is evidence that decision makers frequently exhibit ambiguity aversion (Erbas and Mirakhor, 2007), i.e. that they prefer known risks over unknown risks. When ambiguous prospects are presented to them alongside risky but unambiguously defined prospects, they often opt for the latter. They would rather choose an option with fewer unknown elements than with many unknown elements. For example, individuals prefer to bet on a bag with 50 red and 50 blue poker chips than in one with 100 total poker chips but where the number of blue or red chips is unknown. Sheffrin (2002) argues that the aversion to ambiguity is due to fear of the unknown but, unlike the heuristic biases, it is not a cognitive error, at least to the extent that the perceived ambiguity corresponds to true ambiguity, i.e. that it is not itself a biased judgement. Ghirardato & Marinacci (2001) uses ambiguity aversion to explain the implications of incomplete contracts for the occurrence of the missing markets phenomenon, and selective abstention in elections. Indeed, aversion to ambiguity has been linked to the financial crisis which followed the collapse of Lehman's Brothers in 2008 (Boyarchenko, 2012). The basic argument is that there was too much uncertainty in the financial markets, which lead investors to withdraw in turn making the financial situation worse.

3.1.5 Risk and Risk Perception

In what follows, we will first discuss alternative definitions of risk, for the purpose of showing how different definitions of risk imply different specifications of the utility

function. This is important because, in the IS literature, authors often posit that individuals evaluate some risk-reward trade-off in relation to informational privacy decisions (Milne and Gordon, 1993; Culnan, 2003; Chellappa and Sin, 2005; Hui, Teo and Lee, 2007; Hann, Hui and Lee, 2008), which may be seen as implicitly assuming that individuals maximize the expectation of an appropriate utility function. We will then discuss the difference between risk and risk perception, and illustrate theories of the latter. This is important because a discrepancy between risk and risk perception represents a departure from the assumptions of the neoclassical model, in that it violates the rational expectation assumption, and might occur in settings considered in IS research devoted to the study of privacy-related decisions.

Alternative Definitions of Risk

Definitions of risk differ across disciplines and even within disciplines, and experts and the public often have different interpretations of risk (Renn, 1998; Weber, 2001). One essential element of risk, however, is uncertainty. As put by Weber (2001), in order for a decision or action to appear risky, there has to be some uncertainty about the outcome.

In common definitions of risk, whether explicitly or implicitly, it is often assumed that the relevant outcome is negative, for example the risks associated with a nuclear disaster. Mainstream economic theories, however, adopt a definition of risk that refers to both large gains and large losses. For example, under typical choices of the utility function and other assumptions often made under the neoclassical decision making paradigm, as in the seminal work of Markowitz (1952), risk is the standard deviation of returns (outcomes) and, as such, it is a function (expectation) of both positive and

negative (squared) deviations from the expected outcome. As another and somewhat extreme example, there is also the concept of "*desired*" risk (Machlis and Rosa, 1990). This is where the public seek out thrilling, but risky, experiences such as hang gliding or bungee jumping. This definition on risk implies a convex utility function, which is consistent with risk-loving, instead of the concave specification, consistent with risk-aversion that is more common in economics.

Rosa (1998, p28) suggests a definition of risk referring to uncertain outcomes irrespective of whether they are negative or positive, *"risk is a situation or event where something of human value (including humans themselves) has been put at stake and where the outcome is uncertain."* This definition, however, does not suggest a way to measure risk. Renn et al. (1992) propose that definitions of risk should contain three elements: outcomes that affect what human beings value, uncertainty and a formula to combine both elements. In practice, the specification of each of these three elements is largely dependent on the disciplinary view of the researcher.

Theories on Risk Perception

Risk perception is a judgement that individuals make concerning uncertain events (Pidgeon, 1992). Perception of risk plays an important role in decision making (Slovic and Weber, 2002) and has been of interest to policy makers and researchers for several decades (Sjoberg, 2000). There are many differing approaches to the conceptualisation of risk perception, each of which contributes important arguments to the debate on risk and how risks are perceived. In the Royal Society's 1992 report on risk, risk perception is defined as involving *"people's beliefs, attitudes, judgements and feelings as well as*

the wider cultural and social dispositions they adopt towards hazards and their benefits" (Pidgeon, 1992: 89). In a later contribution, Pidgeon (1998) clarifies that this definition was made deliberately broad to encompass the wide range of multidimensional characteristics of hazards and perception thereof, rather than just an abstract expression of uncertainty and loss.

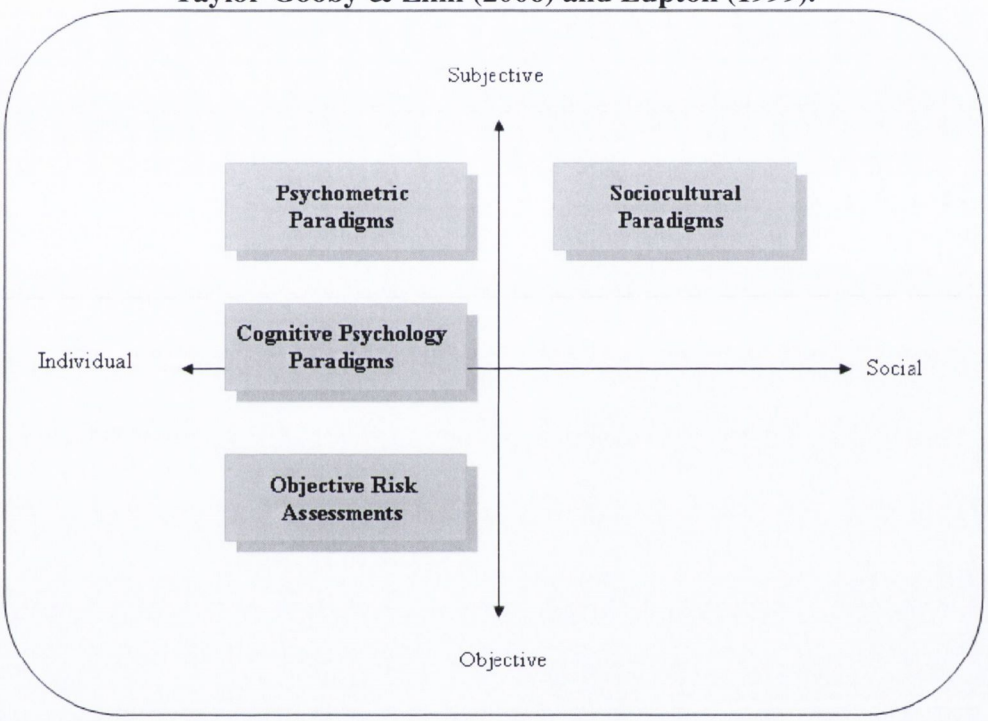
Theories of risk perception can be divided into four paradigms as follows:

1. Theories that portray objective risk assessments;
2. Cognitive psychology theories;
3. Psychometric theories; and
4. Sociocultural theories.

One way to compare the differing approaches to risk perception prevailing in each paradigm is to map them onto two dimensions. The dimensions have been proposed by Renn (2005), Taylor-Gooby & Zinn (2006) and Lupton (1999). The first dimension distinguishes between risks measured at an individual level and risks measured at a social and cultural level in a shared manner across a group. For example, it might be argued that studies within the EUT paradigm typically (though not necessarily) view risk assessment as an essentially individual endeavour whereas sociologists like Douglas (2003) believe that different individuals and groups may judge the same risks differently as they place differing values on a given outcome. The second dimension looks at how risk is interpreted and understood. At one end risks are thought to be real and measurable, as under EUT. They can have an independent existence external to the individual or social group that perceives the risk. At the other end, risks can be thought of as constructionist and subjective. Here the understanding of risk can be a personal/internal construction which can be influenced by social and cultural processes.

In this case, risks will not be perceived by everyone in the same way. Much of the social science research argues that risk is subjective. Slovic (1999: p. 690) suggests that "*risk does not exist "out there", independent of our minds and cultures, waiting to be measured. Instead, human beings have invented the concept of risk to help them understand and cope with the dangers and uncertainties of life.*" Figure 2.2 illustrates where these paradigms lie along subjective-objective and individual-social continuums.

Figure 3.1 Paradigms in Risk Perception Research (adapted from Renn (2005), Taylor-Gooby & Zinn (2006) and Lupton (1999).



3.2 Privacy-Related Decision Making

The common trait of information privacy research that has made use of insights from economics, including those offered by psychologists like Kahneman and elaborated upon by behavioural economists, is the suggestion, implicit or explicit, that privacy is not an absolute but can be assigned an economic value and traded for goods and

services (Posner, 1978) and, ultimately, the idea that informational privacy can be conceptualized as a commodity. In what follows, we will first review how such a perspective emerged in the early IS literature. We will then examine how it is articulated within IS studies that conceptualize decisions concerning privacy in a manner consistent with different paradigms of decision making under uncertainty, i.e. the paradigm that postulates rational and well informed decision makers and the alternative one that allows for limits to rationality and/or to the available information.

3.2.1 Privacy as a Commodity and the Privacy Calculus

Value-based definitions of privacy argue that a call for greater privacy is, fundamentally, antagonistic to the political economy of the information markets (Posner, 1978; Lessig, 2000; Cohen, 2001). In this view, privacy is not an absolute right but is subject to the economic principles of cost–benefit analysis and trade-offs. This view has originated a stream of research regarding privacy as a commodity (Davis, 2010; Johnston, 2012).

Posner (1978) was one of the first to adopt an economic perspective on the modern concept of privacy. He argues that individuals should not have a right to conceal facts about themselves. This conflicts with Warren and Brandeis' (1890) view that people have the right to be let alone. Posner believes that few people truly want to be let alone. Instead, people seek to manipulate the world around them by selective disclosure of facts about themselves. Others, Posner suggests, should not be required to take self-serving claims at face value and should instead be allowed to obtain the information necessary to verify or disprove such claims. He even argues that, at some point,

nondisclosure becomes fraud. He contends that 'prying', or finding out information of a personal nature, enables one to form a more accurate picture of a friend or colleague, and the knowledge gained is useful in social or professional dealings. Additionally, he believes that business and social dealings present opportunities for an individual to exploit others through misrepresenting themselves as better individuals than they really are. In response to this exploitation, others have the right to unmask misrepresentations of that individual (Posner, 1978).

Bennett (1992) further contributed to the formalization of the notion of privacy as a tradable commodity. From this perspective, privacy is still seen as an individual and societal value, but it is no longer an absolute. It can be assigned an economic value and can be considered in a cost–benefit calculation at both individual and societal levels. This calculus, which has become known as the *privacy calculus* (PC), involves weighing the perceived costs against the perceived benefits of the transaction, with disclosure the result of a rational choice when benefits outweigh costs (Wilson and Valacich, 2012). The next section discusses this cost-benefit calculation in detail.

The Privacy Calculus (PC)

The informational privacy and sociology literature conceptualizes the PC by assuming individuals carry out a trade-off calculation based on costs and benefits when determining their course of action. This perspective is found in various sociology and legal studies (e.g., Klopfer and Rubenstein 1977; Laufer and Wolfe 1977; Posner 1981; Stone and Stone 1990) that, consistent with an economic perspective, view privacy not

as an absolute but as subject to interpretation and negotiation (Klopfer and Rubenstein, 1977). For example, as put by Stone and Stone (1990, p.363), "*individuals are assumed to behave in ways that they believe will result in the most favourable net level of outcomes*".

In the presence of uncertainty over outcomes of privacy-related decision, this literature implicitly or explicitly assumes individuals weigh outcomes by their likelihood and the cost-benefit trade-off boils down to a trade-off between some definition of risk[3] and (expected) reward, with the latter defined as benefit from the transaction net of any cost not already included in the definition of risk. Therefore, the more modern literature on the PC suggests that, when requested to provide personal information, individuals perform a risk–reward analysis to assess the outcomes of the disclosure, and respond accordingly (Culnan, 1993; Milne and Gordon, 1993; Milne and Rohm, 2000; Chellappa and Sin, 2005; Dinev et al., 2006; Hui, Teo and Lee, 2007; Hann, Hui and Lee, 2008; Xu et al., 2009).

In this setup, assuming a risk-averse decision maker, the term privacy risk can be used to refer to the broad costs of the decision under conditions of uncertainty and the risk-reward equation describing the trade-off between risk and reward becomes the relevant equation specifying the trade-off between costs and benefits of the decision. Privacy risk lies on one side of such risk-reward equation and some notion of benefit lies on the other side. Given the specific definition of risk and benefits adopted by a given instance of the PC model, then, it should be in principle possible to interpret the model itself as a

[3] An individual's calculation of risk involves an assessment of the likelihood of negative consequences as well as the perceived severity of those consequences (Peter and Tarpey, 1975). The negative perceptions related to risk may affect an individual emotionally, materially, and physically (Moon, 2000).

specialized version of one of the models of decision making under uncertainty reviewed in the previous section, i.e. either those within the neoclassical paradigm or those belonging to the behavioural economics tradition.

Figure 3.2 overleaf summarizes the main constructs, and relations thereof, of the PC model, as it emerges from the above review of the relevant literature. Panel A of the figure offers a more traditional representation of the PC, as it is typically found in IS studies, whereas Panel B offers a representation that makes more direct use of constructs from theories of decision making under uncertainty reviewed earlier, which can be seen as one of the theoretical underpinnings of the model. Panel A emphasizes the effect of privacy concerns, which is a construct that has received great attention in the privacy literature, on the decision concerning whether to disclose personal information. Panel B emphasizes instead the effect of perceived risk and risk aversion antecedents on these two key constructs as well as the effect of the latter of the decision on whether to disclose personal information.

In both Panels, it is shown that, based on available information acquired through learning about the online counterparty and the online environment, the individual forms beliefs about the benefits of the transaction as well as concerns about privacy, which are a function of both the perceived riskiness of the transaction and of the individual's attitudes towards risk (summarized by his/her risk aversion). As explained in Appendix B, perceived risk and risk aversion can be seen as the two key antecedents to privacy concerns, i.e. an individual who perceives greater privacy risk and is more adverse to it will report greater privacy concerns, and the other antecedents typically considered by the literature, can in turn be seen as antecedents to either perceived risk or risk aversion.

We therefore refer to perceived risk and risk aversion as immediate antecedents to privacy concerns and label other antecedents, including the other ones hitherto considered by the privacy literature, as mediated antecedents to privacy concerns. In this setup, the effect on information disclosure decisions of perceived control and trust, as well as attitudes to either the former or the latter is mediated by their influence on either perceived risk or risk aversion.

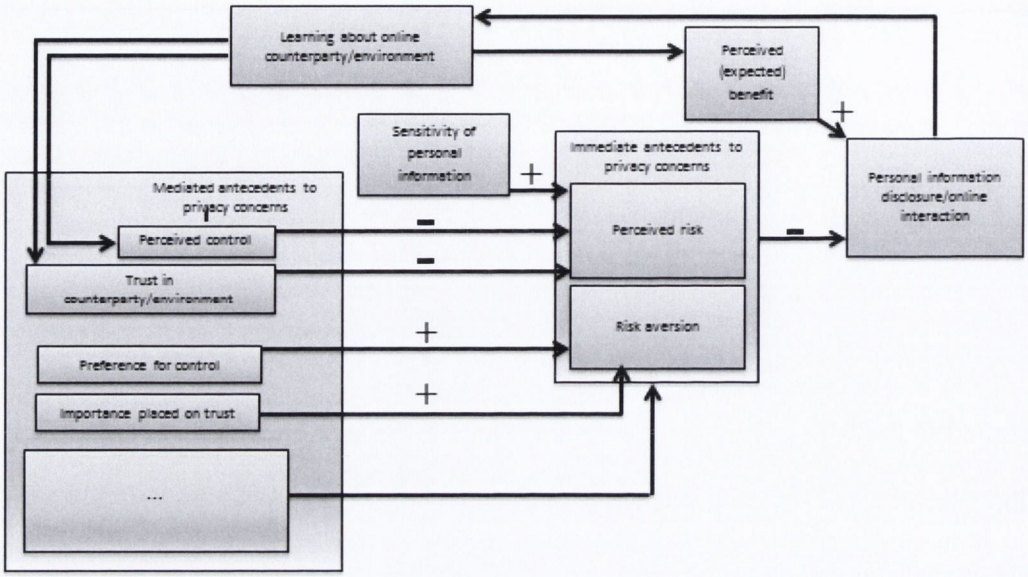
This is made explicit in the flowchart in Panel B of the figure, where it is shown that the individual uses available information to form his/her perception of the benefits and of the riskiness of the interaction in the situation under consideration, having preliminary formed a perception of the control exerted over his/her personal information and of the trustworthiness of the counterparty. The decision whether to disclose personal information so as to interact online then depends on the individual's risk aversion, which in turn depends on the individual's preference for control and importance placed on trust, as well as on the sensitivity of the information that needs to be shared to interact online. In both Panel A and B, however, the flowcharts allow for other inexplicitly modelled influences, for example other mediated antecedents or biases in the assessment of the risks and benefits of the interactions. Much of the literature on IS privacy concerns does not explicitly model such influences but does not rule them out either. The exceptions, that will be discussed shortly, include, on the one hand, studies that assume essentially full rationality in privacy-related decision making, thus explicitly or implicitly relying on EUT, and, on the other hand, studies that explicitly allow for limits to rationality and behavioural cognitive biases.

In any case, the advantage of the representation in Panel B, over the more traditional one offered in Panel A, is that it highlights the different roles of perceived risk and risk aversion. This is useful because perceived risk depends on the situation at hand and can be, in principle, influenced whereas risk aversion is a characterization of individuals' attitudes that are thought to be, at least in the short run, invariant to the specific circumstances of the interaction. That is, a risk-averse person may grow to become more or less so, depending perhaps on life experiences and both socio-cultural and neurobiological influences, but can be taken as given in the short run by an analyst interested in predicting the individual's decision concerning information disclosure and online interaction. This is not the case for perceived risk, which may change depending on circumstances and available information. In the flowchart in Panel B, we also show that trust depends on propensity to trust, which can therefore be seen as a mediated antecedent to trust, risk perception and privacy concern.

Figure 3.2 The Privacy Calculus Model (PC)

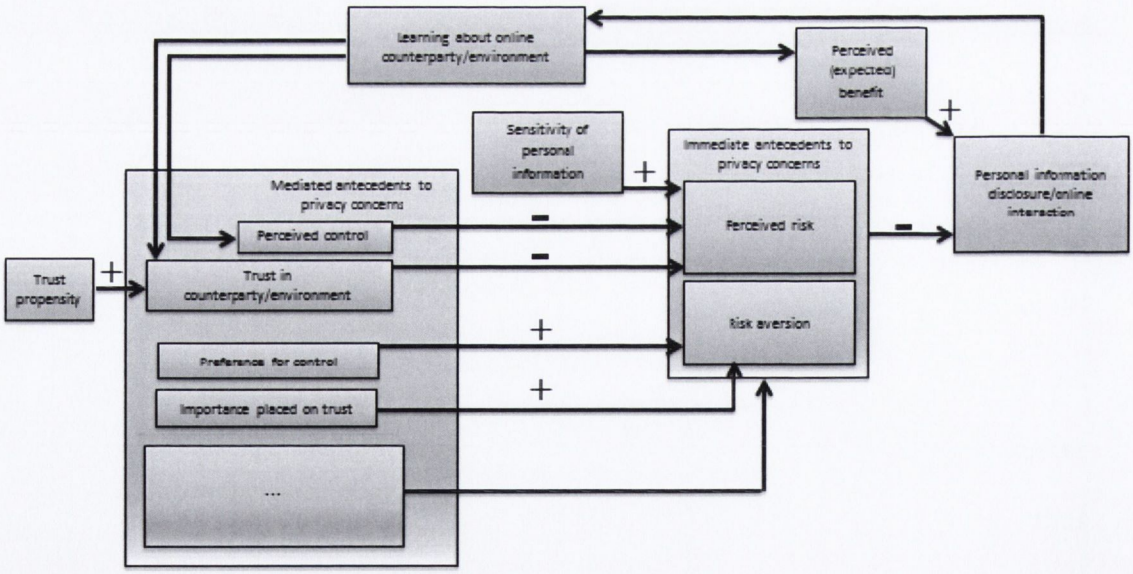
Panel A

(Typical Formulation)



Panel B

(Risk-Based Formulation)



In the PC literature, privacy risk has been defined as the degree to which an individual believes that a potential for loss is associated with the release of personal information to an entity (Featherman, 2003; Malhotra, Kim and Agarwal, 2004). Although privacy concerns have often been conceptualized as a multidimensional construct (Smith et al. 1996; Malhotra et al. 2004), privacy risk has been treated as a construct mainly related to the potential loss of control over personal information (e.g., Dinev and Hart 2006). The literature on privacy has identified sources of privacy risk in organizational opportunistic behaviour, including the selling of personal data to, or sharing information with, third parties, financial institutions (Budnitz, 1998), or government agencies (Preston, 2004; Wald, 2004). A number of e-commerce studies empirically verified the negative effect of perceived risk on intentions to conduct transactions (Budnitz, 1998; Jarvenpaa and Leidner, 1999; Jarvenpaa and Tiller, 1999; Jarvenpaa, Tractinsky and Vitale, 2000; Norberg and Horne, 2007; Norberg, Horne and Horne, 2007; Pavlou, 2003; Pavlou and Gefen, 2004). Additionally, previous studies generally supported the positive impact of privacy risk on privacy concerns (Dinev et al. 2006; Dinev and Hart 2004), and the negative impact of privacy risk on willingness to disclose personal information (Malhotra, Kim and Agarwal, 2004; Xu, Teo and Tan, 2005).

The literature identifies three major components of benefits of information disclosure, namely financial rewards, personalization, and social adjustment benefits. Privacy studies provide empirical evidence that compensating consumers through financial rewards encourages information disclosure (Caudill and Murphy, 2000; Phelps, Nowak and Ferrell, 2000; Hann, Hui and Lee, 2008; Xu, Teo and Tan, 2010). In terms of the value of personalization, Chellappa and Sin (2005) found that the value consumers place on personalization was almost twice as influential as their concerns for privacy

when determining usage of personalization services. White (2004) found that users are more likely to provide personal information when they receive personalization benefits. A study by Lu et al. (2004) demonstrated that social adjustment benefits (defined as the establishment of social identity by integrating into desired social groups) can also have an effect on willingness to disclose personal information.

The Privacy Paradox

There is evidence that individuals often express privacy concerns but behave in ways that seemingly contradict their stated level of concern about privacy (Acquisti and Grossklags, 2005; Acquisti, 2004; Norberg, Horne and Horne, 2007). For example, Sheehan and Hoy (1999) found that stated privacy concerns are negatively correlated with the reported frequency of registering with websites in the past and positively correlated with providing incomplete information during registration. Norberg et al. (2007) found that, for all information categories (personal identification, financial, preferences, demographic, etc.), the level of actual disclosure significantly exceeded individuals' intentions to disclose information. This contradiction between individuals' intentions and actual behaviour has been termed "the privacy paradox" by some researchers (Barnes, 2006; Brandimarte, Acquisti and Loewenstein, 2012; Norberg, Horne and Horne, 2007; Wilson and Valacich, 2012).

Some studies place less importance on the privacy paradox. For example, Smith et al (2011) point out that it is quite common for researchers to measure stated intentions instead of actual behaviour, inferring through references to the theory of reasoned action (TRA) (Fishbein and Ajzen, 1975) that behaviour will match actual intention. If there is

truly a privacy paradox, they argue, this appeal to TRA may be misguided. More generally, they contend that associations between privacy concerns and stated intentions may not be reflective of actual behaviours.

Wilson and Valacich (2012) argue that prior literature that addresses the privacy paradox is limited in two ways. Firstly, like Smith et al. (2011), they point out that the overwhelming majority of empirical privacy research has only captured intentions to divulge personal information, stopping short of recording and comparing actual privacy-related disclosure behaviour. Secondly, they argue that the majority of IS literature concerning the PC has treated the situation specific calculus decision as a rational one, without considering situational factors that might induce non-rational behaviour. The exception to the focus on rational decision-making is the work of Acquisti and colleagues (Acquisti 2004; Acquisti and Grossklags 2003; Acquisti and Grossklags 2005; Tsai et al. 2011), wherein decision-making surrounding privacy disclosure is assumed to be less than fully rational.

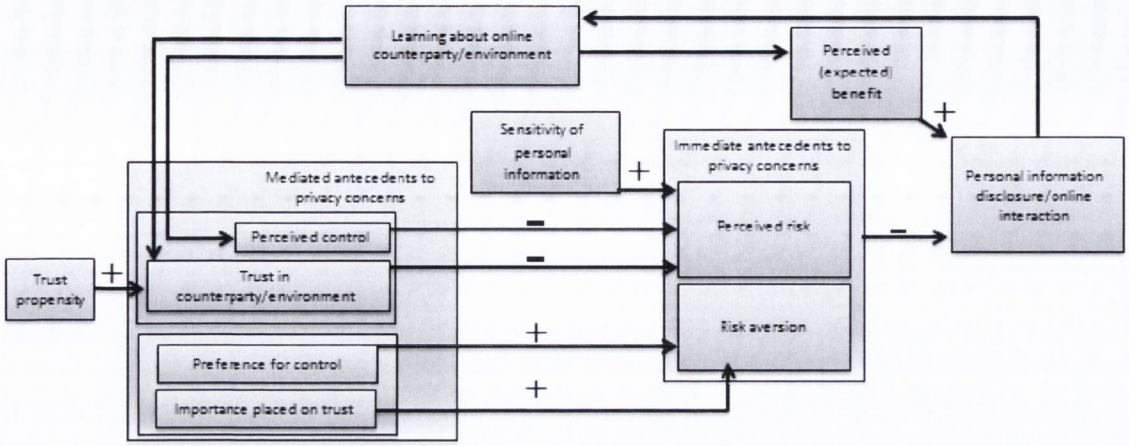
3.2.2 The Privacy Calculus (PC) and EUT

According to EUT, and therefore consistent with the rational decision making paradigm, users should behave in rational ways that maximize expected utility, which is assumed to be an increasing function of expected benefits and a negative function of expected costs and risk. This assumption underlies previous IS research in which the so called *PC* has been modelled and studied. Dinev and Hart (2006) make this assumption specifically in the context of information disclosure on the Internet and cite Culnan and Bies (2003), who argue that "*individuals will disclose personal information if they*

perceive that the overall benefits of disclosure are at least balanced by, if not greater than, the assessed risk of disclosure" (Dinev and Hart 2006, p. 62). A number of models from previous IS privacy research, which have found considerable empirical support, have largely adopted the assumption that users behave rationally when evaluating the costs and benefits of disclosure (Dinev et al., 2006; LI and Keshelashvili, 2006; Xu et al., 2009).

Figure 3.3 below shows a flowchart representing a formulation of the PC model consistent with theories of decision making under uncertainty from within the rational paradigm. The difference between the flowchart in Figure 3.3 and the previous one, namely the one in Panel B of Figure 3.2, is that the model to which the latter refers rules out any influence on privacy concern that cannot be conceptualized as antecedents to either risk perception or risk aversion. In particular, the model rules out the influence of risk assessment error on privacy concern.

Figure 3.3 The PC Model under EUT-Rational Decision Making



3.2.3 Behavioural Economics Insights on the PC

Acquisti and colleagues (Acquisti and Grossklags, 2003; Acquisti, 2004; Acquisti and Grossklags, 2005; Acquisti, 2009), challenge the assumption that users behave rationally when evaluating the costs and benefits of disclosure. Their research uses a behavioural economics perspective and suggests that the privacy paradox is the result of such limitations as psychological distortions (e.g., hyperbolic discounting of risks), limited or asymmetrical information (which implies that users do not know the full implications of disclosure, or at least they do not know it to the extent to which providers of IS technologies and services do), and bounded rationality (i.e., the inability to accurately process all of the probabilities and amounts of benefits and costs related to privacy disclosure) (Acquisti and Grossklags 2003). It is because of these limitations, it is argued by these authors, that users have the tendency to supply private information in return for relatively small conveniences or rewards, even when their stated privacy concerns do not support this behaviour.

As seen in the previous section, this seemingly incoherent behaviour is known as the *privacy paradox* (Acquisti and Grossklags, 2005). This paradox, i.e. the circumstance that stated attitudes towards disclosure of private information do not match disclosure behaviour, remains a puzzling empirical regularity though the evidence concerning its occurrence is largely survey-based, and as such pertaining to self-reported disclosure behaviour, in that almost no study has examined actual disclosure behaviour (Smith et al. 2011). Previous research has considered situational factors evaluated within the PC model in an attempt to explain the paradox (Dinev et al., 2006; LI and Keshelashvili, 2006; Van Slyke et al., 2006), arguing that users rationally evaluate the costs and benefits associated with a specific disclosure decision and that, in certain situations, it is possible for general privacy concerns to be overridden in order to achieve the perceived benefits of disclosure. The assumption that this overriding behaviour is purely rational, however, has been challenged and support has been found for circumstances that cause users' disclosure behaviour to be at least partially irrational (Acquisti and Grossklags 2005a).

Acquisti (2004) highlights a number of difficulties that distinguish individual privacy decision making from that prescribed by classical rational choice theory. First, privacy choices are affected by incomplete information and in particular asymmetric information (data subjects often know less than data holders about the magnitude of data collection and the use of shared or collected personal data). Individuals also know little about associated consequences. Second, the complex life-cycle of personal data in modern information societies can result in a multitude of consequences that individuals are hardly able to consider in their entirety (as human beings, because of humans' innate bounded rationality (Simon, 1957), we often replace rational decision making methods

with simplified mental models and heuristics). Third, even with access to complete information and cognitive power to process it exhaustively, various behavioural anomalies and biases could lead individuals to take actions that are systematically different from those predicted by rational choice theory (Acquisti & Grossklags, 2008).

Incomplete information is relevant to privacy-related decision making for two reasons (Acquisti & Grossklags, 2008). Firstly, individuals have some control over the level of access that other entities have to their personal sphere. For example, an individual's personal data may be concealed from other people's knowledge. Other people may thus have to rely on incomplete information when interacting with that individual. This is the interpretation of privacy as "concealment" that Posner recognized (Posner, 1978). Secondly, incomplete information affects individuals whenever control over their personal or informational sphere is limited or not clearly determinable. For example, information asymmetries often prevent an individual from knowing when another entity has gained access to or used their personal information; in addition, the individual may not be aware of the potential personal consequences of such intrusions. The related difficulties in exercising adequate control over private information have been exacerbated in highly networked, digitized, and interconnected information societies (Varian, 1997).

On a related note, Varian (1997) points out that an individual has little or no control over the secondary use of their personal information, and hence may be subject to externalities whenever other parties exchange their personal data (Varian, 1997). This sense in which incomplete information creates uncertainties relating to privacy is not new in the economic or legal literature on privacy (Acquisti and Grossklags, 2008).

Uncertainty complicates privacy decision making because of the resulting mathematical complexity of evaluating privacy costs and benefits of transactions. For example, individuals have to consider multiple outcomes and associated probabilities rather than purely deterministic outcomes. The complexity of the privacy decision environment leads individuals to arrive at imprecise estimates of the likelihood and consequences of adverse events, and sometimes overlook privacy threats and modes of protection (Acquisti and Grossklags, 2005).

3.2.3.1 Privacy Risk Taking under Bounded Rationality

Consumers may become overwhelmed with the task of identifying possible outcomes related to privacy threats and the means for protection (Acquisti & Grossklags, 2008). Even more so, they may experience difficulties in assigning accurate likelihoods to those outcomes. Policy makers often suggest that providing more information to consumers will help them make better decisions. Such additional information may be provided by commercial entities, e.g., anti-spyware vendors, by consumer advocacy groups, or by peers. However, even if individuals had access to complete information, they may often be unable to process and act optimally on large amounts of data (Acquisti and Grossklags, 2008). Especially when faced with complex decisions regarding the protection or release of personal information. Individuals' innate bounded rationality limits their ability to acquire, memorize and process large amounts of information, and forces individuals to rely on less complex mental models, approximate strategies, and heuristics when making decisions about their informational privacy (Sheffrin, 2002).

Bounded rationality problem solving strategies, typically relying on heuristics or experiential learning rules, adopt qualitative evaluations and solutions to decision making problems that, unlike in models that belong to the rational decision making paradigm, stop short of perfect (numerical) optimization (Acquisti and Grossklags, 2008). Acquisti and Grossklags (2005), through a survey of privacy attitudes and behaviour, demonstrated the presence of simplified mental models that are employed by individuals for protecting informational privacy when making decisions. They found that a number of survey participants confused security and privacy issues when they reported feeling that their privacy was protected by merchants who offered SSL connections to complete online payments. Similarly, Turow et al. (2006) showed that the presence of a privacy policy on a website may be taken by many individuals to represent privacy protection regardless of its content. Another study by Moores (2005) showed that a privacy seal may be interpreted as a guarantee of a trustworthy website. Consumer advocates might suggest that providing individuals with clearly phrased advice or pre-processed information, for example, to avoid a specific product or activity, will help overcome problems of information overload and bounded decision making. Nevertheless, consumers may still use this data in ways which are different from that of expected utility maximization or contradict their own best interest. Good et al (2007) found evidence that even well-presented notices of dangerous behaviours of computer programs (e.g., spyware) may not always lead individuals to abort or regret software downloads. Similarly, Spiekermann & Grossklags (2005) found that individuals' behaviour in an interactive online shopping episode was not significantly affected by substantially modifying the privacy statement of the website.

These studies show that individuals are influenced by additional factors that add to the complexity of determining risks and uncertainties associated with privacy threats (Acquisti & Grossklags, 2008). For example, Tversky and Kahneman (1981) show that the way a problem or question is framed affects how individuals respond to it. Good et al (2006) describe results suggesting that potentially unwanted privacy and security practices discussed in a privacy notice and written in vague language might be considered less intrusive by consumers than a detailed description of possible dangers. Acquisti and Grosslags (2005) conduct a survey detailing how individuals' willingness to accept or reject a company's offer is affected by the presence of uncertainty and ambiguity. The findings show that individuals' willingness to accept the company's offer is negatively affected by the perceived presence of uncertainty and ambiguity.

Tversky, Kahneman, and others have highlighted a number of heuristics that guide individual decision making more than rational choice processes (Kahneman and Tversky, 1972; Sheffrin, 2002). In this context, a heuristic is some technique that helps learning or problem-solving. For example, individuals often anchor on a specific valuation of a good or service, and then adjust that valuation when new information becomes known (Sheffrin, 2002). The value that individuals assign to their own personal information may in fact be assigned through anchoring on a focal and possibly arbitrary value: it is very difficult for an individual to "price" their own information but once a price has been found (perhaps completely arbitrarily, or perhaps by anchoring it to the reward received by a merchant in exchange for that information) it is likely that the consumer's valuation of their own personal data will thereafter orbit around that value (Acquisti and Grossklags, 2008). Other heuristics may also be found in privacy decision making. For example, individuals may tend to discount as improbable those

events that are difficult to picture mentally, such as identity theft (an example of the simulation heuristic (Kahneman and Tversky, 1982)); or may associate trustworthy behaviour with the neat appearance and design of a website (an example for the representativeness heuristic (Sheffrin, 2002)).

3.2.3.2 Privacy Risk Taking and Knightian Uncertainty

From the perspective of individuals having bounded rationality, it is argued that disclosure sometimes occurs as the result of users being unable or subconsciously unwilling to accurately consider the associated privacy risks (Acquisti and Grossklags, 2005). The work of Acquisti and Grossklags also introduces the concept of Knightian uncertainty in the informational privacy literature, as seen in earlier literature. The distinction between risk and Knightian uncertainty can be traced back to the early economics literature.

As noted earlier, individuals assessing the entirety of the damage resulting from privacy breaches will be anchored to the initial judgement of riskiness, and any adjustments based on new evidence will be biased towards such initial judgement. Therefore, decision making processes involving any of the heuristics outlined by Sheffrin (2002) may reflect both cognitive and emotional elements.

In the context of privacy related decision making, this type of uncertainty may arise when individuals perceive that they do not have enough knowledge about how their personal information will be stored and processed/used, to the extent that they cannot quantify the risk involved in submitting their personal information online. In this

situation, individuals perceive Knightian uncertainty or ambiguity. The terms Knightian uncertainty and ambiguity can be used interchangeably to refer to circumstances in which probabilities and payoffs associated with a given event (e.g., an exchange) are neither known nor knowable with precision (Knight, 1921).

Submitting personal information online is, arguably, an ambiguous situation in many instances, given the dearth of knowledge regarding how that information will be processed and stored by third parties. In addition to this, many people do not get formal training before going on the Internet for the first time. They simply log on and find things out for themselves (Varian, 1997). As implied by the financial world put forth by Sheffrin (2002), in such circumstances people employ various techniques, i.e. rules of thumb and inferences from the information at their disposal, when making decisions. These heuristics or rules of thumb can introduce biases into decision making processes.

However, society has not left it entirely up to the individual to protect his/her informational privacy. Governments around the world have already put in place certain safeguards to help individuals protect themselves when online. As already noted in this dissertation, data protection legislation has been implemented in many countries and the European Union has passed a number of directives over the last number of decades to enforce stricter protections on for EU citizens' personal data. Likewise, numerous software development organisations have taken on the challenge of developing systems that protect individuals' informational privacy within the system (London Economics, 2010). In recent years, the European Commission has funded a number of research projects that examine various approaches to protecting individuals' informational privacy (ABC4Trust Project, 2009; PICOS, 2007).

Acquisti and Grossklags (2005) argue that when presented with privacy-related problems, individuals face a number of uncertainties. Firstly, an individual often has only a vague and limited knowledge of the actions they can take to protect their personal information. They have limited knowledge of the possible or actual actions undertaken by others. For example, they have limited knowledge of a company's reasons for collecting their personal information. Secondly, actions taken by the individual (whether as an attempt to protect or trade information) or by another stakeholder often have unpredictable results. For example, it is often unknown whether contact information that has been submitted to a company will be used for unsolicited communication or whether past consumption data will be used for price discrimination strategies. Thirdly, possible states of nature (with associated actions and consequences) may be unknowable in advance, because these states depend on future, unforeseeable events and/or environmental changes (Acquisti & Grossklags, 2008). Fourthly, the more an individual reflects upon a privacy choice before taking action, the more they understand the consequences of that choice and consequently they often decide upon a different course of action than if they had not reflected upon the choice. For example, Acquisti and Grosslags (2005) describe how people change their opinion of which parties should have access to their credit card transactional data the more they are prompted for an answer. Their findings show that individuals sometimes ignore both privacy risks and forms of protection, and even when they are aware of them, they often miscalculate the probability, in terms of financial implications, of the privacy risks occurring.

Finally, Acquisti and Grosslags (2005) point out that privacy protection or invasion is often a by-product of another (and sometimes unrelated) transaction, as acknowledged by the PC literature. This can be seen as a trade-off between privacy and other benefits. The benefit of privacy protection is often linked with other benefits in a complex mix. For example, when an individual purchases a book online (thus saving time), they often have to reveal their credit card details to the online merchant, which may lead to an increased risk of identity theft. Or, in order to receive a monetary discount from a grocery store, they reveal their buying patterns by using a loyalty card, which may increase their probability of receiving junk mail. Comparisons between these benefits are difficult to make because of their interdependent nature. Acquisti & Grosslags (2008), thus, conclude that an individual facing privacy sensitive scenarios may be uncertain about the values of possible outcomes and their probability of occurring, and that sometimes individuals may not even be able to form any beliefs about such values and probabilities. In fact, they may have no knowledge of the possible outcomes of a certain situation since the states of nature may be unknown or unknowable in advance. As a result individuals may sometimes ignore both privacy risks and forms of protection.

3.2.3.3 Soft Paternalism or Nudging in Informational Privacy Protection

Balebako et al (2011) argue that in recent years, there has been growing interest in using lessons from behavioural economics to influence and ameliorate decision making in situations where cognitive and behavioural biases may adversely affect the individual (Loewenstein and Haisley, 2008; Thaler and Sunstein, 2008). This approach is often referred to as soft or asymmetric paternalism, or with the more popular term "nudging."

Soft paternalism aims at countering and overcoming those biases, so as to assist individual decision making (Balebako et al., 2011).[4]

Findings from behavioural economics and behavioural decision research have highlighted challenges in human decision making that lead, sometimes, to undesirable outcomes (Wang et al., 2013). The challenges are often due to lack of information or insight, cognitive limitations and biases, or lack of self-control (Thaler and Sunstein, 2008). Because of those challenges, individuals sometimes make decisions that they later regret. These may include decisions to protect too much, or not enough, personal information (Acquisti and Grossklags, 2005). A number of researchers have investigated or advocated soft paternalistic interventions to help individuals overcome those biases, and nudge them toward behaviour that may increase their welfare (Thaler and Sunstein, 2003; Acquisti, 2009; Balebako et al., 2011). The application of soft paternalistic techniques to online privacy (and security) problems may help users make better online decisions, and avoid regrets (Wang et al., 2013).

Paternalistic policies try to solve decision-making challenges by mandating decisions for individuals. Such policies are often heavy-handed and may generate unintended consequences (Loewenstein and Haisley, 2008). Soft paternalism, on the other hand, avoids coercion; it seeks to steer users in a direction (believed to be more desirable to

[4] Balebako et al. (2011) argue that, as mobile devices and applications become pervasive, privacy risks for users also grow. The accessibility and ease of use of these devices make it easy to broadcast personal information at any time, from anywhere, to friends and strangers. They argue that, while users benefit from and enjoy such streams of information sharing, they also expose themselves to tangible and intangible risks such as the risk of being tracked by commercial entities interested in exploiting users' personal information for profit, surveillance or even being stalked by malicious parties (Balebako et al., 2011). Balebako et al, (2011) also claim that it is difficult for individuals to determine the optimal balance between revealing and hiding personal data. Sometimes individuals are not even aware that information about them is being broadcast, shared, or monitored; other times, while aware of on-going information flows, they do not understand the consequences, or properly assess the risks.

the user as it is based on their own prior judgement, or on external empirical validation), without impinging on their autonomy. A soft paternalistic solution, for instance, would consist of making an individual aware of the biases, lack of information, or cognitive overload that may affect their decision (Balebako et al., 2011).

Nudges are tools of soft-paternalism, and may be used to ameliorate privacy (as well as security) decision making (Acquisti, 2009). In the case of insecure communication channels, or covert data collection, a nudge may take the form of an alert that informs the user of the risk. In the case of mobile devices that store sensitive information (which could be accessed by strangers if the device was misplaced), a nudge might discourage users from storing private data on mobile phones. When information is being disclosed through a smart-phone, nudges may provide alerts about the recipients, contexts, or type of data being shared (Balebako et al., 2011). Many different types of nudging interventions are possible. Some simply consist of informing the user, in which case they relate to privacy research on informed consent. Some focus on making systems simpler to use, in which case, privacy nudges fall into the realm of research on privacy usability. However, other nudges aim at countering specific cognitive and behavioural biases, such as neutralizing the detrimental effects of immediate gratification biases in privacy decision making by altering the individual's perception of the sequence of costs and benefits associated with revealing sensitive information (Acquisti, 2004).

The literature on soft paternalism applied to privacy decision making is in its infancy, and therefore scarce (Balebako et al., 2011). However, a number of recent studies and products focus on mechanisms that may be categorized as nudges. The IS privacy literature offers some examples of these approaches. For example, recent experimental

research has shown that users are interested in protecting their privacy and may even pay for it if appropriate tools and easy to understand privacy policies are provided (Tsai et al., 2011). One series of studies explored the impact of making information about privacy practices on web sites more accessible to buyers (Egelman et al., 2009). The results showed that online customers are more likely to shop online from websites that exhibit more protective privacy policies. Additionally, those customers are willing to pay a premium for privacy. Furthermore, privacy indicators displayed at the moment an individual is shopping online may have an impact on consumer decisions (Egelman et al., 2009). In particular, they increase the willingness to pay for privacy; however, if the indicator is provided only after the shopper has already chosen the website from which to buy, the user will not change their already-made decisions (Egelman et al., 2009). Egelman et al. (2009) found that timing was essential when trying to help people to protect their privacy.

Another study found that simply questioning Facebook users about their online disclosure behaviour and the visibility of their Facebook profiles was sufficient to trigger changes in their disclosure behaviour (Gross and Acquisti, 2005). Application interface design is also important, and should help users notice when changes in context generate changes in information flows and then help them to maintain their privacy (Hull, Lipford and Latulipe, 2011).

Examples of industry products or solutions that influence decision making in relation to privacy take various forms, some provide protection to the user and others encourage them to disclose more information about themselves. Some of these solutions may be interpreted as soft paternalistic for privacy protection, in the sense that they nudge

towards privacy. They include privacy/security usability solutions, simplifications of privacy settings, or tests and delays before one can post information (Wang et al., 2013). More frequent, however, are the examples of products and solutions that nudge individuals to give up even more of their privacy, surrendering sensitive information. These include privacy defaults that are that allow the collection of personal information, a lack of usability in privacy settings interfaces and rewards for sharing data or encouraging friends to share data (Balebako et al., 2011).

In order to help individuals avoid regrettable online disclosures, Wang et al (2013) employed lessons from behavioural decision research and research on soft paternalism to design mechanisms that "nudge" users to consider the content and context of their online disclosures before posting them. They developed three such privacy nudges on Facebook. The first nudge provided visual cues about the audience for a post. The second nudge introduced time delays before a post was published. The third nudge gave users feedback about their posts. Wang et al (2013) tested the nudges in a three-week exploratory field trial with 21 Facebook users, and conducted 13 follow-up interviews. Their results suggest that privacy nudges could be a promising way to prevent unintended personal information disclosure.

3.3 A Synthesis of the Privacy Calculus (PC) Model and Behavioural Economics Insights: the Revised Privacy Calculus (RPC) Model

In this section, we seek to synthesis the work that has been reviewed so far in this chapter and put forth a revised privacy calculus (RPC) model which takes into account

research into bounded rationality and informational privacy decision making in the face of uncertainty, including ambiguity. In what follows, we use Westin's definition of informational privacy. According to this author, and as already seen in the literature review in chapter 2, informational privacy is

> *"the claim of an individual to determine what information about himself or herself should be known to others...This also involves when such information will be obtained and what uses will be made of it by others" (Westin, 2003, p431).*

We interpret online interactions as transactions that involve some uncertain prospect of threat to privacy and some attendant loss[5] that may be suffered by an individual following the release of personal information to an external entity (e.g., an organization, a firm, another individual) and therefore following the debasement, partial or otherwise, of the claim at the heart of the definition of Westin's definition of informational privacy. From the standpoint of this definition, it is possible to view the decision of whether to interact online, thereby in principle putting privacy at risk, as a decision under a condition of uncertainty.

Following the literature on limits to rationality and insights from the psychology and behavioural economics literature, which were reviewed in a previous section of this chapter, we conceptualize individuals as possibly imperfect processors of information who are subject to bias, error and perceptual illusions when making decisions (Sheffrin,

[5] Here, loss is defined broadly, as any undesired outcome (resulting from the disclosure of personal information).

2002; Acquisti and Grossklags, 2008). Following Kahneman and Tversky (1972), we also allow for the possibility that individuals, when coping with their limits to rationality, resort to bias-prone heuristics. Here, the term heuristic is used to refer to the process by which people find things out for themselves, typically by trial and error (Pearl, 1983). Trial and error leads people to develop rules of thumb, following Sheffrin (2002), which may be biased and lead to sub-optimal decisions based on systematic judgement errors, i.e. on a biased assessment of costs and benefits. Furthermore, we allow for the possibility that such bias-prone heuristics may be used by essentially rational decision makers to cope with ambiguity (or Knightian uncertainty), as an alternative to disengagement. That is, in our conceptual framework for understanding individuals' decisions on whether or not to disclose personal information online, we allow for two qualitatively different types of limits to human rationality:

- Inability to assign probabilities to all possible outcomes, which may result in ambiguity or perception thereof

- Cognitive error in the assignment of probabilities to possible outcomes, possibly due to the use of bias-prone heuristics, leading to a systematically[6] wrong assessment of the risk-reward trade-off of online risky prospects

It is worth noting that a subjective rather than objective notion of ambiguity (or Knightian uncertainty) enters the definition of the first type of the limits to rationality listed above. That is, unlike in the standard definition of ambiguity, we do not require it

[6] The circumstance that the error may be systematic is important as it implies that it cannot be dismissed as being, on average, irrelevant.

to be impossible to assign probabilities to outcomes, but simply that the particular decision maker under consideration is not able to do so or at least perceives an inability to do so. This subjective definition of ambiguity is relevant to information disclosure in an online and ICT-mediated setting because, for example, the typical IS user often does not know how to assess the risk that another entity gains access to or uses his/her personal information once it is submitted online (Varian, 1997), whereas an especially experienced and IS-savvy user might know this better. It is by definition impossible to quantify ambiguity and, in the context of IS usage, it might not be possible or useful to define it in objective or absolute terms, but decision makers would perceive it in circumstances in which they felt aware of their own inability to assign probabilities to outcomes of interest.[7] In such circumstances, subjectively defined ambiguity would have the same implications for decision making as objective ambiguity.

Accordingly, we interpret decision-making concerning privacy and disclosure of personal information as an instance of decision-making under different degrees of uncertainty. In accordance with Sheffrin (2002), we classify uncertain events that may occur in on-line and IS-mediated interactions in two categories: risky and ambiguous events. Risky events are those for which individuals can assign a known or knowable probability to each possible outcome. Ambiguous events are those for which such assignment is impossible, either because the probabilities are unknown/unknowable or because one or more possible outcomes are not known/knowable, and therefore are characterized by a qualitatively different type of uncertainty, i.e. Knightian uncertainty. Hence, the term uncertainty is reserved in this research to denote situations

[7] An individual's calculation of risk involves an assessment of the probabilities of negative consequences occurring as well as the perceived severity of those consequences once they occur (Peter & Tarpey, 1975).

characterized by *quantifiable* risk and ambiguity as situations characterized by *unquantifiable* risk, i.e. Knightian uncertainty. At one end of the spectrum, therefore, there are situations characterized by complete or near complete certainty of outcomes whereas at the other end there are situations characterized by considerable uncertainty, with ambiguous situations that can be seen as being characterized by infinite (in a sense, unquantifiable) levels of uncertainty.

Consistent with EUT, with IS studies that adopt the PC model and with a large portion of behavioural models of decision making under uncertainty, we assume that, when *limits to rationality* are *not binding*, IS users make decisions by choosing the course of action that maximizes the expectation of a well-defined utility function. Unlike under the rational decision making paradigm but consistent with the behavioural economics perspective, however, we allow for the possibility that *limits to rationality* are *binding*, either to an extent that leads the IS user to resort to heuristic decision making rules (to 'save on scarce rationality') or to an extent that leads the user to perceive the situation as *ambiguous*. Following the behavioural literature, and especially the work of Sheffrin (2002), we allow for the possibility of systematic error in assigning probabilities to outcomes when the user is subject to limits to rationality and resorts to heuristics.[8] Following the literature on Knightian uncertainty/ambiguity, we posit that the user disengages when he/she perceives ambiguity.

[8] Gilowich et al. (2002) note that using "common sense" generally works to make sense of the world and advocate adaptive behaviour and that, in general, causes resemble effects and appearances are usually very good indicators of reality. In less predictable circumstances, however, people often lack an intuitive feel for probabilistic processes and rely on mental heuristics or their common sense to guide their judgements that can lead to predictable biases such as representative bias, availability bias or anchoring and adjustment. Based on the argument of Gilowich et al (2002), using common sense leaves individuals vulnerable to biases occurring in their judgement, leading them to become more vulnerable in their decision making processes.

Consistent with a lot of the IS literature on the PC, this implies that the IS user evaluates a certain risk-rewards trade-off, which in turn implies certain preferences, perhaps summarized by a utility function of a similar mathematical object, and a certain way to combine preferences with an assessment of the probabilities of outcomes, e.g. the expectation of the utility function or a mechanism with a similar effect (e.g., the expectation of the utility function taken over the possible outcomes or mechanism with a similar function, e.g., the expectation over the 'weighted' gains and losses considered by Kahneman and Tversky (1979).

We assume this to result in a ranking of choices concerning online behaviour that is a positive function of the expected benefit and a negative function of risk. As it can often be the case in the PC literature, preferences are not specified any further. In accordance with this approach and as explained in the previous section, we define privacy risk as the degree to which an individual believes that a potential for loss is associated with the release of personal information to an entity (Featherman, 2003; Malhotra, Kim and Agarwal, 2004). This definition of privacy risk is not derived from an explicit characterization of the decision maker's preferences, as the preferences are not fully specified, but it represents a widely adopted definition in the IS literature. It should be in principle possible to find a specification of preferences, e.g. a particular utility function, which implies this definition of privacy risk. Identifying such specification, however, is outside the scope of the present research but we note that it would represent a worthwhile endeavour for future research.

We also follow the prevailing literature on the PC in defining the reward element of the risk-reward trade-off evaluated by the user. We therefore assume the possible reward to

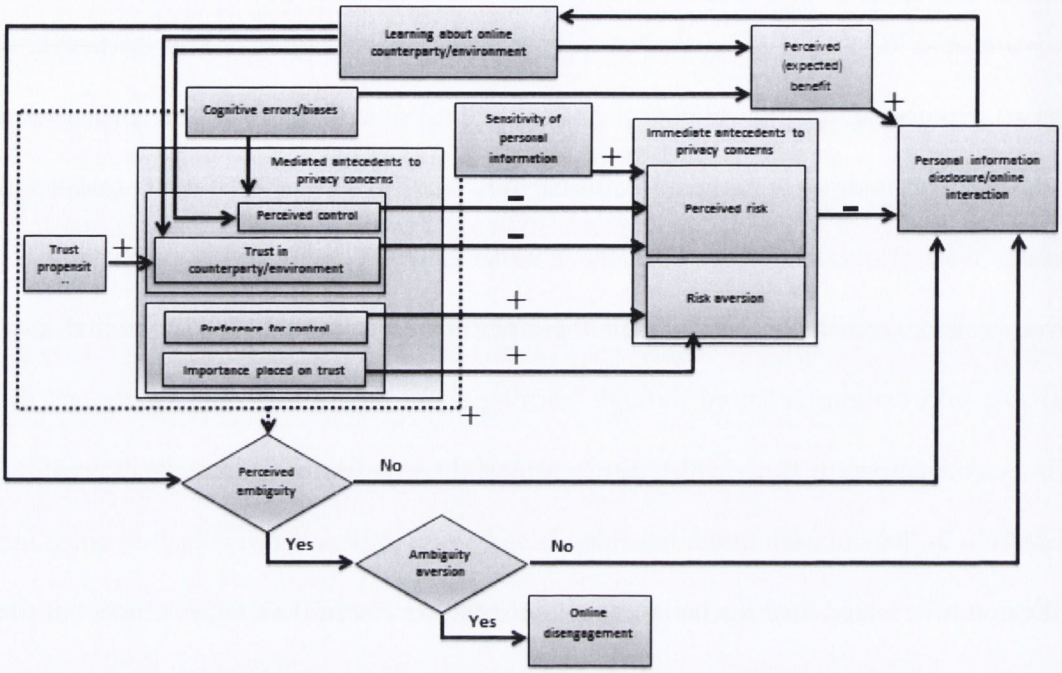
consist of a certain combination of the three main types of benefits of information disclosure, i.e. financial rewards, personalization, and social adjustment benefits. It is worth noting that the fact that the trade-off evaluated by the IS user is a function of financial rewards is coherent with the PC model's tenet that privacy is, to some extent, negotiable, as well as with empirical evidence that compensating consumers through financial rewards encourages information disclosure (Caudill and Murphy, 2000; Hann, Hui and Lee, 2008; Phelps, Nowak and Ferrell, 2000; Xu, Teo and Tan, 2010).

To make the model more complete, and more relevant to our ultimate privacy risk management application, we allow for the circumstance that the decision to disclose and interact online may be mediated by some risk handling behaviour. That is, the individual may decide to undertake risk handling behaviour before deciding to interact, based on his/her own assessment of the expected benefit and risk of the perspective interaction as well as his/her attitudes towards risk and propensity to trust. To model the risk handling decision, we make the realistic assumption that risk handling behaviour is costly, e.g. in terms of administrative costs, delays, missed opportunity to interact, fees for specialized software, etc. The implications is that, for a given level of risk aversion, the rational choice for the individual is to undertake risk handling behaviour only if the expected benefit, net of risk handling behaviour costs, is large enough to compensate for the perceived risk of the interaction. Since risk handling behaviour itself has the potential to reduce risk and hence the perception thereof, the net effect is that the intensity of the risk handling behaviour undertaken in a given set of circumstances increases in the magnitude of both the perceived risk and expected benefit of the interaction.

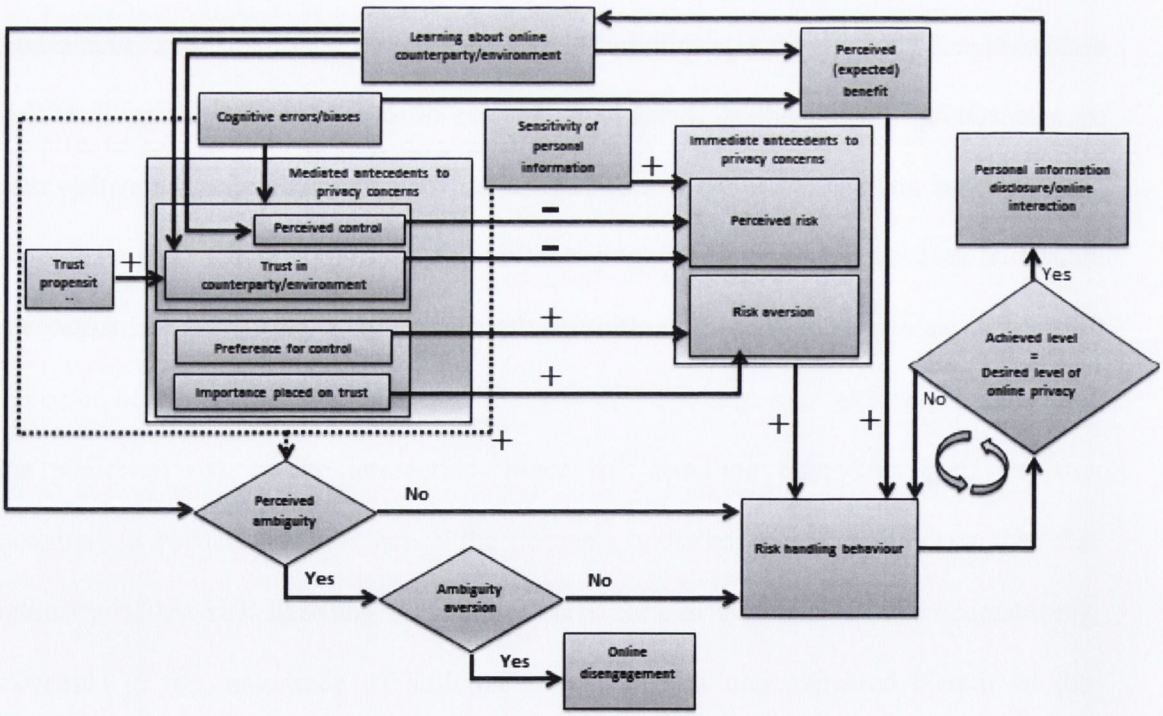
Figure 3.4 overleaf summarizes the main constructs, and relations thereof, of the RPC model. The figure is drawn so as to facilitate the comparison between this model and the traditional PC model (diagrammatically summarized in Figure 3.2 in the previous section). Panel A of the figure focuses on the implications of the model for information disclosure, and is directly comparable to the flowchart in Figure 3.2 for the traditional model. Panel B focuses instead on the possible role of risk handling behaviour in privacy-related decisions. Just like in the traditional PC model, the individual uses available information, acquired through learning about the online counterparty and the online environment, to form his/her perception of the benefits and of the riskiness of the interaction in the situation under consideration, having preliminary formed a perception of the control exerted over his/her personal information and of the trustworthiness of the counterparty. In the revised model, however, the assessment of risk and rewards may be affected by cognitive error and biases and, in the event that the individual perceives ambiguity and he/she is adverse to it, he/she will disengage rather than either interacting or undertaking risk handling behaviour. In this respect, we conjecture that the perception of ambiguity might be enhanced when the personal information that the individual is required to submit is highly sensitive. Accordingly, in this formulation of the model, we allow for a positive effect of the sensitivity of personal information on perceived ambiguity.

Figure 3.4 The Revised Privacy Calculus (RPC) Model

Panel A



Panel B



3.3.1 The Hypotheses

In what follows, we put forth a number of hypotheses consistent with implications of the traditional and revised formulations of the PC model. We start from the hypotheses that hold under the RPC model and then highlight the ones that do not hold in the context of the traditional formulation of the model.

The first set of hypotheses (H1) is that an individual's willingness to disclose personal information in an online interaction is positively influenced by his/her *perceived benefit* (a measure of net expected reward) of the online interaction.

A further set of hypotheses is that an individual's willingness to disclose personal information in an online interaction is negatively influenced by *privacy concerns* and therefore by the (immediate) antecedents to the latter, namely *risk aversion* (H2) and the *perceived level of privacy risk* (H3). As far as H2 is concerned, an individual's willingness to disclose personal information in an online interaction is

a) negatively influenced by his/her *risk aversion*, for a given *level of perceived risk* (regarding how personal information is used by the online counterparty);
b) negatively influenced by *positive* antecedents to risk aversion (such as *preference for control*, for a given level of control perceived by the individual, and *importance placed on trust*, for a given level of trust in the counterparty/online situation and propensity to trust);
c) positively influenced by *negative* antecedents to risk aversion.

As far as H3 is concerned, an individual's willingness to disclose personal information in an online interaction is

a) negatively influenced by his/her *perceived level of risk* (regarding how personal information is used by the online counterparty), for a given level of *risk aversion*;
b) negatively influenced by positive antecedents to perceived risk (such as *perceived lack of control and distrust* of the counterparty/online situation);
c) positively influenced by negative antecedents to perceived risk (such as *perceived control* and *trust* in the counterparty/online situation).

The fourth set of hypotheses (H4) is that an individual's willingness to disclose personal information in an online interaction is negatively influenced by

a) his/her level of *ambiguity aversion*, for a given level of *perceived ambiguity* of the online situation;
b) the level of *perceived ambiguity* of the online situation, for a given level of ambiguity aversion;
c) positive antecedents to either *perceived ambiguity* or *ambiguity aversion* (we conjecture that age may play this role as far as ambiguity aversion is concerned).

In relation to risk handling behaviour, we noted earlier that, under the (realistic) auxiliary assumption that such behaviour is costly to undertake, we can expect it to be undertaken to a greatest extent (i.e., greater risk handling behaviour 'intensity') by subjects who, at the same time, perceived the greatest risk and the greatest potential

benefit from interactions in online environments. Therefore, the fifth set of hypotheses (H5) is an individual's risk handling behaviour intensity is

a) positively impacted by the *perceived benefit* of disclosing personal information online;

b) positively impacted by the individual's *perceived risk* and *risk aversion*;

c) negatively impacted by negative antecedents of the individual's perceived risk (such as *perceived control*, *trust*[9] in the counterparty/online situation and *propensity to trust* in online situations, respectively) and risk aversion;

d) positively impacted by positive antecedents of the individual's perceived risk (such as perceived *lack of control*) and risk aversion (such as *preference for control* in online situations and *importance placed on trust*);

e) negatively impacted by *perceived ambiguity* and the individual's *ambiguity aversion* (because the individual, in the presence of ambiguity, disengages), as well as by their positive antecedents (we conjecture that age may play this role as far as ambiguity aversion is concerned);

f) positively impacted by negative antecedents to *perceived ambiguity*, such as training and education, to the extent that they reduce limits to rationality.

Finally, consistent with the circumstance that we allow for behavioural biases (*availability bias*), we may conjecture that individuals that have perceived a recent privacy breach (say, in the last six months) experience a weaker perception of control over their personal information and perceive greater ambiguity. Therefore, a further

[9] Because, for a given level of actual risk, a greater trust translates into a lower perceived risk and therefore a lesser need for risk handling behaviour.

hypothesis (H6) is that both the individual's willingness to disclose personal information and his/her propensity to engage in risk handling behaviour are negatively influenced by the recent occurrence of a privacy breach, and that both depend negatively on variables, e.g. age and working in the computer industry, that capture the extent to which limits to rationality (familiarity with IS) are binding.

By way of comparison of the traditional and revised formulations of the PC model, we note that H1, H2, H3, H5.a-H5.d are in common to both formulations (even though previous literature on the PC has placed more emphasis on explicitly modelling implications for information disclosure rather than for risk handling behaviour, and therefore H5 have received relatively little attention), whereas H4, H5.e and H6 hold only in the context of the RPC model.

3.3.2 Privacy as an Absolute and the Revised Privacy Calculus (RPC) Model

The intellectual underpinning of the PC model is the conceptualization of privacy as a condition with a relative rather than as an absolute value. It may be argued, however, that the model can be viewed, in a sense, as encompassing both views. From this point of view, an individual who views privacy as a condition carrying an absolute (rather than a relative) value could be characterized as exhibiting an infinite privacy risk aversion or, equivalently, as perceiving an infinite amount of privacy risk. The implication of such characterization is that such an individual would never willingly put privacy at risk, exactly what we would expect from an individual who deemed privacy an absolute. This interpretation of the implications of viewing privacy as an absolute is

however problematic. For example, it might be argued that there are always situations in which even the most privacy loving individual would sacrifice his or her privacy, e.g. if the choice were between the latter and, say, the well-being of a close relative. In the context of the RPC model, a more nuanced approach to the characterization of an individual who deems privacy to be an absolute might therefore envisage that privacy is not the only condition to which the individual associated an infinite amount of risk and/or benefit. While fascinating, however, we leave a further exploration of the implications of viewing privacy as an absolute to future research.

3.4 Conclusions

In this chapter, we first introduced some essential contributions made by the economics literature to the understanding of the decision making problem under uncertainty. We then reviewed IS research that has made use of the insights offered by this literature. We placed a special emphasis on studies that have examined privacy and privacy-related decision making problems and the attendant issue of privacy risk taking behaviour, including efforts to explain the so called privacy paradox. We grouped contributions relevant to the understating of these problems in two classes corresponding to two different paradigms, characterized by different assumptions concerning individuals' rationality. Overall, while available empirical evidence does not conclusively rule out the case for deeming rational decision-making as an effective paradigm for the purpose of explaining privacy-related decision and privacy risk taking, it does offer support for the notion that disclosure is not wholly determined by rational thinking and there remain many opportunities to better understand the role of irrationality in the context of privacy

and disclosure-related behaviours. Indeed, Acquisti (2009) notes that "this is an area of research ripe for further investigation" (p. 74).

We finally bring together insight from the traditional PC model with ideas and suggestions from psychology and behavioural economics. In the resulting model of privacy-related decision making under uncertainty, which is labelled as the revised privacy calculus (RPC) model, the IS user evaluates a trade-off between expected benefit and privacy risk in deciding whether to engage in online interactions but such evaluation, unlike in typical formulations of the PC model, is explicitly subject to limits to rationality, whether subjective or objective and possibly large enough to lead to the perception of ambiguity, and cognitive bias. In the model, the decision maker can decide whether to undertake risk handling behaviour, assumed to be costly, as well as choose whether to interact or otherwise.

It should be noted that, for greater generality, it is the trade-off between expected benefit and overall risk that should be at the centre of the model. That is, there is no obvious reason not to posit that the decision maker evaluates all risks of the online interaction, e.g. the risk of fraud, and not only the risk of losses, i.e. unpleasant consequences, arising from violations of privacy. Though violations of privacy are more or less directly related to other possibly unwelcome circumstances, e.g. fraud, we focus on privacy risk only as privacy is the focus of this study. The implicit assumption is that privacy risk is sufficiently important for IS users to warrant a distinct modelling.

4 Research Methodology

This chapter examines the research methodologies that have been employed in the empirical literature, with a special emphasis on methodologies and related methods appropriate to the study of privacy and privacy-related decision making problems and for conducting research in an engineering environment. In addition, it outlines the methodological framework for the research undertaken as part of this study, namely ADR. It explains how in this research project the ADR methodology plays the role of a sort of meta-methodology, within which, at different stages, we use methods prescribed by other methodologies, i.e. a questionnaire, semi-structured interviews and focus groups, to carry out the learning required by the ADR approach. We outline and motivate the steps of such a multi-method approach, with a greater emphasis on those which occurred during the more advanced stage of the project, i.e. the 'Formalized ADR' stage.

4.1 The Research Process under Alternative Epistemologies

A research process can be defined as a systematic collecting, analysing and interpreting of information in order for an individual, group or organisation to increase their understanding of the subject in which they are interested (Leedy and Ormrod, 2005). According to Lee (2004) and Burrell and Morgan (1985), many social scientists approach their research via explicit or implicit assumptions about the nature of the social world and the way in which it may be investigated. There are three sets of

assumptions essential to any research process, namely ontological, epistemological and methodological assumptions.

Ontological assumptions concern the very essence of the phenomena under investigation. Crotty (2003) defines ontology as the study of *being*. It is concerned with the nature of existence and the structure of reality. Burrell and Morgan (1985) emphasize that social scientists are faced with a basic ontological question of whether there is an accepted and objective definition of reality and whether this "reality" is external to the individual or it is subjective and internal, i.e. the product of the individual's own mind. Lee (2004) remarks that a school of thought's ontology comprises its members' foundational beliefs about the empirical or 'real' world that they are researching. Orlikowski and Baroudi (1991) describe ontological beliefs as essentially having to do with whether the empirical world is assumed to be objective and hence independent of humans, or subjective and hence having existence only through the action of humans in creating and recreating it.

Epistemological assumptions concern the criteria by which valid knowledge about a phenomenon may be constructed and evaluated (Orlikowski and Baroudi, 1991). Epistemology is often defined as the theory of knowledge, i.e. what we know and how we know that we know. Lee (2004), however, finds this definition unsatisfactory because it fails to define the term 'theory'. The problem is further complicated by the fact that what a theory is depends on, among other things, an epistemology. Therefore, Lee conceptualises an epistemology as a broad and high-level outline of the reasoning process by which a school of thought performs its empirical and logical work. In response to this criticism, Crotty (2003) puts forth an alternative definition, that

circumvents the need to make use of the term 'theory', and refers to epistemology as a way of *understanding and explaining* how we know what we know. It might be argued that the controversy over the circularity between the definitions of epistemology and theory hints at a deeper difficulty, i.e. the circumstance that it might be difficult to define epistemology independently of ontology, at least in certain contexts. Along these lines of reasoning, Crotty (2003) emphasizes, like Burrell and Morgan (1985) before him, that ontology informs the theoretical perspective of the researcher because each perspective embodies a certain way of understanding reality (ontology) as well as a certain way of understanding what it means to know (epistemology). Maynard (1994) claims that the relevance of epistemology to a research process is in providing a philosophical grounding for the decision about the kinds of knowledge that are possible and how they are shown to be adequate and legitimate. Therefore, it is necessary that researchers identify, explain and justify the epistemological stance they adopt for every research process upon which they embark.

Finally, methodological assumptions underpin the choice of the research methodology, that indicates which research methods and techniques are considered appropriate for the gathering of data for any research project. Which methods are considered appropriate clearly depend on how the veracity of a theory is established, which in turn depends on the researcher's philosophical perspective. The same epistemology, however, can have several methodologies. An interpretivist epistemology, for example, would recognize ethnography and grounded theory as methodologies. A positivist epistemology would recognise scientific experiments and survey research as methodologies (Crotty, 2003).

While research methodologies will be discussed in detail later in the chapter, the rest of this section discusses some of the main theoretical perspectives used in Information Systems that have recently dominated the scientific debate. We will first explore, by discussing positivism, the objectivist standpoint. We will then examine the constructionist point of view, from the perspective of interpretivism. At this point, however, it is important to note that the comments that will be offered are meant to serve only as an introduction to these perspectives, in that their rigorous discussion is beyond the scope of this work.

4.1.1 Positivism in Information Systems Research

Historically, the positivist research perspective has been the dominant one in information systems research. While positivism dates as far back as Compte and the first half of the nineteenth century, its modern counterpart, logical positivism, was popularised by the Vienna Circle in the 1920s. The Vienna Circle was a group of mathematicians, scientists and philosophers who began meeting in Vienna to discuss recent developments in logic such as Wittgenstein's book *Tractatus Logico-Philosophicus* (1922). Positivism and logical positivism alike can be seen as reflecting the following precepts:

- The phenomenon of interest is single, tangible and fragmentable, and there is a unique, best description of any chosen aspect of the phenomenon.
- The researcher and the object of inquiry are independent, and there is a sharp demarcation between observation reports and theory statements.

- Nomothetic statements, i.e., law-like generalizations independent of time or context, are possible, implying that scientific concepts are precise, having fixed and invariant meanings.
- There exist real, uni-directional cause-effect relationships that are capable of being identified and tested via hypothetic-deductive logic and analysis.
- Inquiry is value-free.

(Orlikowski and Baroudi, 1991). Orlikowski and Baroudi (1991), however, argue that the application to research on social phenomena of these precepts, that typically inform the study of natural phenomena, is problematic. Even many researchers practicing positivist research would agree that some of these precepts are ideals that are routinely compromised in day-to-day research activity. Additionally, Logical Positivism has since been criticized by many as an epistemology but a further discussion is outside the scope of this research.

Ontologically, positivist IS researchers assume an objective physical and social world that exists independent of humans, and whose nature can be relatively easily apprehended, characterized, and measured. For example, organizations are understood to have a structure and reality beyond the actions of their members. The role of the researcher is to "discover" the objective physical and social reality by crafting precise measures that will detect and gauge those dimensions of reality that interest the researcher (Orlikowski and Baroudi, 1991). Understanding phenomena is thus primarily a problem of modelling and measurement, of constructing an accurate set of instruments to capture the essence of the phenomenon. The researcher is seen to play a neutral role in this investigation, and does not intervene in the phenomenon of interest. For example,

when researchers investigate the relationship between information technology and organizational structure, they assume structure to be objective and hence capable of being represented via a number of researcher-devised constructs and measures such as: span of control, division of labour, centralization, formalization, and hierarchical levels (Orlikowski and Baroudi, 1991).

With respect to knowledge, the epistemological belief of the positivist perspective is concerned with the empirical testability of theories, whether this requires theories to be "verified" or "falsified." The search for connections between information technology and changing environmental conditions or organizational forms assumes that the empirical world is largely characterized by knowable, persistent and reliable relationships. To support such an epistemological belief, the positivist research perspective endorses a number of "appropriate" research methodologies. The belief is that following these sanctioned methodologies is the only way in which valid knowledge can be obtained. Sample surveys and controlled experiments are the primary data collection techniques, and inferential statistics is the data analysis method used to "discover" or validate causal laws. The validity and reliability of identifying and measuring instruments are crucial, as are researcher detachment from the research process, random assignment of subjects and control over confounding influences (Orlikowski and Baroudi, 1991).

Positivism has institutionalized certain criteria of validity, rigor, and reproducibility in the conduct of scientific research. It has enforced standards of quality in empirical research, and has sought to build a tradition of cumulative knowledge across the various disciplines in which it is practised. A number of authors argue that much has been

learned about the development and use of IS from the application of methods consistent with a positivist perspective (Galliers and Land, 1988). Positivist research continues to be used in IS research as an effective and appropriate method for gathering information, particularly when information needs to be gathered from a large population (surveys) or from artefacts (Design Science).

4.1.2 Interpretivism in Information Systems

The interpretivist perspective has been enjoying, for some time, increased attention and popularity in many social science fields including organizational studies, political science, sociology, marketing, education, social psychology and indeed information systems (Agosta, 2010). A fundamental distinction between the interpretivist and positivist world views is the former's primary presumption of social constructionism. Interpretivism asserts that reality is a social product and hence incapable of being understood independently of the social actors (including the researchers) that construct and make sense of it. The world is not conceived of as a fixed constitution of objects, but rather as "an emergent social process, as an extension of human consciousness and subjective experience" (Burrell and Morgan, 1985, p. 253). Interpretivism embraces a wide range of philosophical thought which shares the common characteristic of attempting to understand and explain the world primarily from the point of view of the actors directly involved in it. Its history is rooted in the German Idealist tradition. It takes the view that the universe lies in 'spirit' or 'idea' rather than in the data of sense perception (Burrell and Morgan, 1985). According to Orlikowski and Baroudi (1991), the aim of all interpretive research is to understand how members of a social group, through their participation in social processes, enact their particular realities and endow

them with meaning, and to show how these meanings, beliefs and intentions of the members help to constitute their social action.

Ontologically, the interpretive perspective emphasizes the importance of subjective meanings and social-political as well as symbolic action in the processes through which humans construct and reconstruct their reality (Morgan, 1983: 396). For example, this tradition does not presume that organizational structure or social relations are objectively known and unproblematic, instead it attempts to understand how and why individuals, through their socialization into, their interaction with, and their participation in, a social world, give it a certain status and meaning. Meaning and intentional descriptions are important, not merely because they reveal subjects' states of mind which can be correlated with external behaviour, but because they constitute those behaviours. Social reality is understood to be reproduced through on-going interactions. The interpretive philosophy asserts that understanding social reality requires understanding how practices and meanings are formed and informed by the language and implicit norms shared by humans working towards some shared goal (Orlikowski and Baroudi, 1991).

The primary endeavour of interpretivist research is to describe, interpret, analyse, and understand the social world from the participants' perspective. An example of a research method appropriate to generating valid interpretive knowledge is a field study, as it examines humans within their social settings. Following on from the ontological belief that reality is socially constructed, the interpretive researcher avoids imposing externally defined categories on a phenomenon. As well as the researcher coming to the field with a well-defined set of constructs and instruments with which to measure the

social reality, the interpretive researcher often attempts to derive his or her constructs from the field by in-depth examination of and exposure to the phenomenon of interest. The categories and themes that emerge out of this approach are intended to closely couple those relevant to the study's participants (Orlikowski and Baroudi, 1991).

From an interpretivist perspective, the researcher can never assume a value-neutral stance, and they are always implicated in the phenomena being studied. Researchers' prior assumptions, beliefs, values, and interests have the potential to intervene to shape their investigations. Interpretivists recognise the potential for personal bias and usually try to neutralise their bias when conducting research. An important contribution of the interpretive research philosophy is that it reveals the underlying connections among different parts of social reality, by examining the social rules and meanings that make social practices possible (Gibbons, 1987: 7).

A central problem of interpretivist analysis is the issue of mutual knowledge; namely, how we come to know the mind of another person without *being that person*. Descartes, for example, holds that we are capable of knowing only the body of another person because it is perceptually accessible to us, but not the mind of another person because it is not subject to our direct observation. Husserl, on the other hand, contends that, although we have no direct access to the inner consciousness of another person, we are able to "grasp" it based on the knowledge of our own mind. According to Zhao (2007), Alfred Schutz proposes a sociological solution which grounded mutual knowledge on social interaction. Schutz maintains that the mind of the other can be known in a shared social world or what he terms as the 'lifeworld' where individuals become intimately familiar with each other through sustained face-to-face contacts. He divided the

contemporaneous lifeworld into two realms, consociates and mere contemporaries. Schutz maintained that people came to know one another based on shared life experiences in two realms. Firstly, through "growing older together" in the realm of consociates or "fellowmen" and secondly, based on objectified schemes of interpretation through "ideal typification" in the realm of mere contemporaries (Zhao, 2007). The use of interpretivism to understand the social impact of communication technology, particularly the Internet on society, has been an attractive endeavour for many researchers in recent decades (Brown and Lightfoot, 1998; Casey and Embree, 1990; Cass, 1998; Idhe, 1990; Zhao, 2006; Zhao, 2004). There is a long history of philosophical debate over mutual knowledge and surrounding issues but a further discussion is outside the scope of this work.

Like positivism, the interpretive research philosophy has also been subject to criticism (Bernstein, 1978; Burrell and Morgan, 1985; Fay, 1987). Firstly, it is claimed that research from this perspective does not expose or place emphasis on the unintended consequences of action, which by definition cannot be explained by simply explaining the intentions of the humans concerned (Fay, 1987 p. 92). It is argued that these unintended consequences of action are often a significant force in shaping social reality. For example, an important and typically unintended consequence of human action is that which *reinforces* the actions, roles, beliefs, and relative power of members of a group to sustain the structure and practices of that group as a whole over time (Giddens, 1979). Additionally, it has been criticised for not placing enough emphasis on analysing the contradictions which may be endemic in social systems, thereby failing to consider the means by which actors may be blinkered in their self-understanding and limited in their social interactions. For example, Fay (1987) argues that research in this

perspective often "assumes an inherent continuity in a particular society, i.e., it…ignores the possible structures of conflict within a society, structures which would generate change" (Fay, 1987: p. 96). Nevertheless, historical and longitudinal research studies within the interpretive perspective are plentiful.

4.2 Qualitative Research Methods and Methodologies

Qualitative research approaches are often used in the study of phenomena that occur in natural settings. Additionally, the aim of such studies is to examine those phenomena in their totality (Crotty, 2003). These qualitative approaches are not inconsistent with a positivist perspective, though they are more often adopted by research that adopts an interpretivist epistemological viewpoint. Qualitative researchers recognise that the phenomena they are studying have many dimensions and layers, and they try to portray them in their true, complex forms (Leedy and Ormrod, 2005). Qualitative researchers believe that the researcher's ability to interpret and make sense of what they see is critical for understanding these social phenomena. The rest of this section describes a number of qualitative research methods (semi-structured interviews, focus groups and hypothetical scenarios) and methodologies (action research, case study, ethnography and grounded theory research) commonly used in IS.

4.2.1 Semi-structured Interviews

Though there are many types of interviews that can be used for research purposes, we focus on semi-structured interviews as this is the format we use in this research. In semi-structured interviewing, a guide is used, with questions and topics that must be

covered during the interview. The interviewer has some discretion about the order in which questions are asked, but for semi-structured interviews the questions are standardized. This kind of interview collects detailed information in a style that is somewhat conversational. Semi-structured interviews are often used when the researcher wants to delve deeply into a topic and to understand thoroughly the answers provided (Harrell and Bradley, 2009).

The activities that are required in an interview study, in addition to the actual interview, usually consist of scheduling the interviews, preparing interview guides, transcribing the interviews once they have taken place and summary write up of the interviews. Interviewing is time consuming, as the researcher needs to prepare for each interview and undertake it. Effort in relation to analysis must also be taken in to account. Analysis typically exceeds the time spent on the activities listed above by several times (Hove and Anda, 2005).

Good interviewing skills are essential for the effective use of this form of data gathering and they include encouraging the interviewees to talk freely, asking relevant and insightful questions, following up with the interviewees and exploring interesting topics. The required skills of the interviewer are explored and discussed thoroughly in the qualitative interview literature. According to Kvale (1996), an interviewer must master human interaction and have excellent conversational skills. The interviewer should open the interview by re-explaining confidentiality and anonymity (Rapley, 2004), and explain the purpose of the interview and the intentions of the interviewer (Kvale, 1996; Rapley, 2004). It is also important to ask for permission in case the interview is being audio recorded (Rapley, 2004; Weiss, 1994). In order to create a

comfortable atmosphere in which useful information can be elicited, the interviewer should be non-judgmental and sensitive, let individuals talk, and pay attention, as outlined by Taylor and Bogdan (1984). These desired qualities are also found by Kvale (1996), who also emphasized that the interviewer must express him/herself clearly, be gentle, open and sensitive towards the interviewees, but at the same time not take everything said at face value and bear in mind what a subject has said earlier in the interview. It is also important to clarify issues during the interview where possible.

4.2.2 Focus Groups

In a focus group, a collection of people are asked about their perceptions, opinions, beliefs, and/or attitudes towards a product, service, concept or idea. Questions are asked in an interactive group setting where participants are free to talk and discuss the topic at hand with other group members. In the social sciences, focus groups allow interviewers to study people in a more natural conversation pattern than typically occurs in a one-to-one interview. In combination with participant observation, they can be used for learning about groups and their patterns of interaction (Marshall and Gretchen, 1999). In engineering disciplines, especially in ergonomics, a focus group is a survey method to collect the views of users regarding a software system or a website. This method can be used to evaluate users' perception of a software system and to better understand the motivations of users of the system. Unlike other methods used in ergonomics, however, focus groups require several participants, i.e. multiple users or future users of the system (Nielsen, 1993).

Group discussions like those conducted with focus groups often produce data and insights that would be less accessible without the interaction of individuals in a group setting (Lindlof and Taylor, 2002). By listening to others talking about their experiences, the participant's own memories, ideas, and experiences are stimulated. This is also known as the group effect where group members engage in "*a kind of 'chaining' or 'cascading' effect; talk links to, or tumbles out of, the topics and expressions preceding it*" (Lindlof and Taylor, 2002, p. 182). Group members discover a common language to describe similar experiences. This enables the capture of a form of "native language" or "vernacular speech" to understand the situation (Lindlof and Taylor, 2002). Focus groups also provide participants with an opportunity to disclose details about themselves and their experiences in a relaxed setting. For example, in the context of workplace bullying, targeted employees often find themselves in situations where they feel both isolated and that they have no voice. The use of focus groups to study workplace bullying therefore serve as both an effective and ethical venue for collecting data (Tracy, Lutgen-Sandvik and Alberts, 2006).

The analysis and interpretation of focus group data require a great deal of judgment and care, just as any other scientific approach, and regardless of whether the analysis relies on quantitative or qualitative procedures (Stewart, 2007). There is no one best or correct approach to the analysis of focus group data. As with other types of data, the nature of the analyses of focus group interview data should be determined by the research question and the purpose for which the data are collected. The most common purpose of a focus group interview is to provide an in-depth exploration of a topic about which little is known. For such exploratory research, a simple descriptive narrative is quite appropriate and often all that is necessary (Stewart, 2007). More detailed analyses

are simply neither an efficient or productive use of time, unless they serve a particular research objective (Stewart, 2007).

Data analysis can take place at the level of the individual or the group. Focus group data provides the opportunity to analyse the strength with which an individual holds an opinion. If they are presented with opposing opinions or directly challenged, the individual may either modify their position or defend it. Bringing together all the comments that an individual makes in order can enable the researcher to determine whether their view changes in the course of discussion and, if so, further examination of the transcript may reveal which contributions by other focus group members brought about the change. At the collective level, focus group data can sometimes reveal shared understandings or common views. However, there is a danger that a consensus can be assumed when not every person has spoken: the researcher will need to consider carefully whether the people who have not expressed a view can be assumed to agree with the majority, or whether they may simply be unwilling to voice their disagreement (Harding, 2013).

4.2.3 Hypothetical Scenarios

Hypothetical scenario methodology has been used during interviews and focus groups to assess interest in a product and estimate an upcoming need for a service (Persky et al., 2007). This methodology has the benefit of allowing investigators to manipulate important product characteristics and contextual variables to understand better how these factors influence reported interest levels and intentions for use. Hypothetical assessments are often presented using vignette and vignette-type methodology which

generally involves presenting a story about or representation of a person in a situation. Vignettes are a tool with many advantages; product mock-ups can be produced relatively quickly and cost-effectively, can be demonstrated under most conditions without too much special preparation, and have the capacity to convey scenarios in a standardized way.

4.2.4 Action Research

The term "action research" was introduced by Kurt Lewin in 1946. Lewin (1946) formulated his definition of action research and how it differed from traditional positivist science in his letters between 1944 and 1946 in which he expressed profound concern and urgency for finding methods to deal with critical social problems of the time such as fascism, anti-Semitism and poverty (Marrow, 1969). Lewin characterized action research as "*a comparative research on the conditions and effects of various forms of social action and research leading to social action*" (Lewin, 1946, pp. 202-203). This method has since proven very useful when managing change. Action research has been defined as both a model and a process. Rothwell et. al (1995) sees action research as a simplified representation, or model, of the complex activities that occur during a period of change. The model serves as a type of roadmap which provides the individuals involved in the change process with the methods and techniques needed to guide them through the change.

The Action Research approach is dominated by an underlying pragmatic orientation (Baskerville and Myers, 2004). In fact, according to Avison et al. (2001) the active role of the action researcher, defined as involvement and even 'embeddedness' in

organisational change, versus the passive role of the case study researcher makes action research a more viable approach to information systems research. The requirement to solve a real world problem coupled with the need for iterative approaches to software development provides an excellent fit with action research (Butler et al., 2008).

4.2.5 Case Study

Remenyi et al. (2000) define a case study as *an empirical enquiry that investigates a contemporary phenomenon within its real life context, when the boundaries between phenomenon and context are not clearly evident, and in which multiple sources of evidence are used* (Remenyi et al., 2000, P165). A less formal definition is given by Leedy and Ormrod (2005), who state that a case study examines a particular subject i.e. individual, group or organization, or event i.e. process or project, in depth for a defined period of time. An example of this would be when a medical researcher studies the nature, course and treatment of a rare illness for a particular patient. Another example could be when an educator studies and analyses the instructional strategies of a master teacher.

Case studies come in a number of forms from the single case to a large number of cases (15-20 or more). A typical case study involves two to four cases used for comparative purpose (Remenyi et al., 2000). Alternatively theory may be developed in one case and verified, or not, using another, or several other, cases. The case study can be used in two distinct ways, that is to establish valid and reliable evidence and as a vehicle for creating a story or narrative description of the situation being studied. When used in the first way, evidence produced by the case study may be analysed from either a positivist

or an interpretivist perspective. A positivist analysis of a case study would typically include the collection of numerical evidence and the application of one or more techniques of statistical analysis. An interpretivist analysis would require instead a holistic interpretation process. In either scenario, the researcher may spend an extended period of time on site interacting regularly with the people who are being studied. The evidence collected for the research can range from factual observations, interviews, analysis of documents and past records and audio-visual material. When used in the second way, the story or narrative of the situation being studied should represents a research finding in its own right, by providing an explanation of the observed phenomena and demonstrating an understanding of the subjects in their context and environment. Even though this method must present a convincing argument, it does not necessarily have to be presented in quite the same structured way as the evidence collected in the other type of case studies (Remenyi et al., 2000). The single case study can difficult to generalize and therefore are often used for specific types of study. Reliance on a single case study is sometimes seen as a weakness of the application of this method because of a concern in relation to whether the findings are generalizable to other situations (Leedy and Ormrod, 2005).

Case studies are an effective research method for information systems research because they can be used in a number of different ways that accommodate the complexity which is often an inherent part of the IS research process (Remenyi et al., 2000). For example, Information Systems (IS) within organisations are sometimes poorly understood and some organisations find it difficult to implement an effective IS management process. A case study is especially suitable for learning more about a poorly understood situation or process such as the IS management process. The reason for this is that it allows the

researcher to develop a deeper exploration of the characteristics of real-life events like the IS management process or the organisation-wide roll out of a new strategic management system (Remenyi et al., 2000).

4.2.6 Ethnography

Originating with social anthropologists, ethnographic research is a type of field observation in which the culture of a group of beings, usually a society of some sort, is studied. It is usually necessary for the researcher to become involved with the group that is being studied for a substantial period of months or even years (Remenyi et al., 2000). A well-known ethnographer is the British anthropologist and primatologist, Jane Goodall who has studied chimpanzees in their natural habitat since the 1960s. By close observation over a thirty year period, she documented the social organisation of chimpanzees in the wild, including their social nature, their tool-making, their occasional systematic killing of one another, their hierarchy and their social development (Lewis, 2008).

In more recent years, this method of research has become popular in many other disciplines such as psychology, sociology and education (Remenyi et al., 2000). The concept of the type of culture that can be studied has also changed over time, in recent years ethnographies have been used to study cultures in corporations, kindergartens and even homeless shelters (Saunders, Lewis and Thornhill, 2007). Ethnographic research is well suited to providing IS researchers with rich insights into the human, social, and organizational aspects of information systems as ethnographic researchers remains on-site for a long time and observe what individuals habitually do as well as what they say

they do. An ethnographer, thus, obtains a deep understanding of the people, the organization, and the broader context within which they work (Myers, 1999). It may be argued though that ethnography only works for certain research problems and it takes great skill to 'disappear into the background'. In fact the very presence of the ethnographer may influence the environment, but the hope is that this impact will be so small as to not invalidate his/her findings (Myers, 1999).

4.2.7 Grounded Theory

Grounded theory can be defined as an inductive, theory-discovery methodology that allows the researcher to develop a theoretical account of the general features of a topic while simultaneously grounding the account in empirical observations or evidence (Glaser and Strauss, 1967). The major purpose of a grounded theory approach is to begin with the data and use them to develop a theory. More precisely, a grounded theory study uses a prescribed set of procedures for analysing data and constructing a theoretical model from them. The term 'grounded' refers to the idea that the theory that emerges from the study is derived from and grounded in the data that have been collected in the field rather than taken from the research literature (Leedy and Ormrod, 2005). The sociologists Glaser and Strauss (1967) were the originators of the approach, but it is now used in many disciplines such as anthropology, education and psychology (Leedy and Ormrod, 2005). Grounded Theory has some aspects in common with ethnography. They overlap in areas where ethnographers adopt a more 'behavioristic' approach and set about explaining variations in phenomena observed in the field. This type of ethnographic research is concerned with the inductive development of theory (Glaser and Strauss, 1967, Gill and Johnson, 1991).

4.3 Quantitative Research Methods

Quantitative research is the term used to describe research which, as the name suggests, is based on numeric data or data which can be readily converted to numeric values.

In the social sciences and particularly in information systems research, data collection often involves the use of a survey (Remenyi et al., 2000). What follows will review the main quantitative research methods, with an emphasis on those that can be most productively used in IS studies and, in particular, to investigate privacy-related issues.

4.3.1 Survey Research

A survey involves asking a set of questions to elicit information about features of the phenomena of interest. The questions are often asked in the format of a questionnaire but can also be in the form of interviews. A key aim of survey research is to ensure standardisation of data collection. Each participant is assumed to answer questions the researcher has posed in precisely the same way. The standardization is sought to render the survey a more effective measuring instrument (Sapford, 2007).

Dillman (2000) makes a distinction between three types of data variables that can be collected through questionnaires, i.e. data on opinions, behaviour and attributes. Such a distinction is important because it has implications for choices about the way questionnaires are worded. *Opinion* variables record how respondents feel about something or what they think or believe to be true or false. Data on *behaviour* records the actions of respondents. Data on *attributes* record the characteristics of respondents,

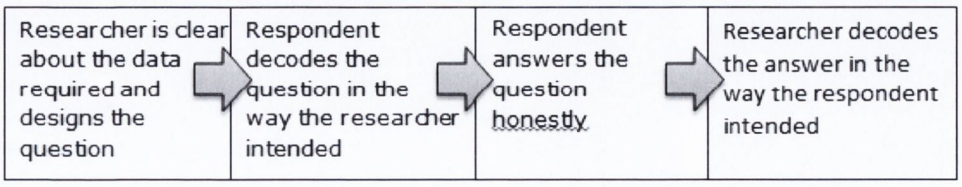
such as age, gender, marital status and occupation, and they are mainly used to help explain how opinions and behaviour differ between respondents and to aid the implementation of sampling schemes aimed at ensuring that the data collected are representative of the population of interest (Saunders, Lewis and Thornhill, 2007).

A key requirement for a survey is to ensure that the questions measure the construct under investigation. Sampling considerations are also important. A good survey design will be of little use if the sample is poor, e.g. small or not representative of the population of interest. The internal validity and reliability of the survey depend on the questionnaire structure and design and the rigor of the pilot testing. As put by Sapford (2007), three requirements need to be met to ensure the validity of a survey:

- Validity of measurement, i.e. the data constitute accurate measurements of what is being measured;
- Validity of sample, i.e. the sample gives an accurate representation of the population of interest;
- Validity of design, i.e. the comparisons (if any) which are being made are appropriate and sufficient to establish the arguments which rest on them.

Foddy (1994) outlines four circumstances that must occur if a question within a questionnaire is to be valid and reliable. Figure 4.1 shows them.

Figure 4.1 Circumstances for a question is to be valid and reliable (Froddy, 1994)



There are three relevant notions of validity of questions (Saunders et al., 2007), i.e.

- Content validity
- Criterion-related validity
- Construct validity

Content validity refers to the extent to which the questions in the questionnaire provide adequate coverage of the problem or circumstances under investigation. This can be ensured through carefully defining the research or through the use of a panel to assess whether each question is essential. Criterion-related validity is concerned with the ability of the questions to make accurate predictions. This is typically examined through the use of statistical analysis, by employing criteria such as correlation to judge the accuracy of the predictions. Construct validity refers to the extent to which the questions actually measure the constructs that are being measured. This notion of validity is especially relevant when referring to constructs such as attitude scales, psychometrics and aptitude tests.

4.3.2 Experiments

Experiments can be usefully employed when researchers want to determine the causes of phenomena being studied or when they want to establish a cause and effect relationship. In the design of an experiment, the researcher considers many possible factors that may cause or influence a particular condition or phenomenon. The researcher then attempts to control for all influential factors, by fixing them at a constant and known level, except those whose possible effects are the focus of the investigation (Leedy and Ormrod, 2005). The classic experiment consists of two or more 'equivalent' groups of subjects (e.g., people). The approach used in experimental

design is to assign people *randomly* from a common pool of subjects, a representative sample of the population under study, into the two groups.

The experiment relies on random assignment to groups as the basis for obtaining two groups that are as similar as possible (Trochim, 2006). A test is then carried out on both groups. This entails the measurement, in each group separately, of a particular characteristic of interest to the researcher. Only one group is then exposed to a treatment or an intervention that the researcher believes may have an effect on the characteristic being studied. Both groups are then retested to measure the characteristic of interest once again. If the characteristic changes for the group that received the treatment or intervention, but does not change for the other group and if everything about the two groups has been the same except for the intervention, then it is reasonable to conclude that the intervention brought about the change that was observed.

The situation defined by the condition in which the experiment is carried out is not only observed, but also manipulated. It can therefore be considered an experimental design (Leedy and Ormrod, 2005). A good experimental design will minimize the effect of outside influences on the evidence while it is being collected. It will also clearly identify the expected effects directly arising from the intervention. The timing of the intervention is a central aspect of the experimental design. It is important to decide when the evidence collection begins, when the intervention is initiated, when the ex-post evidence collection commences and for how long the evidence is recorded (Remenyi et al., 2000).

4.3.3 Quasi Experimental Design

Quasi experiments are experiments which have some, but not all of the characteristics of a true experiment. The element most frequently missing is *random assignment* to groups. These types of experiments are used in situations where randomness is either not possible or not practical. In such a setting, because it is typically not possible to check for all possible effects, alternative explanations for the results obtained cannot be completely ruled out. Whatever the explanations and variables that have not being either taken into account or controlled for, they must be considered during data analysis and interpretation (Leedy and Ormrod, 2005). A good example of a quasi-experiment is a so called natural experiment, where it is nature that does the assignment of groups to the two sets of diverse conditions.

One of the intended purposes for doing quasi-experimental research is to capture longer time periods and a sufficient number of different events to control for various threats to validity and reliability. The hope is that the design will generate stable, reliable findings and tell us something about the effects of time itself. In fact, for a non-interrupted time series, the independent variable is usually time itself. This would be the case, for example, if the researcher was monitoring rises and falls in crime rates and attributing it to changes in society over time (Cook and Campbell, 1979).

In the next two sections we move away from the behavioural science approach to research to examine the Design Science Research (DSR) approach. The next section introduces DSR in the field of IS and the subsequent section looks at a novel

methodology, used in this dissertation, derived for conducting DSR in IS, namely Action Design Research (ADR).

4.4 Design Science Approach to Research in IS

Even though many leading IS academics support the claim that Information Systems (IS) is an applied research discipline (Hevner, March and Park, 2004; Jones and Gregor, 2007; Walls, Widmeyer and Sawy, 1992), the dominant research approaches in IS continue to be positivist or interpretivist in nature. The benefits of these perspectives have often been expounded in the past (Walsham, 1995; Orlikowski and Baroudi, 1991) but, if resolving an engineering problem is the main focus of an IS research project, these approaches alone do not meet the challenge. It is in the typical IS research project, consisting of a quest for a technology-driven problem resolution, that Design Science Research (DSR), according to Hevner and Chattejee (2010), comes into its own. They define DSR as

> *"a research paradigm in which a designer answers questions relevant to human problems via the creation of innovative artefacts, thereby contributing new knowledge to the body of scientific evidence. The designed artefacts are both useful and fundamental in understanding that problem" (Hevner and Chatterjee, 2010: p 5)*

The term artefact is used here to describe something that is artificial, or constructed by humans, as opposed to something that occurs naturally (Simon, 1969; Hevner and Chatterjee, 2010). Like Gregor (2002) and March and Smith (1995), Hevner & Chatterjee (2010) also believe that such artefacts must improve upon existing solutions

to a problem or perhaps provide a first solution to a problem. They broadly define IT artefacts, which are the end-goal of any DSR project as follows:

- Constructs (vocabulary and symbols)
- Models (abstractions and representations)
- Methods (algorithms and practices)
- Instantiations (implemented and prototype systems)
- Better design theories

Design activities are central to most applied disciplines. Research in design has a long history in many fields including architecture, engineering, education, psychology and the fine arts (Cross, 2001). However, IS is a mix of ever changing hardware, software and human requirements that bring with it many challenging design problems. These problems call for new and creative solutions. DSR provides a process by which IS researchers can develop new engineering or software system solutions to meet these continually changing requirements.

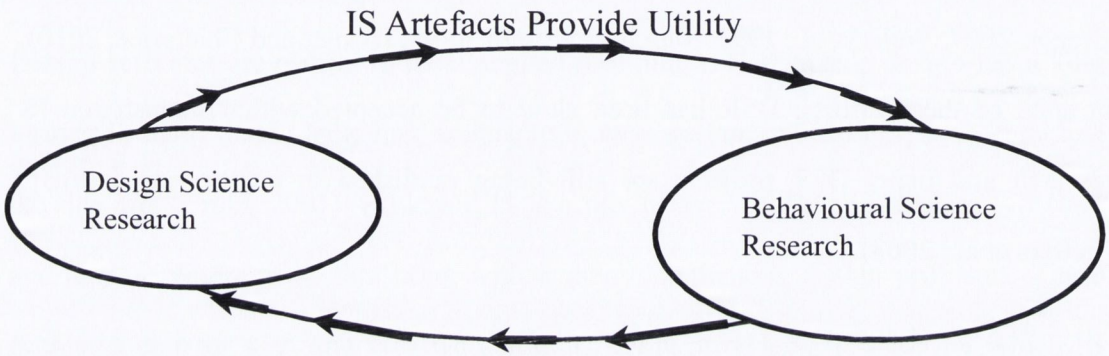
DSR is relevant to IS research as it directly addresses two key issues in the discipline, namely the role of the IT artefact in IS research (Weber, 1987; Orlikowski and Iacono, 2001; Benbasat and Zmud, 2003) and the perceived lack of professional relevance of IS research (Benbasat and Zmud, 1999; Hirschheim and Klein, 2003). DSR supports a pragmatic research approach for the creation of innovative artefacts to solve real-world problems. In fact, many engineering disciplines accept DSR as a valid and valuable research methodology as they place great importance on incrementally finding and effecting applicable problem solutions (Hevner and Chatterjee, 2010). Simon (1969) summed up the difference between traditional research approaches and DSR as follows:

"*Whereas natural sciences and social sciences try to understand reality, design science attempts to create things that serve human purposes*" (Simon, 1969: p 253). Therefore, given the *explicitly* applied character of IS practice and the *implicitly* applied character of IS research, DSR should be viewed as a valid research approach (Peffers et al., 2008). In recent years, a number of leading IS researchers have succeeded in bringing design research into the IS research community, and have shown the validity and value of DSR as an IS research paradigm (Gregor, 2002, Hevner et al., 2004, Jones and Gregor, 2007, Walls et al., 1992, March and Smith, 1995, Hevner and Chatterjee, 2010). In spite of these efforts, DSR has been slow to be accepted within mainstream IS research and many DSR projects are still being published in engineering journals (Peffers et al., 2008).

The IS research discipline to date has produced knowledge in two complementary but distinct research fields, behavioural sciences research and design science research (Hevner et al., 2004). Broadly speaking, behavioural science starts with a hypothesis, then researchers collect data, and either accept or reject the hypothesis (Hevner and Chatterjee, 2010). Eventually a theory may emerge from this process. DSR on the other hand is fundamentally a problem-solving paradigm whose end goal is to produce an artefact or information system which is built and then evaluated (Hevner and Chatterjee, 2010). Working with the technology and going through the process of construction and understanding the artefact is central to this paradigm (Hevner and Chatterjee, 2010). Architects, engineers and computer scientists have always conducted such research. The knowledge generated by this research informs us how an artefact can be improved, how and/or why it is better than existing solutions, and how it can solve the problem being addressed more efficiently (Hevner and Chatterjee, 2010). A key insight into creating

innovative DS artefacts such as database management systems, personal computers, intelligent agents, the Internet and the World Wide Web is to ensure that there exists a complementary research cycle between design science and behavioural science (Hevner and Chatterjee, 2010). The DSR research cycle facilitates the tackling of problems that can occur during the production of information technology applications (figure 4.2).

Figure 4.2 The complementary nature of design science and behavioural science research (Hevner and Chatterjee, 2010)



Artefacts are not exempt from the influence of theories as shown above in figure 4.2. On the contrary, they rely on *kernel* theories that are applied, tested, modified and extended (Walls et al., 1992). Kernel theories may be academic theories or a practitioner theory-in-use. Kernel theories facilitate the formulation of empirically testable predictions linking the design theory to outcomes like system-requirements fit. For example, it should be possible to establish empirically that the application of, perhaps, a decision support system design theory to a particular set of requirements produces better results than applying another type of design theory to the same requirements (Walls et al., 1992). What constitutes a contribution to knowledge with design-type research according to March and Smith (1995) and Gregor (2002) are:

- In the theory-building phase, the value or utility to a community of users is important, especially with the first instantiation of any artefact.
- "Building the first of any set of constructs, model, method or instantiation is deemed to be research, provided the artefact has utility for an important task. The research contribution lies in the novelty of the artefact and in the persuasiveness of the claims that it is effective" (March and Smith, 1995, p. 260).
- With research that builds subsequent constructs, models, methods and instantiations, judgement is based on 'significant improvement"; whether the artefact offers, for example, improvements such as better performance, efficiency or ease-of-use.
- In theory-testing, the evaluation of artefacts is worthwhile design theory research. Different artefacts can be evaluated with respect to different metrics. For example, evaluation of constructs tends to involve completeness, simplicity, elegance, and ease of use. Models are evaluated in respect of their fidelity with real world phenomena, completeness, level of detail, robustness, internal consistency and usefulness in practice. Evaluation of methods considers functionality, efficiency, generality, and ease of use. For example, systems development methods can be evaluated regarding the quality of results obtained by analysts applying the methods.

In addition, it is assumed that the general design principles represented in the artefact are articulated clearly so that they can be followed and tested by others. Simon (Simon, 1969) saw the design process as being concerned with finding a satisfactory design, rather than an optimum design. He believed that "*both the shape of the design and the*

shape and organisation of the design process are essential components of a theory of design" (Simon, 1969, p. 130). Cross (2001) on the other hand gives less importance to theory but stresses knowledge that is acquired through the process of building the artefact.

4.5 The Action Design Research (ADR) Methodology

ADR straddles design research and action research. From this perspective, ADR can be said to focus on changing IS design and development practices through problem solving in response to specific client needs. ADR is an action-oriented research methodology. The purpose of any action-oriented research is to generate knowledge that can be used to address practical concerns of organizations (Small and Uttal, 2005). Action-oriented research projects can focus on any issue or concern and usually have some type of change (e.g., individual, social, organizational) as a goal. Common to nearly all action-oriented research approaches is that they involve some type of collaboration between researchers and practitioners.

Because of the nature of the research problems addressed, an important principle of action-oriented research is that understanding cannot be achieved independent of its context, time, and place. Action-oriented research projects may resemble case studies in that the focus is usually on gathering information that will inform the specific situation and not on how the findings might be generalized elsewhere (Small and Uttal, 2005). Another principle of action-oriented research is the idea that research can never be value free. This idea is common among the views of many in the field of interpretive research (Walsham, 1995). Action-oriented research calls for heightened attention to how power

and trust shape the relationship between partners and how this relationship shapes the findings of the project. The practitioners' perspective is kept at the forefront to ensure that the researcher's view does not dominate the way knowledge is created and defined. For the research findings to be useful, they must be constructed in a way that is meaningful to stakeholders outside of academia.

Action-oriented research such as ADR assumes that valid knowledge comes from a variety of sources and that academic and practitioners each possess valuable knowledge, practices, and insights that can contribute to the success of a research project (Strand et al., 2003). DeVault (1999) observed that researchers need specialized skills and must devote more sustained attention to any investigation than is usually practical for practitioners. Conversely, using research results effectively to promote change requires the pragmatic evaluative and strategic skills of practitioners, honed through more daily participation in front-line work than most researchers experience. Together, researchers and practitioners can combine their different kinds of knowledge and skills to produce insightful and usable findings (Small and Uttal, 2005). Similarly, Van de Ven describes engaged scholarship as a participative form of research for obtaining the views of key stakeholders to understand complex problems (Van de Ven, 2007). By exploiting differences between these viewpoints, he argues that engaged scholarship produces knowledge that is more penetrating and insightful than when researchers work alone. According to Costello et al. (2011), engaged scholarship has a number of facets:

1 A form of inquiry where researchers involve others and leverage their different perspectives to learn about a problem domain;

2 A relationship involving negotiation, mutual respect, and collaboration to produce a learning community;

3 An identity of how scholars view their relationships with their communities and their subject matter.

According to Mathiassen, et al. (2008), engaged scholarship undertakes the challenge of conducting research that advances science while at the same time enlightening professional practice. In Van de Ven's view, in order to achieve this, researchers must increase the likelihood of advancing knowledge for science and practice by engaging with practitioners and other stakeholders in four ways;

- *Informed basic research* that is undertaken to describe, explain, or predict a social phenomenon;
- *Collaborative basic research* is similar to informed basic research, but it entails a greater sharing of power and participation between researchers and stakeholders;
- *Design and evaluation research* focuses on normative knowledge related to design and evaluation of policies, programs, and models for solving practical problems within a profession; and
- *Action research* applies intervention to address a problem of a specific client while at the same time contributing to academic knowledge.

ADR engages practitioners predominantly through both design and evaluation research and action research. ADR focuses on normative knowledge related to design and evaluation of policies, programs, and models and uses this knowledge to apply interventions to address a design problem of a specific client, while at the same time contributing to academic knowledge. It also entails considerable sharing of power and participation between researchers and stakeholders.

Mathiassen & Nielsen (2008) argue that the degree of collaboration with stakeholders is an important distinguishing feature of engaged scholarship in IS research. However, variation in stakeholder collaboration not only helps distinguish different forms of 'basic research', it applies equally well to distinguishing forms of 'design and evaluation research' and 'action research'. They propose a similar way of classifying forms of engaged scholarship within IS research:

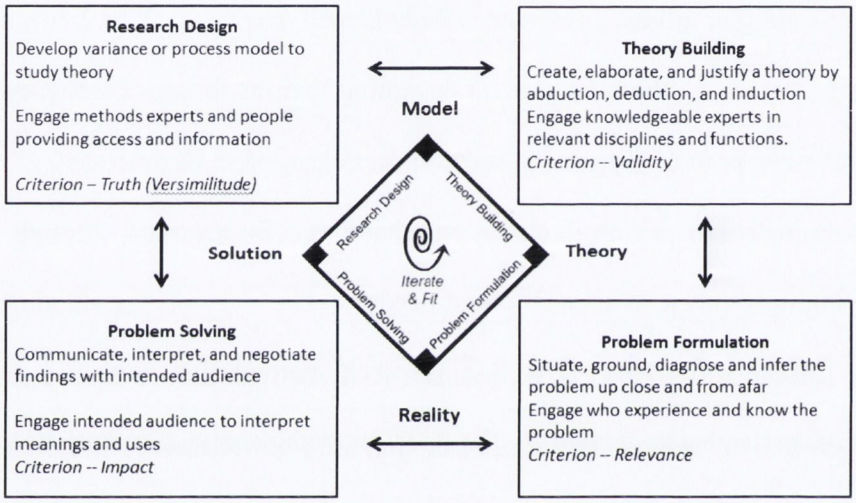
1. *Practice research* which focuses on understanding IS practices with the purpose of informing or advising relevant stakeholders.
2. *Design research* which focuses on designing various forms of software products with the purpose of supporting stakeholders engaged in IS practices.
3. *Action research* which focuses on changing IS practices through problem solving in response to specific client needs.

Sein et al. (2011) argue that ADR is a research method that explicitly recognises software products as being shaped by the interests, values, and assumptions of a wide variety of communities of developers, investors, and users, without letting go of the essence of design research i.e. innovation and dealing with a class of problems and systems. These interpretations of the ADR methodology link it strongly to the concept of engaged scholarship i.e. "a participative form of research for obtaining the views of key stakeholders to understand complex problems" (Van de Ven, 2007: p. 9). Figure 4.3 shows Van de Ven's representation of engaged scholarship for problem solving. According to him, engaged scholarship involves four stages. These stages can happen in any sequence:

1. Problem formulation – situate, ground, diagnose, and infer the research problem by determining who, what, where, when, why, and how the problem exists up close and from afar.

2. Theory building – create, elaborate, and justify a theory by deductive, and inductive reasoning.
3. Research design – develop a variance or process model for empirically examining the alternative theories.
4. Problem solving – communicate, interpret, and apply the empirical findings on which alternative models better answer the research question about the problem.

Figure 4.3 Engaged scholarship for problem solving (Van de Ven, 2007)



When engaged scholarship takes place within the context of a software design and development environment, Sein et al, (2011) claim ADR as an appropriate research methodology. ADR effectively combines two rich research traditions from the action research domain and the design science domain.

Typically, in IS projects, ADR (1) addresses a problem situation encountered in a specific organizational setting by intervening and evaluating; and (2) it constructs and evaluates a software product that addresses the class of problems typified by the encountered situation (Sein et al., 2011).

Since the ADR methodology focuses on information systems, it deals with certain critical issues that do not arise in other settings (Sein et al, 2011). First, evaluation of the IS cannot be sequential as suggested in prior, stage-gate models of DSR. Second, controlled evaluation efforts are difficult to design and conduct. Finally, innovation must be defined for the class of IS being built (Sein et al, 2011). To address these issues, the ADR methodology specifies a number of stages and key principles that should guide the organization of the research work within each stage. The stages and principles, as explained by Sein et al. (2011), are the following:

- Stage 1: problem formulation;
    - Principle 1: Practice-Inspired Research
    - Principle 2: Theory-Ingrained Artefact
- Stage 2: building, intervention, and evaluation (BIE);
    - Principle 3: Reciprocal Shaping
    - Principle 4: Mutually Influential Roles
    - Principle 5: Authentic and Concurrent Evaluation
- Stage 3: reflection and learning;
    - Principle 6: Guided Emergence
- Stage 4: learning formalisation.
    - Principle 7: Generalized Outcomes

4.5.1 ADR Stage 1: Problem Formulation

The trigger for the first stage of the ADR methodology occurs when a problem is perceived in practice or anticipated by researchers. It provides the impetus for undertaking the task of formulating the research problem. The problem formulation

stage identifies and conceptualizes a research opportunity based on existing theories and technologies (Sein et al., 2011).

Principle 1: Practice-Inspired Research

This principle emphasizes viewing field problems (as opposed to theoretical puzzles) as knowledge-creation opportunities. ADR seeks these opportunities at the intersection of technological and organizational domains, although the degree of novelty can vary across the two. The intent of the ADR team should not be to solve the problem per se as a software engineer or a consultant might wish to do. Neither should it be only to intervene within the organizational context of the problem. Instead, the ADR researcher should generate knowledge that can be applied to the class of problems that the specific problem exemplifies. As a result, the research activity is problem-inspired (Markus, Majchrzak and Gasser, 2002).

Principle 2: Theory-Ingrained Artefact

This principle emphasizes the circumstance that the ensemble artefacts created and evaluated via ADR are informed by theories. To define what constitutes a theory, Sein et al (2011) used Gregor's (2006) criterion of "the power to generalize." Gregor considers systems of statements that allow generalization and abstraction to be theories. The level of predictive power can vary, and theories can range from universal laws to ones with more restricted scope, such as the technology acceptance model (TAM). Sein

et al (2011) believe that Gregor's theories of Type IV (explanation and prediction theories) or Type V (design theories) are likely candidates for ADR.

4.5.2 ADR Stage 2: The Building, Intervention and Evaluation (BIE) Stage

The second stage of ADR uses the problem framing and theoretical premises adopted in stage one. These premises provide a platform for generating the initial design of the IT artefact, which is further shaped by organizational use and subsequent design cycles. Carried out as an iterative process in a target environment, this phase interweaves the building of the IT artefact, intervention in the organization, and evaluation (BIE). The outcome of the BIE stage is the realized design of the artefact. During BIE, the problem and the artefact are continually evaluated, and the design principles are articulated for the chosen class of systems (Sein et al., 2011).

Principle 3: Reciprocal Shaping

This principle emphasizes the inseparable influences mutually exerted by the two domains: the IT artefact and the organizational context. The ADR team may engage in recursive cycles of decisions at finer levels of detail in each domain (Sein et al., 2011).

Principle 4: Mutually Influential Roles.

This principle points to the importance of mutual learning among the different project participants. ADR researchers bring their knowledge of theory and technological

advances, while the practitioners bring practical hypotheses and knowledge of organizational work practices (Sein et al., 2011).

Principle 5: Authentic and Concurrent Evaluation

This principle emphasizes a key characteristic of ADR, that evaluation is not a separate stage of the research process that follows building. Instead, decisions about designing, shaping, and reshaping the ensemble artefact and intervening in organizational work practices should be interwoven with on-going evaluation (Sein et al., 2011).

4.5.3 ADR Stage 3: Reflection and Learning

The reflection and learning stage moves conceptually from building a solution for a particular instance to applying that learning to a broader class of problems. This is a continuous stage which works in parallel with the first two stages. At this stage it is critical to perform conscious reflection on the problem framing, the theories chosen, and the emerging ensemble. This is to ensure that contributions to knowledge are identified. It is also important to adjust the research process based on early evaluation results to reflect the increasing understanding of the ensemble artefact (Sein et al., 2011).

Principle 6: Guided Emergence

This principle captures a vital trait of ADR, which is the interplay between two seemingly conflicting perspectives: that of design and emergence. It emphasizes that the software product will reflect not only the preliminary design created by the ADR team

but also its on-going shaping by end users, perspectives, and participants, and by outcomes of authentic, concurrent evaluation (Sein et al., 2011).

4.5.4 ADR Stage 4: Learning Formalisation

The objective of the fourth stage of ADR is to formalize the learning. Following Van Aken (2004), the situated learning from an ADR project should be further developed into general solution concepts for a class of field problems. Casting the problem-instance into a class of problems facilitates this conceptual move. Researchers outline the accomplishments realized in the IT artefact and describe the organizational outcomes to formalize the learning. These outcomes can be characterized as design principles and with further reflection, as refinements to theories that contributed to the initial design.

Principle 7: Generalized Outcomes

Generalization is challenging because of the highly situated nature of ADR outcomes that include organizational change along with the design and development of a software product. The resulting set is, by definition, a bundle of properties in different domains. This set represents a solution that addresses a problem (Sein et al., 2011). Both solution and problem can be generalized. This move from the specific-and-unique to generic-and-abstract is a critical component of ADR. Sein et al. (2011) suggests three levels for this conceptual move: (1) generalization of the problem instance, (2) generalization of the solution instance, and (3) derivation of design principles from the design research outcomes.

4.6 The Methodological Framework for This Research: A Mixed Methods Approach

As noted in the introductory chapter, a large part of the research that underpins this dissertation was integrated within a commercial software (henceforth, the product) development project. The principle research methodology is ADR, which was first devised by Sein et al (2011). Accordingly, the research itself is seen as an ADR project. Throughout the research, the Author (i.e., the author of this thesis) was embedded in the company that was developing the product. In the research project, ADR plays the role of an overarching methodological framework, effectively a sort of meta-methodology, within which, at different stages, we use methods prescribed by other methodologies, i.e. a survey, semi-structured interviews and focus groups, to carry out the learning required by the ADR. From within the overarching framework in which the ADR methodology plays the organizing role, this research employs a combination of both qualitative and quantitative research methods. The next two sections outline and motivate the steps of such multi-method approach, with a greater emphasis on those which occurred during the more advanced stage of the project, i.e. the 'Formalized ADR' stage, which will be described in greater detail later in dedicated chapters. The subsequent section outlines, for each step and for the research methods used at each step, relevant ethical considerations. The final section concludes.

4.6.1 Methodological Steps

In what we defined (in the introductory chapter) as the *exploratory stage* of this research, i.e. essentially before the Viva Voce defence, we first reviewed the literature

on privacy and privacy concerns, as well as cognate fields such as the IS literature on trust. In retrospect, from the point of view of the formalized ADR methodology that we later adopted, this can be seen as a first step undertaken to initiate the organizational learning required to carry out the ADR project and both the research and the product development tasks within it. In broad terms, the objective of this initial step was to identify the privacy risk management features to include in the product. Along the same lines, still within the exploratory stage and without awareness of the potential of the project as an instance of ADR, we then conducted a survey of online behaviour, mainly focussing on IS users attitudes towards privacy, on their privacy concerns and on the online behaviour that they deploy to manage the risk of threats to their online privacy.

The online questionnaire was originally made up of questions previously validated by the literature and the questions were subsequently fine-tuned, after a series of reviews from both academics and fellow PhD students, to better reflect the needs of this research. The main reason for altering these questions was that the original questions were seeking to capture a variety of constructs traditionally considered in the IS literature on privacy, such as propensity to trust (Malhotra, Kim, & Agarwal, 2004) and informational privacy concern (Dineva & Hart, 2004; Smith, Milberg, & Burke, 1996), whereas, for the purpose of this research, we needed questions to more specifically instrument for the variables that influence individuals' willingness to disclose personal information online and risk handling behaviour. The questions for measuring privacy risk handling behaviour were not taken directly from Drennan et al (2006), but their work was a significant influence.

Out of a concern that a number of constructs, including aspects of risk and ambiguity aversion and heuristic biases such as 'availability', 'representativeness' and 'anchoring and adjustment', were measured weakly or inadequately by the online questionnaire, we carried out twenty semi-structured interviews primarily with the aim of gathering more conclusive evidence on the presence of such biases and, more generally, to clarify issues and relations between variables that were not clarified by the questionnaire. The semi-structured interviews were conducted two months after the questionnaire was completed by respondents, in the spring of 2011. The interviews focussed especially on ascertaining the presence of heuristic bias among respondents in relation to their willingness to disclose personal information and on understanding their risk handling behaviour.

These activities provided the essential insight that was required to characterize the second stage of the research, i.e. the stage that took place after the Viva Voce defence and to which we referred earlier as the *formalized ADR stage*, as an ADR project. These activities provided insight that proved essential in the development of the RPC model and to help refine it. For example, after we developed a first formulation of the model, we used the result of the survey, i.e. the questionnaire and semi-structured interviews, to test it. The results of the tests were discussed with the rest of the development team and other stakeholders and helped us understand the product that we were trying to develop as well as the model of privacy-related decision making that we hoped would offer guidance in such development endeavour. This led to substantial refinements of the model and, eventually, to the formulation given in the final part of chapter 3.

This iterative refinement of theory based on empirical evidence and intra and inter-organizational engagement is a distinctive trait of the ADR methodology. For reasons of space and to allow the reader to focus on the part of the research that produced the more substantive results, however, the tasks undertaken during the exploratory stage shall not be discussed further. After developing the formulation of the RPC model given in the final part of chapter 3, we used the results of the survey, i.e., the questionnaire and semi-structured interviews, which had been conducted during the earlier stage of the project, to subject the model itself to extensive tests, based on multivariate regression analysis of the questionnaire results and on the in-depth analysis of the semi-structured interviews. The relatively favourable nature of the findings of this step led us to undertake the more salient step of the ADR methodology, i.e. we used the model to guide the derivation of design principles for the development of a privacy risk management electronic postal system. The latter was then embedded in a prototype of the commercial product. Because the building of privacy into commercial IS technologies must be done in a systematic way, existing best practices and guidelines, i.e. those based on the concept of PbD introduced by Cavoukian (1998) and which builds on the FIPs outlined by the Organization for Economic Cooperation and Development (OECD) in 1980 (Gellman, 2012), are also used to aid in the development of the privacy risk management electronic postal system. These were taken into consideration when developing the product for its first release cycle, and the RPC Model.

The first version of the commercial product, once ready, was then subject to tests to assess the extent of user satisfaction with and, more generally, user reaction to its features. The results of these test were then used to make inferences on the privacy

design principles that guided the development of the privacy risk management information system embedded in the product and therefore, indirectly, to test our RPC Model (which is used to guide the derivation of the design principles in the first place). More specifically, a series of focus groups were conducted to ascertain the level of acceptance among users of the product and we used the feedback from the focus group to draw indications on the validity of the RPC Model that, in conjunction with PbD principles, guided the development of the product.

4.6.2 Qualitative and Quantitative Research Methods Combined

For some time, there has been growing recognition of the value of qualitative methods in social, behavioural, organizational, and evaluation research. This recognition is manifest in studies and research methodology texts such as Kaplan and Duchon, (1988) and Ghauri and Gronhaug (2010). While quantitative methods have many advantages, one significant drawback is that such studies are restricted to readily measured static constructs, they neglect aspects of cultural environment, and social interaction and negotiation that could affect not only the outcomes, but also the constructs under study (Kaplan and Duchon, 1988). These aspects often underlie information systems research, and interpreting information systems in terms of social action and meanings has been popular for a number of decades, as evidence has shown that information systems development and use is a social as well as technical process that includes problems related to social, organizational, and conceptual aspects of the system (Kling & Scacchi, 1982; Lyytinen, 1987).

When research involves such aspects of a technical system, as it is the case in the present study, it is believed that combining qualitative methods with quantitative methods provides a richer, contextual basis for interpreting and validating results (Bonoma, 1985). Combining these methods introduces both testability and context into the research. Collecting different kinds of data by different methods from different sources provides a wider range of coverage that may result in a fuller picture of the unit under study than would have been achieved otherwise (Bonoma, 1985). Moreover, using multiple methods increases the robustness of results because findings can be strengthened through triangulation, i.e. the cross-validation achieved when different kinds and sources of data converge and are found congruent (Bonoma, 1985; Benbasat, 1984).

Ghauri and Gronhuag (2010) define triangulation of data as the combination of methodologies in the study of the same phenomenon. Through data triangulation, the accuracy of results can be improved by collecting data through different methods or even through collecting different kinds of data. Additionally, mixed methods are used to enhance the validity of the research when correctness or precision is important. Triangulation of data can cause issues to emerge within the research study that may not have previously been observed. Sometimes, with a mixed method approach, it can be difficult to judge whether the results of the methods employed are consistent or not. Different methods can come up with contradictory results. This may be perceived as problematic, but contradictory results often result in a better understanding of the phenomenon under study and new research questions. Triangulation is particularly useful in IS research to check for method bias. Using multiple methods to examine the

same phenomenon and checking for consistencies enhances confidence in research analysis and results (Ghauri and Gronhaug, 2010).

4.6.3 Ethical Considerations in the Project

The questions contained within the online questionnaire, semi-structured interviews and focus groups were designed to elicit information from the participants regarding their perception of online privacy. Due to this, some questions may have been considered personal by some participants and as a result, they may have been unwilling to answer such questions. In order to eliminate this concern, the first page of the questionnaire informed the participants of the code of ethics that the researcher was following and the level of data collection necessary for completing the questionnaire. This information sheet, was also given (with slight modifications) to the members of the semi-structured interviews and the focus groups at the beginning of each interview process and each participant was given time to read it and ask any questions they had. Even though we were not allowed to participate in the focus groups, the research company carrying out the focus groups agreed to distribute the one page information sheet and agreed to comply with what was stated on the sheet. This information sheet can be viewed in Appendix C of this work.

The anonymity of all participants was fully guaranteed, except for the focus groups where participants were informed prior to taking part that their first name would be required to take part and that a recording of the focus group was taking place. While giving such detail and information was important to meet the high ethical standards which informed this research, it was also essential to ensure that privacy concerns

experienced by participants did not introduce a bias in the questionnaire itself or in the responses given during the interviews and focus groups. Additionally, these ethical considerations were clearly repeated in all the emails that were sent when requesting participation.

Regarding the questionnaire, completion of the questionnaire was voluntary and an option was given to all participants at the end of the questionnaire to submit their email address if they were willing to participate in follow-up interviews. By not submitting their email address, all respondents were ensured anonymity. Participants of the semi-structured interviews and the focus groups were guaranteed that all recording used during the interview time would be stored securely and not used for any other purposes other than the current research. All respondents were informed prior to participation of the estimated length of time of the survey and they were given a contact email address that they could contact if they wished further information regarding the research. It is important to note here that to a degree, anonymity will be reduced by questions seeking a participant's age, gender or profession. However, there is an option in the questionnaire/interview/focus group to skip any questions if desired.

4.7 Conclusion

In this chapter, we examined qualitative and quantitative research methods and their advantages and drawbacks, before putting forth the methodological framework for the research that lies at the heart of this dissertation. We considered methods used both in social sciences and engineering, placing relatively more emphasis on methods used in IS to investigate problems related or similar to those that emerge in the study of privacy

and privacy-related decisions of IS users, and conceptualized the research project that underpins this dissertation as an instance of ADR, though this perspective only emerged as the project progressed. A key methodological implication of viewing the research project in this way is that it rationalizes the mixed-method approach that was adopted to carry out the learning required at the different stages of the project itself. The chapter outlines and motivates both the methodological steps undertaken as part of the study and the methods of inquiry to which we resorted within each step. Such steps, and the associated methods, are described and discussed in detail in later chapters. The chapter also offers a discussion of ethical considerations arising within each step.

5 The Survey: the Questionnaire and Semi-Structured Interviews

This chapter outlines the results of the preliminary empirical analysis and testing of the RPC model during the initial stages of the ADR project. The survey was conducted to make inferences on the relations between constructs implied by the PC models considered in chapter 3, i.e. the traditional formulation and the revised one put forth in an effort to enrich the model with insight from psychology and the behavioural economics literature, thereby at the same time offering an assessment of the validity of the constructs defined by these models. Ultimately, using the survey, we tested the models and used the results of this analysis to draw indications for the subsequent stages of the ADR project.

As outlined in chapter 4, the first step of the survey was an online questionnaire, which was followed by a regression analysis of the findings and semi-structured interviews. The target population was adult IS users in Ireland. This is admittedly only a small subset of a possibly much larger population of interest. For example, it would be interesting to survey samples drawn from a population including IS users in different countries, not least because international socio-cultural differences might influence online behaviour, and include non-IS users as well as IS users. Due to resource availability and time constraints, we leave these questions to future research. In the regression analysis of the results, however, we did introduce control variables, as shall be explained later in the chapter, so as to indirectly and at least to partially control for some of these influences.

In the next section, we describe the online questionnaire, motivate the choice of questions used to capture constructs defined within the PC model and the revised version thereof, with special emphasis on privacy concerns and their antecedents and how they can be used to identify observable proxy variables for privacy risk and privacy risk aversion. We then explain how the data gathered from the questionnaire is analysed, how this data and multiple linear regression are used to test implications of extant theories of privacy and especially of our RPC model, and the results of this analysis. We then describe and analyse the semi-structured interviews. A discussion of the implications of the findings is offered in the final section.

5.1 The Questionnaire

The majority of questions in the questionnaire were drawn from existing instruments cited within the literature, reviewed in chapter 2, but modified to reflect the needs of this research. Given the difficulty of forming a sample representing the 'true' population, or even of defining ex-ante an appropriate sampling scheme, we also asked the respondents to provide information on variables that may be correlated with un-modelled socio-demographic influences on attitudes to privacy, so as to be able to use them as control variables in the regressions estimated in subsequent tests of the PC model.

The sources from where the original questions were taken are given in Appendix C. As a first step of the process that lead to the final formulation, a preliminary draft of the questionnaire was presented to an academic with significant expertise in instrument

design. As a result of this review, the questionnaire underwent considerable redrafting, which incorporated the expert's recommendations, with significant changes being made to the layout and content of the questionnaire. This included changes to the position and structure of the questions and the addition of new questions, not previously considered by the literature.

Once these recommendations were implemented and some further revision had been carried out to ensure clarity and readability, the questionnaire was circulated among a group of fellow PhD students. Their recommendations were also considered and a selection of the recommendations was implemented. The questionnaire was then presented at a doctoral forum where further feedback from fellow PhD researchers and academics was received and applied. The questionnaire was then first piloted on a small scale sample of subjects and then administered to a larger sample of the target population, i.e. IS users in Ireland.

The next section briefly describes the pilot survey and follow-up interviews. We then give details on the questions included in the final configuration of the questionnaire and their mapping to constructs of interest, including a discussion of how we use the privacy concern construct, previously considered by the literature, to proxy for privacy risk perception and risk aversion, and a discussion of the statistical rationale for how the constructs are sampled. We then describe the distribution of the questionnaire and the regression analysis of the results. The final section summarizes our main findings and concludes the chapter.

5.1.1 Preliminary Steps: The Pilot Survey and Follow-up interviews

The sample population for the pilot questionnaire was a snowball sample of participants which consisted of 60 friends on the social networking site Facebook and 20 academics and doctoral students from various universities. The response rate for the pilot was high (66%). In general, feedback from the pilot survey was positive. The questionnaire was seen to be of reasonable length and well written in that each question was understandable. A considerable number of respondents availed of the open question at the end of the survey to provide feedback. We had requested them to do so when distributing the pilot questionnaire. Therefore, many immediate issues that the respondents encountered were recorded within the open questions.

An interesting finding that appeared a number of times throughout the pilot survey feedback was the question of individuals taking "responsibility" for what they put on the Internet. It seems that the participants of the pilot survey saw a need for individuals to take responsibility for their own online privacy by educating themselves about the risks they take when submitting their private information online and being aware of the possible implications. Samples of comments made by participants include:

> *"I think people should be aware of putting compromising material onto the net, but there also has to be a network and retailer level of commitment to non-abuse of material or it will lead to withdrawal of data or people submitting incorrect data to 'fool' the system."*

"To me, online privacy is not a reliably regulated right to having risk-free online experiences. It's more of a skill that is developed by using common sense, skepticism, and extreme caution."

"There should always be the possibility to contact the parties with whom you do business. Most issues can be resolved this way. However, any business dealings involve some kind of risk, and we should know what steps to take to minimize that risk, or what we can do in the event that our privacy is compromised."

Another suggestion that arose from the feedback was that there should be questions regarding whether online users are aware of the technology being used on each website to safeguard online privacy. For example, it was suggested that there should be questions regarding whether users are aware of privacy seals and of the fact that, to indicate that the site has encryption enabled, there should be a small icon resembling a lock in the bottom right part of the browser.

When the pilot survey was complete and all suggested changes were made to the questionnaire, it was presented again to the same academic with expertise in instrument design. This time, she was reasonably satisfied with the content of the questionnaire. She made a few recommendations in terms of improving clarity and structure, which were implemented.

A series of seven follow up interviews were conducted with a selection of respondents to the pilot questionnaire. These respondents talked their way through the questionnaire, highlighting issues as they were coming across them. The main reason for these

interviews was to address any issues that respondents may have overlooked the first time they completed the questionnaire. Once these interviews were complete, the questionnaire was amended and reviewed by the interviewees one final time to ensure each issue had been satisfactorily resolved. The questionnaire was then ready to be distributed to the target population.

5.1.2 Mapping between Survey Questions and Constructs

The final set of questions in the online questionnaire is set out in Table 5.1 (which continues over a number of pages). From the questionnaire, we sought to sample proxy measures for nine constructs, i.e. (1) willingness to disclose personal information (*Willingness*), (2) perceived benefit from doing so (*PerBen*), (3) perceived risk (*PerRis*) in doing so, (4) propensity to trust (*PropTru*), (5) importance placed on trust (*ImpTru*), (6) control preference (*ContPref*), (7) ambiguity aversion (*AmbAver*), (8) availability bias (*Avail*) and (9) extent of (or propensity to engage in) risk handling behaviour (*RiskHand*). The questions on constructs (1) to (8) are based on the questions drawn from the literature and adapted as explained in the previous section, whereas the questions on construct (9) are, to the best of our knowledge, novel. This list of constructs includes all the constructs appearing in the RPC model, as per the flowchart in Figure 3.3, except the more situation-specific ones, e.g. sensitivity of the personal information required for the interaction, which would be very difficult to sample using standard survey methods. That is, in the survey, we only attempt to capture variation of attitudes and self-reported behaviour across subjects rather than variation of behaviour across circumstances (per subject or classes thereof). Smith et al. (2011) acknowledge that this is a common limitation of empirical studies in the literature on informational

privacy, which we seek to address in part by carrying out semi-structured interviews and in part by employing ADR as our overarching methodological framework in subsequent chapters.

The survey uses the following number of questions to investigate each one of the nine constructs, based on those considered in the diagrammatic representation of the model in Figure 3.3, as well as essential demographic information (as already mentioned, the full set of questions can be found in Table 5.1):

1. Willingness to disclose personal information (4 Likert-scale questions)
2. Perceived benefit (5 Likert-scale questions)
3. Perceived risk (2 Likert-scale questions)
4. Preference for informational control (4 Likert-scale questions)
5. Ambiguity aversion (4 Likert-scale questions)
6. Propensity to trust (4 Likert-scale questions)
7. Importance placed on trust (1 Likert-scale question)
8. Potential for availability bias (1 main question)
9. Risk handling behaviour (7 Likert-scale questions)
10. Risk handling behaviour before and after a breach (8 Likert-scale questions)
11. Age (1 question)
12. Sex (1 question)
13. Education level (1 main question)
14. Possession of a home computer (1 main question)
15. Computer use at work (1 main question)
16. Employment in the computer industry (1 main question)

The first set of questions, i.e. those drawn from the existing online privacy literature and focussing on the first seven constructs, were grouped by construct (as per Table 5.1), into matrices of choices. For example, the questions on *willingness to disclose personal* information, i.e. construct (1), are grouped in the matrix of choice shown in Figure 5.1. They are based on those taken from an instrument developed and validated by Dinev and Hart (2004), which itself was based on an original instrument developed by Smith et al (1996), and listed in Appendix C (the original seven point scale was reduced to five for consistency with other questions). Following feedback from the pilot focus-group, however, we modified somewhat both the wording of the questions and the definition of the scales for the answers, so as to increase the chance that the questions capture willingness to disclose personal information (i.e., propensity to do so) rather than concerns regarding doing so. The matrix of choices reported in Table 5.1 and shown in Fig. 5.1 reflects these changes.

Figure 5.1 Willingness to disclose personal information

6. In each of the following situations, how often do you supply personal information? When...

	Always	Frequently	Occasionally	Rarely	Never
A) Taking part in social networking	○	○	○	○	○
B) Being in with a chance to win something	○	○	○	○	○
C) Taking part in discussion forums	○	○	○	○	○
D) Paying bills	○	○	○	○	○
E) Carrying out activities such as online voting	○	○	○	○	○

Notes: The matrix of choice question for the construct "Willingness to disclose personal information".

The questions concerning the *perceived benefit* construct, i.e. construct (2), were a selection from those employed by Li and Keshelashvili (2006) and Hann et al. (2005) and listed in Appendix C[10], adapted to take into account suggestions made by the participants of the pilot study on how to increase the chance that the questions capture the construct of interest, and were put in the format of a matrix of choices.

The questions on *perceived privacy risk*, i.e. construct (3) in the list above, are based on questions used in the literature to measure privacy concerns and especially on those listed in Appendix C, which have been used by Dinev and Hart (2004) and Smith et al. (1996). This is because, as explained earlier, we view such concerns as antecedents to *perceived privacy risk.* The upshot of this approach is that privacy concerns are, at least in principle, observable whereas perceived privacy risk is situation-specific to an extent that it is difficult to measure with standard survey methods (this is a difficulty shared by the vast majority of studies on privacy concerns, as lamented by Smith et al. (2011)).

As far as *risk aversion* is concerned, a fully rigorous approach would require its estimation from observation of the individuals' willingness to take risks in a variety of situations, including in the personal and professional sphere and in their financial investment choices. This approach is, however, impracticable in our current circumstances and we leave it to future research. In this study, we use instead two alternative proxy variables for risk aversion. As it has been done, implicitly or explicitly, in previous empirical IS research on the PC (Phelps, Nowak and Ferrell,

[10] The questions that were included were selected based on their marginal contribution to the Cronbach's alpha of the composite score that, as explained later, would be constructed using the answers to the questions themselves.

2000; Dineva and Hart, 2004; Dinev and Hart, 2006; Castaneda and Montoro, 2007), the first proxy is *preference for* (*informational*) *control*[11], i.e. i.e. construct (4). The second proxy, is *importance placed on trust*, i.e. construct (5), because, as noted in Appendix B, previous literature has found that "trust mediates the relationship between privacy concern and willingness to transact online" (Belanger and Crossler (2011), but see also Van Slyke et al (2006)). Accordingly, we view the importance placed on trust by an individual as a positive antecedent of his/her risk aversion. To measure this construct, we asked survey participants whether "*When disclosing personal information online it is more important to trust the online third party to whom it is being submitted because it is important to be fully in control of how it is collected, used and shared*" and added this question to the matrix of choices for propensity to trust, i.e. construct (6) described below, anchoring the answers in the same way as for the questions used to measure the latter. We are, however, conscious that both proxy variables might be very context-specific and therefore that they might not fully capture the individual's risk aversion. While, as noted, we leave attempts to adopt a different approach to future research, we nonetheless sought to gain insight into whether this might be the case in the semi-structured interviews that followed the questionnaire.

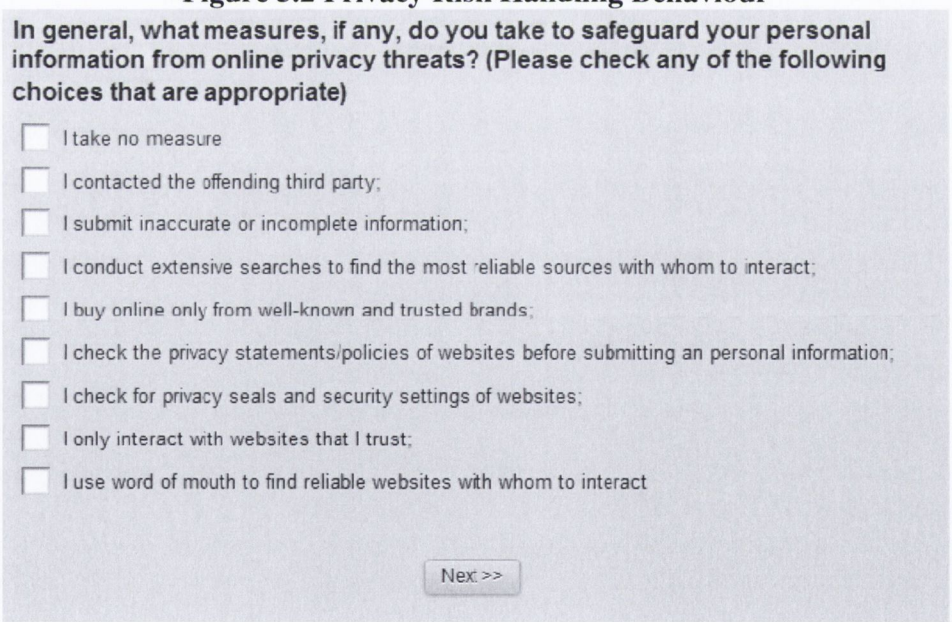
Questions on *trust propensity*, i.e. construct (4), closely reflect those used by Malhotra et. al (2004) and illustrated in Appendix C. Those on ambiguity aversion are based on the questions used by Malhotra et. al (2004) to measure individuals' "awareness of privacy practices", which we interpret as preference for control/disclosure regarding the

[11] As noted earlier, although privacy concerns have often been conceptualized as a multidimensional construct (Smith et al. 1996; Malhotra et al. 2004), the IS literature on privacy risk has placed special emphasis on the role of the potential loss of control over personal information as an antecedent to privacy concerns (e.g., Dinev and Hart 2006).

use of personal information. As for the potential for availability bias, i.e. construct (8), we asked the survey participants how often they had experienced privacy threat over the previous 6 months and sought answers along a 5-point Likert scale anchored at Always (Or Very Often) = 5 and Never = 1.

The second set of questions, which focus on *risk handling behaviour*, i.e. those on constructs (9) and (10), are based on those used by Drennan et al. (2006) and reported in Appendix C, and are shown in the format of a list of choices, as exemplified by the screenshot in Figure 5.2. While these questions are based on the questions from Drennan et al. (2006), they are used in a unique way for comparing differences between individuals who have recently experienced a (real or perceived) privacy breach and those who have not.

Figure 5.2 Privacy Risk Handling Behaviour



Notes: The list of choices for privacy risk handling behaviour from the online questionnaire.

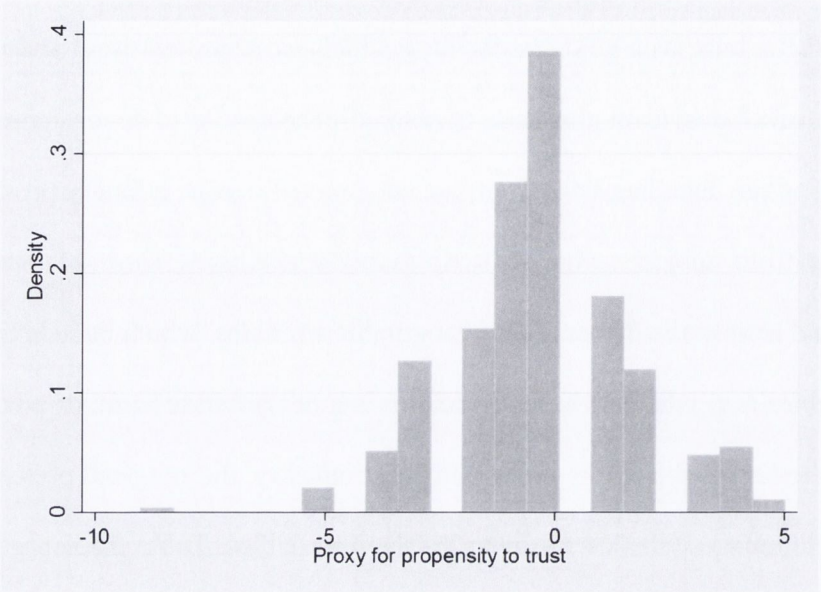
To sum up, the questions for constructs (1) to (8) were put in the form of matrix of choices whereas those for constructs (9) and (10) are put in the form of a list of choices. For the questions used to measure willingness to disclose personal information and the potential for availability bias, we used the five point Likert scale with Always (Or Almost Always) = 5, Frequently = 4, Occasionally = 3, Rarely = 2, and Never = 1, as shown in Figure 5.1. For all other questions put in the form of matrices of choices, each question in the matrices used the five point Likert scale with Strongly Agree = 5, Agree = 4, Neutral = 3, Disagree = 2, and Strongly Disagree = 1. For the questions concerning risk handling behaviour, instead, each question required a binary answer, with a 'tick' representing a positive answer ('Yes') and not ticking representing a negative answer ('No'). The questions concerning demographic circumstances were in a stand-alone format and formulated in the obvious way.

We used the survey results to generate variables to measure each one of the nine constructs. The construction of the key variables is summarized in the last column of Table 5.1. Following Yu (2011), the answers to questions put in the form of matrices of choice were combined to get a composite score for the corresponding construct. For example, there was one matrix of choice which measured a subject's level of informational privacy control preferences and the matrix consisted of four Likert scale questions. As outlined in Table 5.1, the scores on all four questions were added up to give a composite score for the construct. This process, as detailed in the table, was repeated for all questions put in the form of matrices of choice. For some constructs, we did not use the scores on all the questions included in the relevant matrix of choice and, in some cases, we used different subsets of questions from the same matrix of choices to construct variables for two or more constructs, as detailed in Table 5.1. We used

Cronbach's alpha, as well as the indications of the pilot study and of a preliminary analysis of the results, as a guide in deciding which scores to leave out and whether to use subsets of scores from the same matrix of choices for two or more different constructs. For risk handling behaviour, we constructed instead a binary proxy variable by assigning 1 to subjects who declared to undertake some form of risk handling behaviour and zero to the others. The demographic variables, which include age and the binary variables sex, whether the individual uses a computer at home or a computer at work and whether he/she works in the computer industry, did not need proxying. Table 5.2 reports summary statistics for many of these variables. Table 5.3 reports pairwise sample correlations between the variables.

An advantage of aggregating scores for individual answers into composite score variables is that the result is more likely to resemble a normally distributed random variable, leading to a greater efficiency of inference procedures and making it more meaningful to enquire about correlations and other measures of association between the variables and the underlying constructs. As an example of the distribution of the constructed composite score variables, Figure 5.3 plots the histogram of *PropTru*, i.e. the proxy for propensity to trust.

Figure 5.3 Propensity to Trust



Notes. This figure plots the constructed proxy for propensity to trust *PropTru*.

As can be seen from Table 5.3, Panel A, willingness to disclose is highly positively correlated with perceived benefit and negatively correlated with perceived risk. Age, education and the availability bias proxy, which is the dummy variable indicating whether the participant has experienced a privacy breach in the last six months, are also all negatively correlated with willingness to disclose personal information. From Panel B, which reports robust (conservative) Bonferroni-adjusted *p*-values of the test that the pairwise correlation is equal to zero, we see that willingness to disclose personal information is significantly correlated to perceived risk, perceived benefit, age and education. The fact that the sign of these correlations is coherent with the RPC model represents evidence of so called convergence validity of the constructs, to the extent that the values of constructed variables represent valid measurements of the constructs that they are designed to measure, and therefore preliminary evidence in support of how willingness to disclose personal information is explained within the RPC model.

Notably, the risk handling behaviour variable appears to be correlated to a significant extent to all variables, as shown in Table 5.3 Panel A. As suggested by the more conservative Bonferroni p-values reported in Panel B of this Table, however, the most significant association appears to be with the variables concerning using a computer at work and working in the computer industry (apart from the variables that are correlated by construction with *RiskHand*, that is those measuring risk handling behaviour under representativeness bias, i.e. *RepRiskHand*, and the change of risk handling behaviour under availability bias, i.e. $\Delta RiskHand$). This fact is coherent with the RPC model, to the extent that using a computer at work and working in the computer industry implies less binding limits to rationality, a lesser propensity to perceive ambiguity in online situations and ultimately a greater propensity to engage in risk handling behaviour. This represents evidence of convergence validity of the constructs, again to the extent that the values of constructed variables represent valid measurements of the constructs that they are designed to measure, and therefore preliminary evidence in support of how risk handling behaviour is explained within the RPC model.

The ambiguity aversion variable (*AmbAver*) is highly positively correlated with age. The perceived risk variable (*PerRis*) is negatively correlated with the propensity to trust variable (*PropTru*), suggesting that the two variables might be measuring, at least to some extent, the same construct. Though this is not desirable, we shall seek to overcome this problem in the specification of the multiple regression model that will be considered in the next section. It is hoped that, by simultaneously controlling for different, albeit imperfectly measured effects, their statistical identification will be possible.

While the coherence between the sign of the significant correlation coefficients in Table 5.3 offers, as noted above, preliminary evidence on the convergence validity of the constructs involved by the RPC model, the evidence in favour of so called discriminant validity of the constructs is less clear cut. Moreover, there are a number of significant correlations between various other variables that are not predicted by the model, though they are not ruled out either, suggesting that disentangling causality relations from mere correlations and (direct or indirect) reverse causality might be especially challenging.

Table 5.1 Questionnaire Constructs and Associated Proxy Variable

Questions Included in the Questionnaire for Each Construct and Associated Proxy Variable

	Construct	Associated Questions	Associated Proxy Variable	Proxy Variable Definition
1	Willingness to disclose personal information	In each of the following situations, how often do you supply personal information? When… (a) Taking part in social networking; (b) Being in with a chance to win something; (c) Taking part in discussion forums; (d) Paying bills; (e) Carrying out activities such as online voting; (f) Shopping online	$Willingness_i$	$Willingness_i = (a) + (b) + (c) + (e)$
2	Perceived benefit	(a) When submitting personal information online, the benefits outweigh the risks (b) I submit my personal information online for the convenience of being able to bank online; (c) I submit my personal information online for the convenience of being able to shop online; (d) I submit my personal information online for the convenience of paying bills this way; (e) When submitting personal information online there is potential for gain	$PerBen_i$	$PerBen_i = (a) + (b) + (c) + (d) + (e)$
3	Perceived risk	(a) When submitting personal information online, there is risk involved; (b) When submitting personal information online, there is potential for loss; (c) many unexpected problems can arise	$PerRis_i$	$PerRis_i = (a) + (b)$
4	Informational control preference (control preference-related proxy for risk aversion)	(a) To me online privacy is being able to control how my personal information is used; (b) To me online privacy is being able to feel confident that my personal information is safeguarded against inappropriate sale or loss; (c) My online privacy is threatened if I don't feel fully in	$ContrPref_i$	$ContrPref_i = (a) + (b) + (c) + (d)$

		control of the situation; (d) When disclosing personal information online it is more important to be in control of how it is collected, used and shared than to trust the online third party to whom it is being submitted		
5	Ambiguity Aversion	When I am asked to supply personal information in order to obtain a service that I need on a website and I feel that information is unnecessary, the website should: (a) Make the submission of that private information "optional"; (b) Explain clearly why I need to submit the personal information in return for the service I am seeking; (c) Have a clear statement that is readily accessible on the site of how a user's personal information will be used; (d) Provide a means of contacting the company to express your view or make a complaint	$AmbAver_i$	$AmbAver_i = (a) + (b) + (c) + (d)$
6	Propensity to trust	(a) In general, my perception of online companies is that they are mindful of my best interests when handling my personal information; (b) In general my perception of online companies is that they are truthful about their use of my personal information; (c) In general my perception of online companies is that they are motivated by their best interests, rather than mine, when handling my personal information; (d) In general my perception of online companies is that they are secretly collecting, using and selling personal information for their own competitive advantage; (e) When disclosing personal information online it is more important to trust the online third party to whom it is being submitted because it is important to be fully in control of how it is collected, used and shared	$PropTru_i$	$PropTru_i = (a) + (b) + (c) - (d)$
7	Importance placed on trust (trust-related proxy for risk aversion)	(a) In general, my perception of online companies is that they are mindful of my best interests when handling my personal information; (b) In general my perception of online companies is that they are truthful about their use of my personal information;	$ImpTru_i$	$ImpTru_i = (e)$

		(c) In general my perception of online companies is that they are motivated by their best interests, rather than mine, when handling my personal information; (d) In general my perception of online companies is that they are secretly collecting using and selling personal information for their own competitive advantage; (e) When disclosing personal information online it is more important to trust the online third party to whom it is being submitted because it is important to be fully in control of how it is collected, used and shared		
8	Potential for availability bias	(a) How often in the past 6 months have you experienced a potential threat to your online privacy?	$Avail_i$	$Avail_i = (a)$
9	Risk handling behaviour	In general, what measures do you take to safeguard your personal information from online privacy threats (all 0/1 binary scores): (a) I take no measure; (b) I contacted the offending third party; (c) I submit inaccurate or incomplete information; (d) I conduct extensive searches to find the most reliable sources with whom to interact; (e) I buy online only from well-known and trusted brands; (f) I check the privacy statements/policies of websites before submitting an personal information; (g) I check for privacy seals and security settings of websites; (h) I only interact with websites that I trust; (i) I use word of mouth to find reliable websites with whom to interact	$RiskHand_i$	$RiskHand_i = - (a) + (b) + (c) + (d) + (e) + (f) + (g)$
10	Change in risk handling behaviour following a privacy breach	If you have experienced a privacy breach in the last six month, what additional measures are you taking to safeguard your personal information that you were not taking before (all 0/1 binary scores): (a) I took no different measure than before; (b) I submit inaccurate or incomplete information; (c) I conduct extensive searches to find the most reliable sources with whom to interact; (d) I buy online only from well-known and trusted brands;	$dRiskHand_i$	$dRiskHand_i = - (a) + (b) + (c) + (d) + (e) + (f) + (g) + (h)$

		(e) I check the privacy statements/policies of websites before submitting personal information; (f) I check for privacy seals and security settings of websites; (g) I only interact with websites that I trust; (h) I use word of mouth to find reliable websites with whom to interact		
11	Age	How old are you?	Age_i	Integer numeric value of answer
12	Sex	Are you male/female?	$Gender_i$	1 for male and 0 for females
13	Education level	What was the last year in school/college that you completed? (a) Junior/Inter Certificate; (b) Leaving Certificate (or equivalent); (c) Some college (1-3 years); (d) College graduate (degree level); (e) Postgraduate (degree +); (f) Prefer not to answer	Education	Integer numeric value of answer
14	Home computer	Do you have a computer at home?	Home_comp	1 for yes and 0 for no
15	Work computer	Does your work involve spending time on a computer?	Work_comp	1 for yes and 0 for no
16	Employed in the computer industry	Do you work in the computer industry?	Comp_Indust	1 for yes and 0 for no

Note: We do not report results on all the questions in the online questionnaire because they do not appear to play an important role in the identification of the effects of interest and as such they are not essential for our inferences. In order to save space we omit to report results on analyses that include these variables. This is to focus on the results that are more relevant for the purpose of testing the revised privacy calculus model.

Table 5.2 Summary Statistics

Variable	Obs	Mean	Std.Dev.	Min	Max
Willingness	372	3.67	2.35	0	12
RiskHand	419	3.56	1.34	0	7
RepRiskHand	419	0.14	0.77	-2	1.5
ContrPref	383	10.21	2.32	0	12
AmbAver	419	18.88	2.99	10	25
PerRis	411	6.59	1.19	2	8
PerBen	371	12.72	3.56	0	20
PropTru	419	-0.33	2.00	-9	5
ImpTru	376	1.53	0.50	1	2
Avail	419	3.10	2.16	0	6
dRiskHand	376	0.87	1.47	-1	5
Age	371	3.39	1.16	1	6
Education	367	5.13	1.01	2	6
Home_comp	370	0.99	0.10	0	1
Work_comp	373	0.99	0.12	0	1
Comp_ind	370	0.24	0.42	0	1

Notes. This table reports summary statistics, i.e. number of available observations, sample mean and sample standard deviation, minimum and maximum, for the variables that measure the nine constructs and for the demographic variables.

Table 5.3 Correlation Matrix

Panel A

	Willingness	RiskHand	RepRiskHand	ContrPref	AmbAver	PerRis	PerBen	PropTru	ImpTru	Avail	dRiskHand	Age	Gender	Education	Home_comp	Work_comp	Comp_ind
Willingness	100.00																
RiskHand	-7.44	100.00															
RepRiskHand	-4.09	**22.37	100.00														
ContrPref	-1.72	**13.81	7.94	100.00													
AmbAver	-3.37	**-12.99	-4.50	**16.11	100.00												
PerRis	**-19.93	**11.38	-3.40	**15.33	**10.64	100.00											
PerBen	**31.73	**10.97	1.03	-2.28	2.36	-7.83	100.00										
PropTru	7.65	**-10.28	1.88	*-9.26	**12.72	**-17.93	**13.39	100.00									
ImpTru	-6.70	**11.15	**12.06	-6.51	-1.23	2.90	**16.01	**11.09	100.00								
Avail	*-9.77	**10.36	*9.48	5.46	**-22.02	**14.54	**-13.32	**-11.42	-2.31	100.00							
dRiskHand	2.27	**27.77	-7.50	6.71	*-9.21	**18.21	-1.96	**-16.22	-6.68	4.91	100.00						
Age	**-37.26	**12.74	5.81	7.38	**19.37	**18.89	-0.31	-3.96	4.61	*8.83	-4.55	100.00					
Gender	5.07	*-8.65	8.27	0.06	**11.95	-7.70	6.47	*9.27	-0.40	-2.74	**-20.99	-5.95	100.00				
Education	**-27.75	**17.21	4.04	4.15	**16.34	**17.02	*10.12	**-11.03	7.46	5.50	-2.37	**48.98	6.71	100.00			
Home_comp	6.55	**11.02	-1.06	6.76	6.63	5.06	-0.85	3.24	0.66	-1.88	*9.70	3.05	-3.74	7.23	100.00		
Work_comp	6.90	**-18.05	-3.97	1.86	-1.63	-3.74	-3.78	**10.52	-7.82	3.67	-6.89	2.07	-1.46	**-10.94	1.23	100.00	
Comp_ind	0.95	**22.47	-4.34	2.27	0.30	5.33	**16.70	7.67	**17.26	-2.53	**13.36	-2.08	**-22.10	0.92	-0.44	-6.43	100.00

Panel B

	Willingness	RiskHand	RepRiskHand	ContrPref	AmbAver	PerRis	PerBen	PropTru	ImpTru	Avail	dRiskHand	Age	Gender
Willingness													
RiskHand													
RepRiskHand		0.001											
ContrPref													
AmbAver													
PerRis	0.027												
PerBen	0.000												
PropTru						0.055							
ImpTru													
Avail					0.002								
dRiskHand		0.000				0.053							
Age	0.000				0.024	0.035							
Gender												0.015	
Education	0.000												0.000
Home_comp													
Work_comp		0.094											
Comp_ind		0.002											0.006

Notes. Panel A of this table reports the matrix of percentage pairwise correlation coefficients, each estimated the largest available number of observations, for the variables indicated in the first row and column. One and two asterisks denote significance at the 10 and 5 percent significance level. Panel B reports robust (conservative) Bonferroni-adjusted *p*-values of the test that the pairwise correlation is equal to zero. To improve legibility, we report only *p*-values not exceeding 10 percent, i.e. only those that indicate rejection at least at the 10 percent level of the null hypothesis of zero correlation. All variables are denoted as in the text.

Methodological note on Sampling of Constructs and Inferences

The univariate summary statistics in Table 5.2, the correlation coefficients in Table 5.3 and histograms like the one in Figure 5.3 all imply a parametric approach to modelling the relation between the variables under consideration. This approach relies on tests on the parameters of such relation, so called parametric tests, to formulate inferences on the relation of interest. Such tests are more efficient and yield more precise results (Motulsky, 1995; Saunders, Lewis and Thornhill, 2007; Ghauri and Gronhaug, 2010) than non-parametric ones[12] and are therefore widely used in social science research (Yu, 2011). The size of our sample is 420 individuals and therefore relatively large. In this situation, while parametric modelling requires the specification of the distribution of the variables that enter the distribution of interest, parametric tests are also robust to distributional assumptions. [13]

Likert-type scales, however, are technically ordinal scales. It is therefore not obvious that such an approach is applicable. The main argument against using parametric tests for Likert-scale data is that, as ordered categories, the intervals of Likert-scales are neither equal nor formally comparable and any parametric operation applied to them is thus formally invalid (Yu, 2011). From this perspective, nonparametric tests are more

[12] That is, they are more powerful against a specific null hypothesis of interest, though this is especially the case in the presence of small sample sizes.

[13] As argued by Motulsky (1995), the issue of choosing between parametric and non-parametric tests only arises when the sample size is small as appropriate transformations of test statistics, which typically involve averages of the variables entering the relations of interest, are guaranteed to be normally distributed, as a consequence of the Central Limit Theorem, regardless of the distribution of the variables themselves. Hence, the non-parametric tests are powerful enough and the parametric tests are robust enough when working with large samples that both categories of tests are sufficient to yield rigorous, reliable results. It is only small data sets that present a difficulty as the distribution of relevant statistics may depart more sharply from the normal, possibly in unknown ways.

appropriate for this type of data. A way around this difficulty is that, when considering Likert-scale data, once two or more Likert or ordinal items are combined, the number of possible values for the composite variable begins to increase (in our case beyond 5 categories) and a much stronger argument that these composite scores can be treated in the same way as 'continuous' variables can be put forth (Newsom, 2011). Thus, ordinal-scaled data is not 'inappropriate' for parametric tests (Yu, 2011). Like Newson (2011), Yu (2011) emphasises that, in place of a single Likert-scale, it is common to combine many items to produce a composite score, and by doing so, ordinal-scaled data is converted into a form of interval-scaled data or continuous-*like* data, thus making the use of parametric tests more valid for Likert-scale data. In our case, there are five categories within each Likert scale[14] and the composite scores are based on three or more such questions, suggesting that they can be treated as continuous.

5.1.3 The Distribution of the Online Questionnaire

As explained in the introduction to the chapter, the target population for the online questionnaire were *regular online adult users in Ireland.* An efficient approach to forming a representative sample would be to resort to stratified sampling, so as to form a sample as close as possible to random by explicitly modelling and removing possible biases introduced by the sampling scheme. In order to form a stratified sample, the population is typically divided up into a set of smaller separate sub-groups or strata. Then a simple random sample is taken from each stratum. The strata can be natural groupings, such as age ranges or ethnic origins. Stratified sampling is beneficial in that,

[14] Therefore it is possible, and very often researchers have done so, to treat them as continuous variables and use parametric tests to analyse them (Johnson and Creech, 1983; Zumbo and Zimmerman, 1993).

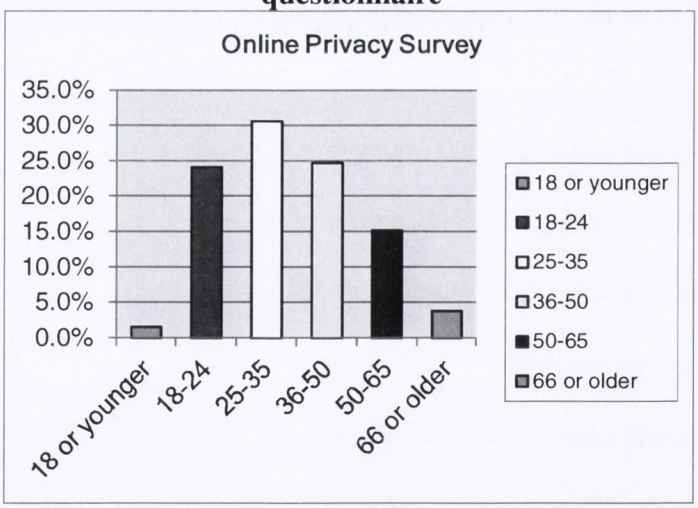
at least to some extent, it allows controlling for influences beyond those of direct interest. Due to resource availability limitations (especially at the initial stage of the research), however, we could not pursue this approach and we leave it for future research. In the present study, to form a sample as representative as possible, the target population, we conceptually break down the latter by age groups, as there is consistent evidence across previous research, such as the research on privacy concerns surveyed in Appendix A, that attitudes to online privacy vary considerably with age (Harris Interactive, 1999; Bellman et al., 2003; Forrester Research, 2010), and form as wide and as representative as possible samples of these age groups. Though, admittedly, this is an imperfect sampling scheme, likely to introduce some biases in the sample, we strived to mitigate the impact of this problem on our inferences by taking it into account in the subsequent empirical analysis, i.e. in the multivariate regression analysis of the questionnaire results, by including in the regression model a number of control variables, as well as in the semi-structured interviews. Five age groups were surveyed. These were:

1. 18 years and under;
2. 18 years – 24 years;
3. 25 years – 35 years;
4. 36 years – 50 years;
5. 50 years and over.

Respondents in the first two groups (Under 18 and 18-24) were largely represented by undergraduate and post graduate students. These two groups represented the younger generation of online users. The third and fourth groups of participants (25-35 and 36-50) were generally employees of a university. Finally, the last group of users were largely represented by members from two Rotary clubs in Dublin and were from the age

of 50 and upwards. In all, the questionnaire was sent out to 2500 individuals. There were 420 responses to the questionnaire. This was a response rate of a little under 17%. The graph below shows the spread of age groups that participated in the survey. In the resulting sample of individuals of the young age groups, lower levels of education are not represented but the sample hopefully contains enough diversity in educational attainment (i.e., high school leaving certificate but enrolled in an undergraduate program, earned undergraduate degree, attending a postgraduate degree, earned a postgraduate degree) so as to allow, in the subsequent regression analysis, the identification of the effect of education. Similar considerations apply to the sample of individuals in the older age groups, whose education levels are even more diverse, but with the caveat that there is limited variation in their socio-economic circumstances.

Figure 5.4 The spread of age groups that participated in the online privacy questionnaire



The recruitment process consisted of three stages. The first stage involved requesting students from Trinity College Dublin and Dublin and Waterford Institutes of Technology to participate. The second stage consisted of requesting the entire number

of employees (both administrative and academic staff) of Trinity College Dublin, and the third stage involved requesting two Dublin Rotary clubs to participate in the questionnaire. All respondents were recruited by using group mailings via email. The Rotary club was used to reach the older generation of online users.

5.1.4 Regression Analysis of Questionnaire Results

A multiple linear regression framework, specified as a generalized linear model (GLM), is used to estimate the relations between the constructs sampled through the questionnaire, with a special emphasis on whether seven of them, i.e. perceived risk, perceived benefit, informational privacy control preferences, importance placed on trust, ambiguity aversion, availability bias and trust propensity, can be seen as determinants of the other two, i.e. risk handling behaviour and willingness to disclose personal information. In doing so, we test specific hypotheses previously considered by the literature and implications of the two possibly complementary theoretical frameworks that we adopted as the conceptual underpinning of our analysis, i.e. the PC model prevalent in the IS and sociology literature and our RPC model, with its emphasis on bounded rationality and insights and ideas from the behavioural economics literature.

To this end, we first estimate specifications of regressions that include, on the right hand side, the variables typically considered by the literature as well as those suggested by our RPC Model. The most general version of the regression model, where dep_i denotes either $Willingness_i$ or $RiskHand_i$, is the following

$$dep_i = Const.$$

$$+\beta_1 ContrPref_i + \beta_2 AmbAver_i + \beta_3 PerRis_i + \beta_4 PerBen_i$$
$$+\beta_5 PropTru_i + \beta_6 ImpTru_i$$
$$+\beta_7 Avail_i + \beta_8 Age_i + \beta_9 Gender_i + \beta_{10} Education$$
$$+\beta_{11} Home_comp_i + \beta_{12} Work_comp_i + \beta_{13} Comp_Ind_i$$
$$+u_i \qquad (5.1)$$

Here, the explanatory variables are denoted as in Tables 5.1-5.3 and u_i denotes a regression error term. The estimates of this model and restricted versions thereof are reported in Table 5.4 and Table 5.5, for dep_i equal to $Willingness_i$ and $RiskHand_i$, respectively. For each model, we report point parameter estimates together with robust heteroskedasticity-adjusted standard errors and associated p-values under the null that the corresponding coefficient is equal to zero.

Our estimation methodology follows the "*general-to-specific*" approach, along the lines of Campos, Ericsson and Hendry (2005). We start with the most general regression model and we then eliminate regressors that appear not to explain the dependent variable, i.e. that carry statistically insignificant regression coefficients. Following this procedure, we eventually settle on the models in the last lines of Table 5.4 and Table 5.5 for $Willingness_i$ and $RiskHand_i$, respectively (where, apart from the constant, we only leave variables that are significant at the 15 percent level).

Model for willingness to disclose personal information

As far as the model for *Willingness* is concerned, the final specification includes all variables except (the proxy for) informational privacy control preference and the

dummies for the occurrence of a recent privacy breach and for whether the subject works in the computer industry, i.e. *ContrPref*, *Avail* and *Comp_ind*, respectively. While the fact that these variables do not appear to be significant regressors is somewhat surprising, all other variables enter the regression with an estimated sign that is consistent with recent information privacy modelling, e.g. Dinev and Hart (2004), augmented by our RPC model. In particular, our results suggest that the willingness to disclose personal information is positively related to the perceived benefit of the interaction, consistent with findings reported by Dinev and Hart (2006), Malhotra et al. (2004), Dinev et al. (2006), and Smith et al. (2011) to name a few, ambiguity aversion, gender (females are more willing to disclose, though only marginally so) and to two proxies for familiarity with ICTs, i.e. having a computer at home and carrying out computing tasks at work. Willingness to disclose personal information is instead negatively related to individual perceptions of risk in online interactions, the importance placed on trust, age and education. The negative relation with risk perception was already detected by Fetherman and Pavlov (2003), Malhotra et al. (2004) and Dinev and Hart (2006).

The fact that, in our estimates, willingness to disclose personal information depends in a positive fashion on the *perceived benefit* of the interaction and in a negative fashion on *perceived risk* (as per H1 and H3.a) is consistent with both the traditional and revised formulation of the PC model. It represents prima facie evidence of convergent and divergent validity of the perceived benefit and perceived risk constructs, respectively, and hence of the validity of the idea at the heart of the PC model, i.e. the expected risk-reward trade-off and its implication for the relation between the construct pertaining to

willingness to disclose personal information and both the perceived benefit and perceived risk constructs.

As noted, it is surprising that the estimated coefficient of *preference for control*, a variable that we are using as a proxy for *risk aversion*, is not significantly negative (in fact, it is positive and insignificant). It is in contrast with H2.b. Rather than to a failure of H2.b and hence of H2, however, this might be due to measurement error (a so called error in variable problem), not least because the coefficient of our second proxy for risk aversion, namely *ImpTrust*, which we interpret as a positive antecedent of risk aversion, is negative and therefore in agreement with H2.b. That is, as admitted in the construction of the variable, it is possible that *ContrPref* is a poor proxy for *risk aversion*. One concern, in this respect, is that, as shown in Table 5.3, it correlates possibly too much to *perceived risk*. Unfortunately, as already explained, obtaining a better proxy for risk aversion would require careful modelling and estimation of risk preferences that, in the context of the present study, would be unfeasible. We therefore leave this task to future research, though in the semi-structured interviews we will seek to gain at least some insight into the true relation between preference for control of personal information and privacy risk aversion. On a somewhat different note, the fact that *Willingness* is significantly and negatively related to *ImpTrust*, as well as being consistent with H2.b, implies that the greater the importance our subjects place on trust, the less inclined they are to disclose personal information when interacting online. This suggests that our typical subject considers online environments relatively untrustworthy.

Even more surprising is the fact that, as implied by the positive and significant coefficient of *AmbAver*, our estimated regression suggests high willingness to disclose

personal information for individuals whose *ambiguity aversion* is high (against H4.a). Taken at face value, this finding appears in contrast with the RPC model. This is not necessarily so, however, as it may be rationalized by recognizing that, in our regression model, we face an unavoidable omitted variable problem. The RPC model posits a negative relation between willingness to disclose personal information and both *perceived ambiguity* and *ambiguity aversion*, i.e. we should be testing jointly for H4.a and H4.b. Here, the relevant notion of perceived ambiguity is the level of ambiguity perceived by the IS user in the typical online interaction, since *Willingness* refers to the willingness to disclose personal information in such context. But, as noted, our survey (like all surveys that have been used in the empirical literature on the PC, as lamented by Smith et al. (2011)) only measures attitudes and a-situational intentions, rather than situation-specific circumstances. We therefore do not have data on *perceived ambiguity*, which is either highly situation-specific or observationally undistinguishable from *ambiguity aversion* (an individual who perceived the typical online interaction as ambiguous is most likely ambiguity-averse)[15], but only on *ambiguity aversion*. As it is typically the case in omitted variable problems, estimates of the coefficient of the included variable, i.e. *ambiguity aversion*, are biased and inconsistent if the omitted variable, i.e. the perceived ambiguity of specific online environments, is correlated (due to sampling bias or for some underlying influence) with the included variable, i.e. *ambiguity aversion*. If the coefficient of both the included and the omitted variable were negative, as predicted by the RPC model, the correlation between the two variables would have to be negative to explain the observed positive coefficient of the included variable, i.e. of ambiguity aversion. This is plausible, i.e. it is plausible that the

[15] In the case or risk perception and risk aversion, we sought to avoid this difficulty by using, as proxy variables for risk aversion, variables that capture general traits of individuals' risk aversion, such as preference for control and propensity/importance placed on trust.

more ambiguity-averse individuals might deem the typical online interaction less ambiguous, possibly because of a tendency to avoid ambiguous situations in the first place. In the setup of our questionnaire, this possible omitted variable problem was unavoidable, because of the already noted problem that we can only observe attitudes and intentions rather than actual behaviour in specific circumstances or environments. We therefore left further investigation of this effect to the semi-structured interviews and, to a lesser extent, to the focus-groups carried out in a later stage on the ADR project (as well as to future research), as in such settings it is easier to tease out determinants and possible influences on reported attitudes and intentions. That is, the assessment of the true sign of the relation between willingness to disclose information and ambiguity aversion, which is important for the purpose of assessing the validity of our PC model, is a task that we carried out as part of our subsequent analysis, which relied on interviews and focus groups. In particular, as explained in a subsequent section of this chapter, in the semi-structured interviews we sought to ascertain whether the more ambiguity-averse individuals do exhibit a tendency to avoid ambiguous situations, which would lead them to deem the typical online interaction less ambiguous and would explain the observed sign of ambiguity aversion coefficient under the revised calculus model.

Additionally, the fact that familiarity with ICTs increases willingness to disclose personal information (picked up by the positive and significant sign of the coefficients of *Home_comp* and *Work_comp*) is coherent with our RPC model to the extent that such familiarity entails lower limits to rationality (or 'less bounded' rationality) in online interactions and therefore a weaker impulse to disengage. That is, this evidence is coherent with H6. It is not coherent, however, with the traditional formulation of the PC

model, or at least with formulations that neglect limits to rationality, as in this case the coefficients of *Home_comp* and *Work_comp* should not be significantly different from zero. On a somewhat related note, *Education*, exerts a negative influence on the willingness to disclose, suggesting either a cultural bias in relatively educated subjects towards an emphasis on privacy, possibly deemed more as an absolute and less negotiable, or a greater awareness of privacy risks among the educated subjects, or both. This is important, as evidence that education affected attitudes towards privacy so as to render the more educated more inclined to view it as an absolute, would imply a serious limitation of the PC model, revised or otherwise. Unfortunately, our sample does not contain enough variation in the level of education to elicit indications in this respect and therefore, just like for the relation between ambiguity and ambiguity aversion, we sought to shed some light on this through the semi-structured interviews, on which we report in the relevant section of the chapter. The negative sign of the coefficient of *Age* suggest that the older individuals become, the less willing they are to disclose personal information. In so far as age is a proxy for the extent to which limits to rationality (familiarity with IS) are binding, this is consistent with H6 and therefore with the revised version of the PC model rather than the traditional one.

Model for risk-handling behaviour

As far as the model for *RiskHand* is concerned, the final specification includes all variables except *Avail*, i.e. the proxy for the availability of a recent negative experience, *Age* and *Work_comp*, i.e. the proxy for whether the subject carries out computing-related tasks at work. All other variables, which are left in the final specification, enter the regression with an estimated sign that is consistent with recent information privacy

modelling, e.g. Dinev and Hart (2004), Malhotra et al. (2004), Dinev et al. (2006), and Smith et al. (2011) augmented by features of our RPC model (under the auxiliary but arguably realistic assumption that risk handling behaviour is costly). Our results suggest that the intensity of risk handling behaviour increases with the perceived benefit and perceived risk (*PerBen* and *PerRisk*) of the online interaction, with our first and second proxy for risk aversion (namely preference for control, *ContPref*, and importance placed on trust *ImpTru*), with education and with familiarity with ICTs, as proxied for by whether the subject has a computer (*Home_comp*) and whether he/she works in the computer industry (*Comp_ind*), and that it decreases with propensity to trust (*PropTru*) and ambiguity aversion (*AmbAver*). Also, as implied by the marginally negative coefficient of *Gender*, men are inclined to undertake somewhat less intense risk handling behaviour than women.

The fact that the intensity of risk handling behaviour increases with the perceived benefit and perceived risk (*PerBen* and *PerRisk*) of the online interaction is consistent with H5a. and H5.b. In agreement with the RPC model, risk handling behaviour is especially beneficial when both the expected benefit and the risk of interacting are high because it is assumed to be costly, and therefore it is undertaken only when a suitable combination of such circumstances warrants the cost necessary to do so[16]. The positive and significant coefficients on our first and second proxy for risk aversion, namely

[16] In the privacy calculus model, expected utility is a negative function of risk and a positive function of the expected benefit. Also, risk handling behaviour is assumed to be, in one way or another, costly. Hence, as explained in the final part of chapter 3 and as per our set of hypotheses, we would expect more intense risk handling behaviour by subjects who, at the one time, perceived the greatest risk and the greatest potential benefit from interactions in online environments (whereas, in the presence of high perceived risk but low expected benefit, or vice versa, disengagement may be the rational choice). The fact that the declared intensity of the risk handling behaviour increases both with the perceived benefit and perceived risk is, therefore, in line with the privacy calculus model, both in the traditional formulation and in our revised one, and highlights the role played, in the decision of how to interact online, by the rational assessment of risks and benefits.

ContPref (preference for control) and importance placed on trust (*ImpTru*) is consistent with H5.d.

A somewhat similar line of reasoning applies to the interpretation of the coefficients of propensity to trust (*PropTru*). Propensity to trust leads to perceive a privacy threat as less likely. Therefore, arguably in agreement with intuition and elementary introspection as well as with H5.c of the RPC model, expected utility of risk handling behaviour would be higher for a subject with lower propensity to trust. Such a subject would be more inclined to undertake the costs required to deploy the risk handling behaviour.

The negative coefficient of *AmbAver* is consistent with our RPC model in that the assumed reaction of individuals to ambiguity is simply withdrawal. That is, whereas a certain amount of risk handling behaviour is the optimal choice in the presence of privacy risk in that it improves the risk-reward profile of the decision to interact, the optimal choice in the presence of ambiguity perception and of aversion to it (both indistinguishably captured by *AmbAver*) is not to engage in risk handling behaviour but to disengage altogether. It is therefore consistent with our ambiguity-augmented PC model that subjects who are more averse to ambiguity undertake less, not more, risk handling behaviour. These results, therefore, extend Drennan et al's (2006) findings by suggesting that the opportunity to deploy privacy risk handling behaviour does not lead to increased online disclosure of personal information *in ambiguous scenarios*. Finally, intensity of risk handling behaviour appears to be related to measures of limits to rationality, consistent with H6, in that declared risk handling behaviour intensity is greater for subjects with greater education and familiarity with ICTs (as proxied for by *Home_comp* and *Comp_ind*).

It should be emphasized that all our variables, except the demographic ones, measure attitudes and our dataset essentially captures variation in attitudes and typical self-reported behaviour across subjects. They do not capture variation of behaviour across circumstances (per subject or classes thereof). Smith et al. (2011) acknowledge that this is a common limitation of empirical studies in the literature on informational privacy, which we seek to address in part by carrying out semi-structured interviews and in part by employing ADR as our overarching methodological framework. We will also seek to address further in future research. In our current survey dataset, there is only one variable that can be used to infer how behaviour changes with circumstances, namely *dRiskHand*, which is the change in risk handling behaviour reported by subjects after having suffered a recent privacy breach (i.e., a breach in the last 6 months). In Table 5.6 we report results of the regression of this variable on the same set of explanatory variables used in the regression model for risk handling behaviour (*RiskHand)*. The change in magnitude and sign of certain coefficients is intriguing. Perceived benefit is now no longer significant in explaining variation in risk handling behaviour across subjects and the sign of the coefficient of *ImpTru*, i.e. importance placed on trust, is now reversed (i.e., from positive to negative). That is, after the breach, subjects who place the greatest importance on trust turn away from the risk handling behaviour strategies considered in the survey. A possible explanation is that, explicitly or implicitly, they primarily rely on trust in deciding whether to interact and this is likely broken in the aftermath of a breach. This reaction, however, is typical of a subject who suffers from *representativeness* and *availability bias* in that it is unduly influenced by recent events and does not correspond to an assessment of whether, based on circumstance and counterparty-specific information, trust should be accorded or

withdrawn. Also, the coefficient of *ContPref* is no longer significant, possibly suggesting a loss of confidence in the ability to control the use of personal information following a privacy breach.

Table 5.4 GLM Regressions (Dependent variable: *Willingness*)

Model	*Const.*	*PerBen*	*PerRis*	*PropTru*	*ImpTru*	*ContrPref*	*AmbAver*	*Avail*	*Age*	*Gender*	*Education*	*Home_comp*	*Work_comp*	*Comp_ind*
1	*** 3.63	*** 0.23	*** -0.25	-0.03	** -0.41	0.02	0.02	0.00	*** -0.63	0.06	-0.25	*** 1.97	* 0.67	-0.12
	0.92	0.00	0.00	0.62	0.05	0.76	0.45	0.93	0.00	0.38	0.22	0.00	0.08	0.68
	(0.000)	(0.000)	(0.000)	(0.618)	(0.046)	(0.757)	(0.450)	(0.931)	(0.000)	(0.375)	(0.224)	(0.000)	(0.076)	(0.679)
2	*** 3.43	*** 0.23	*** -0.24	-0.03	* -0.39		0.05		*** -0.61	0.10	-0.30	*** 1.95	** 1.14	-0.05
	0.00	0.00	0.00	0.67	0.08		0.18		0.00	0.15	0.12	0.00	0.03	0.87
	(0.000)	(0.000)	(0.000)	(0.670)	(0.082)		(0.183)		(0.000)	(0.150)	(0.116)	(0.000)	(0.034)	(0.868)
3	*** 3.27	*** 0.23	*** -0.25	-0.03	* -0.42		* 0.05		*** -0.60	0.13	-0.31	*** 1.96	** 1.14	
	0.00	0.00	0.00	0.66	0.06		0.05		0.00	0.15	0.11	0.00	0.03	
	(0.000)	(0.000)	(0.000)	(0.660)	(0.055)		(0.052)		(0.000)	(0.146)	(0.110)	(0.000)	(0.030)	
4	*** 3.35	*** 0.23	*** -0.24		* -0.44		** 0.05		*** -0.61	0.12	* -0.30	*** 1.92	* 1.09	
	0.00	0.00	0.00		0.07		0.04		0.00	0.11	0.10	0.00	0.07	
	(0.000)	(0.000)	(0.000)		(0.074)		(0.035)		(0.000)	(0.114)	(0.096)	(0.000)	(0.072)	

Notes. This table reports the estimates of regressions of the dependent variable *willingness* against alternative sets of regressors, listed in the top row. The estimation method is GLM with clustered GLS standard errors. For all included regressors, we report the coefficient estimates followed by the associated standard errors and *p*-values (in brackets) of the null hypothesis that the coefficient is equal to zero. One, two and three asterisks are used to draw attention to when this null is rejected at the 10, 5 and 1 percent level, respectively.

Table 5.5 GLM Regressions (Dependent variable: *RiskHand*)

Model	*Const.*	*PerBen*	*PerRis*	*PropTru*	*ImpTru*	*ContrPref*	*AmbAver*	*Avail*	*Age*	*Gender*	*Education*	*Home_comp*	*Work_comp*	*Comp_ind*
1	0.05	0.03	0.05	*** -0.09	** 0.18	*** 0.06	* -0.03	0.00	0.06	-0.08	*** 0.14	*** 1.66	-1.21	*** 0.61
	0.94	0.11	0.11	0.00	0.02	0.00	0.05	0.91	0.41	0.12	0.01	0.01	0.12	0.00
	(0.938)	(0.113)	(0.107)	(0.000)	(0.020)	(0.003)	(0.053)	(0.911)	(0.411)	(0.115)	(0.005)	(0.005)	(0.122)	(0.000)
2	0.05	0.03	* 0.05	*** -0.09	** 0.18	*** 0.06	** -0.03		0.06	-0.08	*** 0.14	*** 1.66	-1.20	*** 0.61
	0.92	0.10	0.08	0.00	0.02	0.00	0.05		0.40	0.11	0.01	0.01	0.14	0.00
	(0.924)	(0.097)	(0.079)	(0.000)	(0.021)	(0.004)	(0.054)		(0.397)	(0.108)	(0.005)	(0.005)	(0.140)	(0.000)
3	0.07	* 0.03	* 0.05	*** -0.09	** 0.19	*** 0.06	** -0.03			-0.09	*** 0.17	*** 1.64	-1.11	*** 0.61
	0.90	0.10	0.06	0.00	0.01	0.01	0.01			0.11	0.00	0.01	0.16	0.00
	(0.900)	(0.096)	(0.055)	(0.000)	(0.014)	(0.005)	(0.014)			(0.112)	(0.000)	(0.007)	(0.163)	(0.000)
4	0.03	* 0.03	* 0.05	*** -0.09	*** 0.19	** 0.06	*** -0.03			-0.08	*** 0.18	*** 1.64		*** 0.61
	0.96	0.07	0.05	0.00	0.01	0.01	0.01			0.12	0.00	0.01		0.00
	(0.955)	(0.070)	(0.051)	(0.000)	(0.007)	(0.013)	(0.008)			(0.120)	(0.000)	(0.008)		(0.000)

Notes. This table reports the estimates of regressions of the dependent variable *RiskHand* against alternative sets of regressors, listed in the top row. The estimation method is GLM with clustered GLS standard errors. For all included regressors, we report the coefficient estimates followed by the associated standard errors and *p*-values (in brackets) of the null hypothesis that the coefficient is equal to zero. One, two and three asterisks are used to draw attention to when this null is rejected at the 10, 5 and 1 percent level, respectively.

Table 5.6 GLM Regressions (Dependent variable: *dRiskHand*)

Model	*Const.*	*PerBen*	*PerRis*	*PropTru*	*ImpTru*	*ContrPref*	*AmbAver*	*Age*	*Gender*	*Education*	*Home_comp*	*Work_comp*	*Comp_ind*
1	0.15	0.02	*** 0.20	-0.05	*** -0.35	0.01	** -0.05	-0.05	*** -0.44	-0.02	*** 1.32	-0.66	*** 0.46
	0.27 (0.787)	0.57 (0.570)	3.26 (0.001)	-1.21 (0.226)	-3.76 (0.000)	0.71 (0.477)	-2.44 (0.015)	-1.08 (0.282)	-11.20 (0.000)	-0.29 (0.770)	2.79 (0.005)	-0.60 (0.550)	3.11 (0.002)
2	0.14		*** 0.19	*** -0.07	* -0.24		*** -0.05		*** -0.42		*** 1.33		** 0.41
	0.33 (0.745)		3.01 (0.003)	-3.28 (0.001)	-1.95 (0.051)		-2.74 (0.006)		-9.95 (0.000)		3.25 (0.001)		2.41 (0.016)

Notes. This table reports the estimates of regressions of the dependent variable *dRiskHand* against alternative sets of regressors, listed in the top row. The estimation method is GLM with clustered GLS standard errors. For all included regressors, we report the coefficient estimates followed by the associated *t*-statistics and *p*-values (in brackets) of the null hypothesis that the coefficient is equal to zero. One, two and three asterisks are used to draw attention to when this null is rejected at the 10, 5 and 1 percent level, respectively.

5.1.5 Summary of Main Findings from the Questionnaire

The survey and the attendant regression analysis of the responses provides evidence that the willingness to disclose personal information in an online interaction is positively influenced by the *perceived benefit* of the online interaction and negatively influenced by *perceived risk*, consistent with both the traditional and the RPC model. Unfortunately, due to the fact that the survey does not provide data on situation-specific circumstances, we were unable to directly estimate the effect of (*perceived*) *ambiguity* but we were able to argue that, if (*perceived*) *ambiguity* and *ambiguity aversion* were negatively correlated, our survey findings would be consistent with the RPC model, and we left the investigation of the sign of their correlation to the semi-structured interviews that were conducted after the questionnaire and that are examined in the next section.

Also, in accordance with the PC model, we found that risk handling behaviour (self-reported) intensity is positively impacted by *perceived privacy risk* and, consistent with the realistic auxiliary assumption that risk handling behaviour is costly, by the *benefit* of disclosing personal information online. Interestingly, the individual's *preference for control* in the online situation, which proved to be a weak proxy for privacy risk aversion in the regression for willingness to disclose personal information, turns out to be highly significant in explaining risk handling behaviour (self-reported) intensity. This is coherent with the PC model (both the traditional and our revised version thereof). We also find that an individual's reported risk handling behaviour intensity is negatively impacted by the individual's propensity to trust and by the individual's

ambiguity aversion (because the individual, in the presence of ambiguity, disengages), consistent with the RPC model.

Finally, consistent with the circumstance that we allow for behavioural biases, we found that individuals that have perceived a privacy breach in the previous six months experience a weaker perception of control over their personal information (availability bias) and that familiarity with ICT relaxes rationality limits, hence increasing both the willingness to disclose personal information and the intensity of the self-reported risk-handling behaviour.

5.2 The 20 Semi-structured Interviews

The interviews were conducted two months after the questionnaire was completed, in the spring of 2011. They were primarily carried out to seek to better capture constructs that were weakly measured by the questionnaire, such as cognitive biases, e.g. availability and representativeness and anchoring and adjustment, as well as unwillingness to disclose personal information in ambiguous circumstances, and to shed light on implications of the RPC model that remained unclear after the regression analysis of the results.

A complete list of the questions asked of the participants in the semi-structured interviews is available in Appendix E of this dissertation.

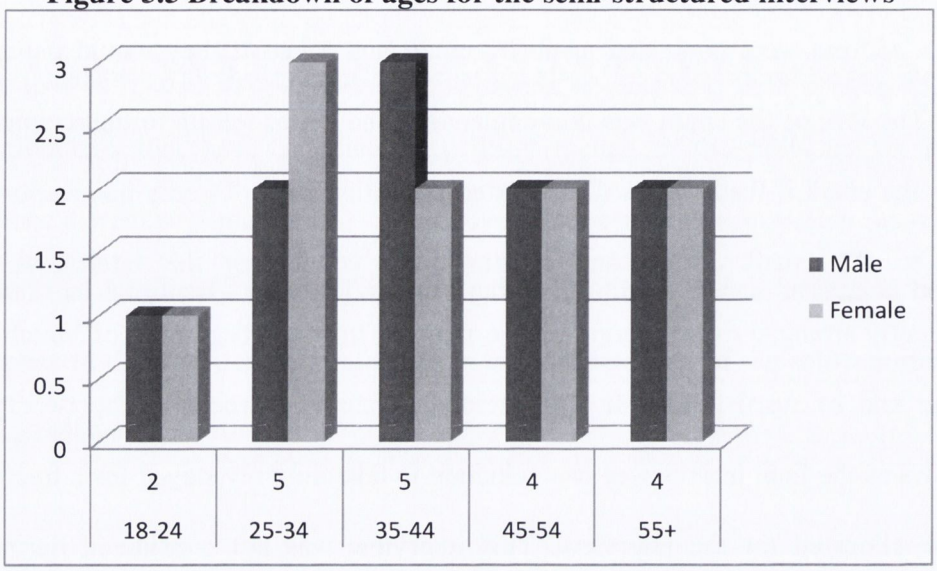
Respondents to the questionnaire had previously been asked to submit an email address if they were willing to participate further in the project by being interviewed regarding their attitudes towards privacy and online behaviour. All respondents that had submitted an email address were contacted again by email and asked if they would participate further. The tone of the email was non-demanding and it was left up to the recipients to reply to the email if they were still interested in participating. Twenty one respondents replied to the email. Times and locations for conducting the interviews were subsequently arranged over a period of two months, from the beginning of March 2011 until the end of April 2011. It was decided to analyse twenty of the twenty one interviews as the final interviewee was reluctant to talk and only stayed for a fraction of the time allocated for the interview. This interview was not considered during the analysis. Like the online questionnaire, the semi-structured interviews followed the same code of ethics outlined in chapter 4 of this thesis. In what follows, we first offer details on the demographic composition of or sample of interviewees, we then outline the method that we followed in analysing the interviews and finally we report the results of the analysis.

5.2.1 The Demographics of the Respondents

Before presenting the analysis of the interviews, we give a brief description of the interviewees. A total of 20 individuals agreed to participate in the semi-structured interviews. The gender divide of the respondents was even, with ten male respondents and ten female respondents. The majority of respondents were within the two middle age groups of 24-35 and 35-50 years. The 18-24 year olds were represented by just two individuals and the age groups above 55 years were represented by four individuals,

leaving fourteen individuals within the age group of 25-54 years. Figure 5.5 shows a breakdown of ages for the interviewees.

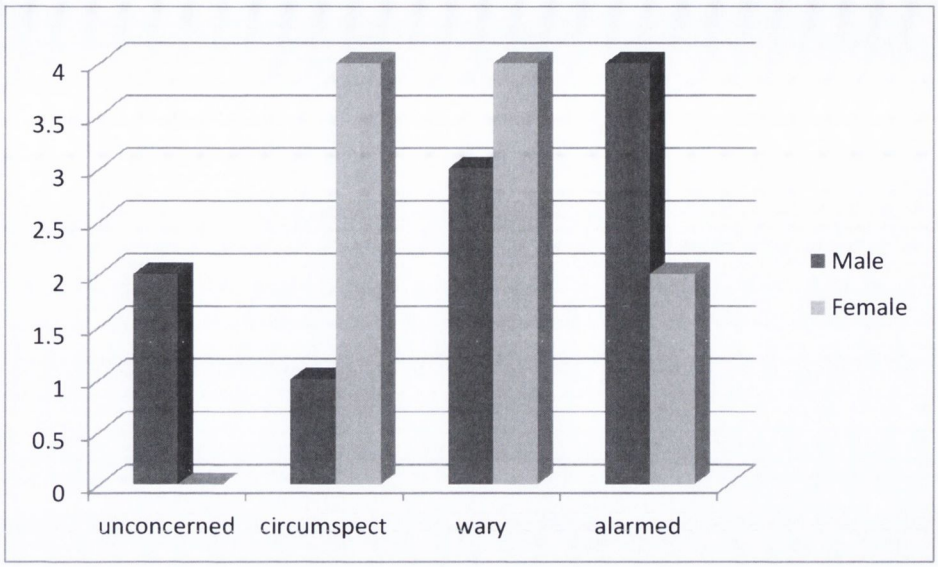
Figure 5.5 Breakdown of ages for the semi-structured interviews



Notes: The 18-24 year olds were represented by just two individuals and the age groups above 55 years were represented by four individuals, leaving fourteen individuals within the age group of 25-54 years.

Sheehan's (2002) four-part typology for the classification of individuals according to their privacy tendencies was used to group the respondents, i.e. the latter were classified in the following four categories: the unconcerned, the circumspect, the wary, and the alarmed. The interviewees were categorised according to their responses to questions that were taken from previous research (Sheehan, 2002) and used to determine an individual's level of online privacy concern (see Appendix D for the questions taken from Sheehan (2002)). All four categories were present among the 20 interviewees. Figure 5.6 shows a breakdown of interviewees according to this classification.

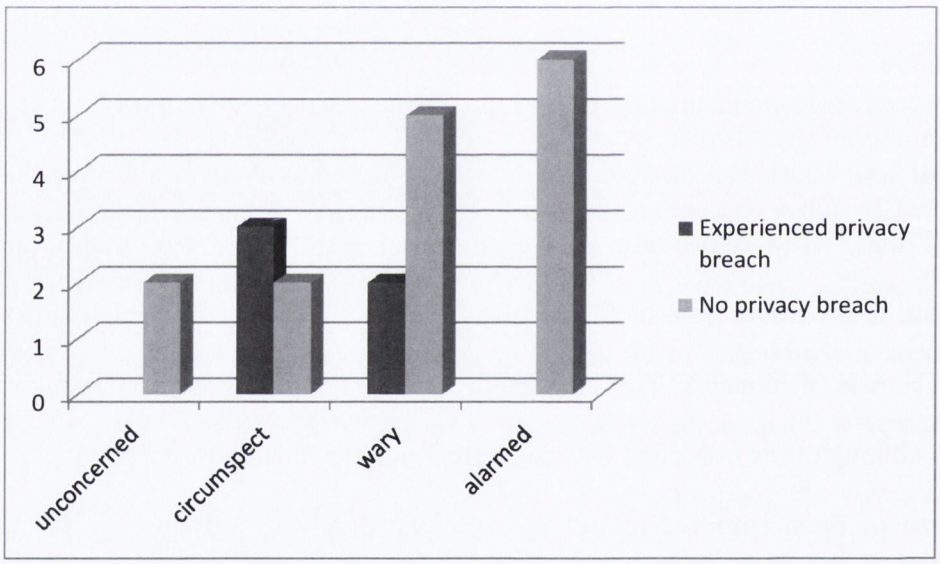
Figure 5.6 A breakdown of interviewees according to Sheehan's (2002) privacy classification



There were two respondents that fit into the unconcerned Internet users category, both male and both under 30 years old. They rarely complained about privacy breaches and reported that, when registering on websites, they rarely saw the need to provide inaccurate information. Five of the participants fit into the circumspect Internet users group (1 male, 4 female). These respondents had minimal concerns about privacy overall, although they conceded that there are situations that cause them some concern and some of them admitted to having experienced privacy breaches in the past. In addition, they reportedly often provide incomplete information or 'spam' email addresses when registering for websites. The wary Internet users group consisted of 3 males and 4 females who declared to experience moderate concern in most online situations and higher than average concern in some specific situations. Their concerns reportedly increase when they feel that clandestine data collection is taking place. They also occasionally complained about privacy breaches, and explained that they are likely to provide inaccurate information if they ever register for websites. The final group,

alarmed Internet users, consisted of 4 male and 2 female interviewees. The alarmed Internet users complained about the potential for privacy breaches but none admitted to having experienced a privacy breach in the past, they explained that they rarely register for websites and, when they do, they provide minimal amounts of data. Interestingly, this lends support to our earlier conjecture that more ambiguity-averse individuals might deem the typical online interaction less ambiguous because of a tendency to avoid ambiguous situations in the first place. Figure 5.7 shows a breakdown of the participants who have experienced a privacy breach in the past.

Figure 5.7 A breakdown of interviewees who have experienced a privacy breach in the past

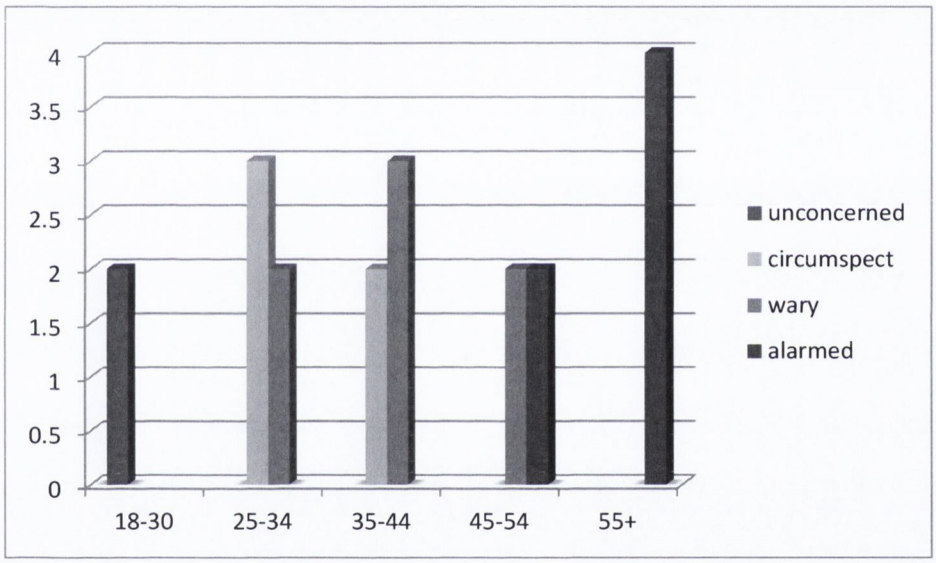


Note: The circumspect Internet users experienced the most privacy breaches followed by the wary Internet users. The alarmed Internet users experienced no previous informational privacy breaches.

The majority declared to refrain as much as possible from interacting online and again that, in the event that they do interact, they try to gather as much information as possible about the counterparty with whom they are considering interacting before making a decision. One of them explained that he uses Internet cafes, when in need to interact

online, to ensure his location remains protected. Interestingly, however, only one alarmed user declared using 'spam' email addresses[17]. The rest reportedly prefer instead to altogether refrain from interacting. Figure 5.8 shows the breakdown in ages among the interviewees. The vertical axis represents the number of participants and the horizontal access shows the age group of the participants. It is interesting to note that as age increases so too does the interviewees' privacy risk perception, as captured by the classification.

Figure 5.8 A breakdown of interviewees according to age and privacy risk perception



Notes: As age increases among the interviewees, so too does their perception of privacy risk

[17] This is an email address linked to an email account that is set up for use by the user when wishing to sign up for an online service, which requires the submission of an email address, but is suspicious that in signing up they may be subjecting themselves to the potential for receiving 'spam' email. By submitting the email address of the 'spam' account, the user avoids receiving 'spam' email to their normal email account.

5.2.2 Analysis Method

The analysis of the data gathered during the interviews was carried out using the Constant Comparative Method (CCM) for data analysis (Glaser, 1965). Since this dissertation uses both qualitative and quantitative approaches to data gathering, the CCM appears to be an especially a good fit. In order to best compare the results of the semi-structured interviews with the results of the online questionnaire conducted for this research, the CCM method of analysis was used to explore in more depth the tentative hypotheses. The CCM allows the researcher to take a "ground up" approach to theory formulation and allows the data speak for itself. Two common approaches to the analysis of qualitative data are the following:

1. When the data analyst wishes to convert qualitative data into (as Glaser (1965) puts it) crudely quantifiable form to test hypotheses, the data is first coded and then analysed. The categorisation, assessment, and analysis of the data is then accomplished systematically in a way that provides proof or otherwise for a given proposition.

2. The second approach is most appropriate when the analyst wishes to generate theoretical ideas, i.e. new concepts and their properties, hypotheses and interrelated hypotheses. In these scenarios, the analysis cannot usefully be confined to the practice of coding first and then analysing the data, since the analyst is constantly redesigning and reintegrating his/her theoretical notions as the data is reviewed (Glaser, 1965).

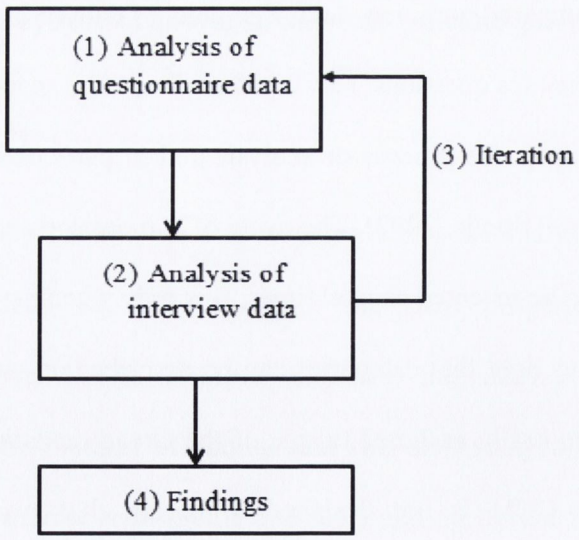
The CCM, however, provides the analyst with a third approach which combines, by a procedure of constant comparisons, the explicit coding procedure of the first approach and the style of theory development of the second. The purpose of the CCM, i.e. joint coding and analysis, is to generate theory systematically. At the same time, it does not prevent the development of theory by adhering completely to the first approach which is designed for provisional testing, not for discovering hypotheses (Glaser, 1965). In the work of Glaser and Strauss constant comparison is important in developing a theory that is grounded in the data (Glaser and Strauss, 1967). It is designed to enable researchers to develop a theory more or less inductively, by categorising, coding, delineating categories and connecting them. Constant comparison goes hand in hand with theoretical sampling (Boeije, 2002). This implies that the researcher decides in what order data will be analysed on the basis of theoretical concepts. In this way, questions that arise from the analysis of and reflection on previous data can be answered by analysing new data. Examples of such questions are interpretations of phenomena as well as delineating categories or finding relations between categories. The data is then analysed again and compared with new data. The units of data to be analysed should be chosen in a way that enables questions, new or otherwise, to be answered efficiently and effectively. This facilitates the process of analysis and in particular the progression of the comparative process (Boeije, 2002). The cycle of comparison and reflection on 'old' and 'new' material can be repeated several times. It is only when new cases do not bring any new information to light that categories can be described as saturated. This means that these cases can be easily assigned to one of the already existing categories in the growing theory. The CCM is not designed to ensure that two analysts working independently with the same data will achieve the same results; it is designed to include some of the imprecision and flexibility which aid the creative generation of theory

(Glaser, 1965). Thus, with this method, the systematic approach to substantiating or disproving hypotheses is facilitated without losing the richness and contextual basis for interpreting and validating results common in qualitative data analysis. The CCM is described by Glaser (1965, p. 439) as comprising four stages:

1. comparing incidents applicable to each category;
2. integrating categories and their properties;
3. delimiting the theory;
4. writing the theory.

The approach taken for analysing the semi-structured interviews was an application of the CCM approach to not only the interviews, but also to previous steps of the research project itself, especially by making constant reference to the results of the online questionnaire. Figure 5.9 shows this 4 step iterative approach to analysis.

Figure 5.9 The Constant Comparative Method



Notes: The CCM has a 4 step iterative approach to data analysis

According to Patton (1990) a primary decision when analysing interviews with the CCM is whether to begin with single case analysis or cross case analysis. For the purposes of this research, initially a cross case analysis of five interviews was undertaken, by examining the first five interviews and noting similarities and differences in the recorded answers to common questions. Once these five interviews were analysed, more interviews were added to the comparisons until all twenty interviews were analysed and compared and all results were recorded and classified and cross-classified.

5.2.3 Results

In what follows, we discuss the responses of interviewees on (self-reported) risk handling behaviour, how such behaviour changes in the face of ambiguity, the relation between ambiguity and ambiguity aversion, and the unwillingness by the more educated participants of the online questionnaire to disclose personal information online, (which, as seen earlier, is of importance in interpreting the result of our regression analysis), the influence on risk handling behaviour of age and importance placed on trust, the relation between trusting behaviour and representativeness bias, and evidence on the influence on risk perception and therefore, indirectly, on risk handling behaviour of heuristic biases such as representativeness, availability, anchoring and adjustment.

Risk Handling Behaviour

All interviewees agreed that they have undertaken risk handling behaviour of some sort in the past. This risk handling behaviour ranged from reporting questionable online behaviour to simply ensuring their antivirus was up to date. They all agreed that such risk handling behaviour was necessary. Undertaking risk handling behaviour was often equated to the physical world where individuals argued that common sense guides individuals to put a coat on when it is raining and not to walk alone after dark; it is this same common sense that individuals need to use in the online world. It was generally agreed that children and certain vulnerable adults need to be protected. Legislation should be put in place to protect the vulnerable in society from risks on the Internet and more of an emphasis should be placed on ICT education in schools and on teaching people how to distinguish between the benefits and drawbacks of ICTs for all age groups. It was also generally agreed that there are certain situations that individuals need to avoid in order to stay safe, such as omitting to update anti-virus software and submitting credit card details to "unsafe" websites.

From the findings of the online questionnaire, the five most common actions taken by individuals to protect their online privacy are, in order of frequency of occurrence:

1. buying from well-known and trusted brands;
2. interacting only with trusted sites;
3. Submitting inaccurate information online;
4. Setting up spam accounts to deal with unwanted email;
5. Abstaining from disclosing personal information online or disengagement with the Internet completely.

These are also the instances of risk handling behaviour more often recurring in the accounts of the interviewees. More specifically, seven interviewees said that they supplied false information to sites that were not fully trusted in exchange for a one-off service; eight interviewees had multiple email accounts or "spam" accounts to avoid the threat of receiving spam in their official email accounts and six interviewees combined both of these actions. These latter interviewees, who combined "spam" email accounts and supplied false information to sites, tended to be younger in age, while the older generation 35+ in general refrained from submitting information to sites they believed were unsafe. This group (35+), in general, carried out less privacy risk handling behaviour. Eleven interviewees, predominantly in the younger age groups, stipulated that interacting *only* with trusted sites was fundamental to protecting oneself online. The submission of credit card details to sites that were not deemed trustworthy was rare. As one respondent (in the young female and circumspect Internet user category) put it, transacting "in the wild" was foolish conduct. The majority of respondents within these 3 categories (of unconcerned, circumspect and even wary internet users) felt that taking risk handling behaviour measures, such as interacting only with sites that were deemed trustworthy or submitting false information to less trusted sites and submitting 'spam' email addresses is sufficient to protect themselves against the threat of an informational privacy breach. Table 5.7 below shows a breakdown of reported privacy risk handling behaviour among the interviewees.

Table 5.7 A breakdown of privacy risk handling behaviour among interviewees

	Unconcerned	Circumspect	Wary	Alarmed
Submitting false information	2 male	4 (1 male, 3 female)	1 male	
Multiple email accounts	1 male	4 (1 male, 3 female)	2 male	1 female
Both false info and multiple email accounts	1 male	4 (1 male, 3 female)	1 male	
Interacting with well-known brands	2 male	5 (1 male, 4 female)	4 (1 male, 3 female)	
Other forms of risk handling behaviour	2 male	5 (1 male, 4 female)	4 (1 male, 3 female)	3 male
Offline risk handling behaviour				6 (4 male & 2 female)

In what follows, we will discuss aspects of the reported risk handling behaviour and its relation to constructs of interest in our research.

Ambiguity and Risk Handling Behaviour

From the table above, it can be seen that the males within the "Alarmed" Internet user category undertake none of the privacy risk handling behaviour deployed by the other interviewees and all 6 participants (4 male and 2 female) in this category placed very little importance on trust, as implied by the fact that none places any importance on dealing with well-known brands (i.e., trusted sites). All four "alarmed" males refused to interact online if there was any indication of ambiguity in the situation. Two of these males were in the 55-+ category and two were in the 35 – 44 age category. One 55+ "alarmed" male interviewee claimed that if he does not know enough about the online

counterparty he just will not interact with them. He prefers instead to take measures offline to meet his needs. He argued that:

> *"I just don't know enough about computers to use them for everything, if I'm comfortable with the situation - fine, and I'll use my work computer for work reasons but if there is a hint of what you call...ambiguity...I won't go there."*

He admits that, when faced with a situation in his working environment where it is in the best interests of his employer to interact online with certain individuals, he always first makes physical contact by ringing the premises of the online entity and then finding the entities premises on Google maps to ensure the entity actually exists before making an online commitment. He believes these actions eliminate ambiguity of the terms of the interaction. The other 55+ "alarmed" male was equally averse to ambiguity. He admitted to doing the following in the presence of ambiguity:

> *"I have even driven 7 hours round trip to check out a potential supplier before I decided to deal with them online. I needed to check out their premises and check them out, you know...what they are like as people, before I feel confident to deal with them virtually"*

Another "alarmed" male in the 35-44 age category, and of US origins, admits, for work reasons, to surfing the web anonymously to access services or information he wouldn't access in his personal life. He is a researcher who researches terrorist groups and feels that if he did not take extreme measures, even while located in Ireland, to protect his identity he would be in trouble with the US authorities for surfing websites that are deemed by them as a threat to national security. In order to protect himself completely

he accesses these sites from Internet cafes and uses pseudonyms to get what he needs for his research.

> *"I am very fatalistic when it comes to informational privacy. This bothers me but it is the way it is and I can't do much about it. I have no illusions about the situation, I feel powerless in the current age with the current web tools."*

According to him, in his personal life he is also very careful about submitting any information about himself online. He refuses to join Facebook or any other type of social network and is reluctant to submit his credit card details online. He believes that the marketing companies that collect personal information are only the tip of the iceberg and the real threat comes from the US government who are tracking and logging all online movements:

> *I am more cautious about submitting information to governments than to private enterprise. It also depends on the information you are submitting. The government can get their hands on any data if they want it but they have an active system of surveillance with no due process if you are caught even for US citizens. If your data gets compromised by a private company, the worst that could happen is financial loss whereas with government you have not backdrop…*

Finally, the fourth "alarmed" male Internet user between the ages of 35-44 is reluctant to even talk about his actions online with regard to informational privacy. According to him, he minimises online interaction as much as possible as it is the only way that personal information is 100% protected. He argues that every situation is ambiguous because we cannot be sure who will get their hands on the information once it is

submitted and therefore ambiguity, according to him, can never be eliminated. Therefore, abstinence is the only solution. He dismisses trust as being not possible in online situations:

> *"Trust is difficult to define at the best of times. Don't trust anyone online. There is no way you can guarantee any information you submit online will not be abused, even if you believe the company you submit it to is trustworthy. Security measures are always fallible. You cannot have 'verified' trust online. This word is very naïve for online situations – it is not objective enough to be verified. Unless you spend a lot of time back tracking.*

Regarding the two female alarmed Internet users, they reportedly engage in very limited privacy risk handling behaviour. Both ladies were in the 55+ age category. The first lady that was interviewed, however, is becoming more aware of the risks involved in transacting online:

> *"I used to never have privacy concerns but now after hearing about so many privacy breaches, I would now be much more aware of my privacy and how it can be threatened."*

Recent privacy breaches that were reported on the media have increased her concern for her privacy. This indicates she may be prone to availability bias when assessing her risk of informational privacy breach and to representativeness bias when assessing which online entities to submit her personal information to online, e.g. if they haven't already been breached they must be safer. Both these biases could lead her to make incorrect decisions in online situations. She went on to say that these media reports were the

primary reason for her increased concern regarding her informational privacy. Like her "alarmed" counterparties she believes trust in online situations is impossible:

> *"I think trust is aspirational when talking about online situations. I would like to think trust was involved but even if you perceive that a site is trustworthy, there are other variables at play that cannot be accounted for..."*

This lady demonstrated biased beliefs, leading to severely affected (i.e., restrained) online behaviour on the Internet. She refused to submit credit card details over the Internet but found submitting such information over the telephone was acceptable:

> *"Yes, preventative actions are necessary to protect yourself against dodgy websites, for example, I would never give my credit card details online, but over the phone seems fine – don't ask me why!"*

She admitted that the more she hears about privacy breaches happening on the Internet the less inclined she is to submit her credit card details online regardless of the website and would prefer to submit them over the phone instead. She also admitted that if she really needed to interact online (for buying airline tickets for example) and the situation was ambiguous to her, i.e she "*couldn't assess the risks involved*" she would defer to her son who would complete the task for her, remarking that:

> *"My son knows all about computers so I let him take care of the things I would be too scared to do. I know we have to book our flights online so he always does that for me as he knows how to do it safely"*

Finally, the second "alarmed" lady also demonstrated elements of bias in her reactions. She indicated that she always has anti-virus on her machine at home. In her

employment, installing anti-virus is taken care of by the IT department. However, she always finds it a challenge to update her anti-virus for her computer at home. When she first bought anti-virus a few years ago, she refused to buy it online as she was afraid that hackers might realise she was currently vulnerable because she was buying anti-virus software. So she went to her local computer store to buy an anti-virus CD. Even then installing it at home was a time consuming and lengthy ordeal. As a result of this challenge, over time she decided to buy a laptop so that she could take her computer into the shop to have anti-virus installed and to generally ensure her computer was safe as she did not trust her own ability to keep her home computer safe by herself. Apparently, she has struck up a good friendship with the owner of the shop and now trusts him to keep her safe on the Internet. When she was asked what influences her decision to submit information online she replied that she relies on herself rather than on trusting other sites:

> *"The instinct to protect, this is an internal thing as opposed to external – it's there all the time when online – awareness of protecting oneself is what guides me online."*

One key purpose of the interviews was to help ascertain whether ambiguity and ambiguity aversion are negatively correlated, to establish whether the positive sign of the estimated coefficient of the latter in the regression model for the willingness to disclose personal information is consistent or otherwise with our RPC model. The responses of the subjects who were interviewed do support this conclusion, in that those who have the greatest aversion for ambiguity (i.e., the subjects who were classified as concerned and alarmed) also reported experiencing privacy breaches less frequently because they reverted to offline tactics to eliminate the online ambiguity, i.e. travelling

to meet prospective suppliers, or asking their son to carry-out online activities that were deemed ambiguous, or asking an expert in a shop to protect their laptop from harm. In a nutshell, due to their aversion for ambiguity, they interacted online cautiously enough so as to perceive online interaction as relatively unambiguous. That is, the risk handling behaviour determined by their ambiguity aversion likely influenced the level of ambiguity of the online context in which they elected to interact.

Trust and Risk Handling Behaviour

All "alarmed" internet users said that they place little or no emphasis on trust and indeed undertake minimal risk handling behaviour, rather preferring to abstain from submitting personal information online completely whenever possible. This finding reflects the earlier one from the online questionnaire that the greater the importance placed on trust by respondents the more risk handling behaviour they undertake. Another related finding was that none of these "alarmed" Internet users were under the age of 35, supporting the finding from the online questionnaire that age has a negative impact on users' willingness to disclose personal information, and suggesting that this relation is mediated by the importance placed on trust, which is greater in the younger age groups.

Furthermore, lack of familiarity with ICT is reportedly a barrier to their willingness to disclose personal information, similar to the online questionnaire finding that familiarity with ICTs increases users' willingness to disclose personal information. Likewise, all six interviewees in this category declared to be very averse and sensitive to ambiguity and that, when ambiguity is perceived, they either abstain from submitting personal

information or, when under duress, such as when in need to accomplish a task for work or to buy a plane ticket, they undertake extreme measures to eliminate it. The rest of the interviewees (unconcerned, circumspect and wary), declared that, once they feel they are interacting with trusted websites, they are more willing to disclose personal information, depending on the perceived benefit of the disclosure and the level of sensitivity of the information being requested. In situations where trust is low, the circumspect and unconcerned agreed that, by carrying out a number of risk-handling measures to reduce risk, such as disclosing incorrect personal information and/or providing spam email addresses, they can become to various degrees comfortable with interacting online, in exchange for a perceived benefit. They reportedly believe the risk is quantifiable and can be reduced to a sufficient level by carrying out risk handling behaviours.

A total of 11 participants indicated that trust was important when submitting personal information online. They were asked if they conduct risk-handling behaviour on sites that they deem trustworthy. All 11 of the interviewees stated that, if they trusted a site, there would be minimal or no need to carry out risk handling behaviour on that site. Risk handling behaviour is reportedly only carried out on less trusted websites where there is a risk involved in submitting personal information. The risk handling behaviour is conducted to eliminate or reduce that perceived risk to an acceptable level so that disclosure can take place. Five of these 11 interviewees, however, argued that sometimes they would still submit a spam email address to a trusted site if they felt there was a risk of receiving marketing email from the sites. Overall, these findings can be interpreted as indicating that, once a website is deemed trustworthy and, individuals are willing to disclose personal information essentially regardless of available risk

handling behaviour options. The next section looks at how the trustworthiness of a website is assessed by the interviewees.

Trustworthiness, Representativeness and Availability Bias

One crucial question is how individuals get to trust a site. All 11 interviewees who indicated that trust was important when submitting personal information online were asked the following question:

How did you decide in the first instance that a site was trustworthy?

Table 5.8 shows the breakdown of response to this question, i.e the factors influencing their decision when assessing the trustworthiness of a website..

Table 5.8 Factors influencing interviewees decision-making processes

	Unconcerned	Circumspect	Wary	Alarmed
Media sources		2 (1 male, 1 female)	3 (1 male, 2 female)	0
Look and feel of the site	1 male	1 female	0	0
Word of mouth	1 male	2 female	1 female	0

One male and one female from the circumspect Internet user category and one male and two females from the wary Internet user category relied on media sources to determine whether they believed a website was trustworthy or not when deciding to interact for the first time with that site. This would indicate that availability bias may have positively influenced their decision to interact with these sites. They relied on the media as a source of information when assessing the trustworthiness of a site. Availability bias can work in favour of some companies in that it can trigger the process that leads to the building up of trust, as evidenced by a discussion with one of the interviewees about Google, a female circumspect Internet user in the 25-34 age group. She admitted that

she would trust Google much more with her personal information than the Irish government due to the fact that Google's security "is much more dynamic" than the government's. When asked what she meant by this statement she explained that Google protects their data stores much better than the government does and they conduct much more research into the area of security. She argued that they also invest much more money in the area of security and protecting their information systems. When pressed for more information on how she came to this conclusion she admitted that her assessment of Google's security was based on what she read in the newspapers about the company. Even though she argued that Google invests a lot of money in security and in protecting their information systems, she did not mention the fact that Google uses the information gathered from their customers for their own benefit and sometimes without the consent of their customers (Lilly, 2013). This information was also available in the media at the time of the interviews taking place (Parr, 2010). A "circumspect" male reported the following:

> *"Well I'd heard about this site called Amazon that everybody was raving about so I thought...it must be ok if everyone has interacted with it and the reports are all good..."*

After having interacted with the site in question for the first time and having had a positive experience, then over time and with the increase of positive experiences, trust built up between him and the site. Initially availability of information from media sources, however, influenced his decision to see the site as trustworthy. Reliance on track record alone is also a symptom of representativeness bias, as it might not be very costly for the IS provider to break the user's trust (for example, due to the user's inability to spread the word about the track record being broken) and therefore it might

not form a solid basis for the building up of reputational capital on the part of the IS provider. It is, in practice, difficult to discriminate between trusting behaviour and behaviour induced by representativeness bias (the two constructs might even be evolutionary linked) and therefore leave further attempts to do so to future research.

One male from the unconcerned category and one female from the circumspect category explained that they began trusting a site simply by assessing the look and feel of the site. These interviewees might be prone to anchoring and adjustment bias because basing the whole decision of whether or not a site is trustworthy on the look and feel of that site can be dangerous. If at first glance, a site looks trustworthy due to it appearing professional and attractive, then, after that initial anchoring and under the influence of anchoring and adjustment bias, any adjustment to the assessment (made by the user due to accumulation of evidence becoming available as a result of on-going interaction) usually remains unduly close to the initial impression, i.e. that of trustworthiness. One of the interviewees that based her assessment of a site's trustworthiness on its look and feel qualified her response in the following way:

> *"when I do submit credit cards I use a card with very little credit so if there is a breach then minimal damage occurs. I always check for security settings on the site too – the lock symbol at the bottom of the page and https in the URL"*

This would indicate that she doesn't rely solely on the look and feel but also on risk handling behaviours such as minimising the potential for loss by using a specific credit card and checking security settings on the site. The situation is slightly different with the interviewees that relied on word of mouth for their assessment of the trustworthiness

of a website. They sought advice from already trusted sources to assess the website. As a young male from the "unconcerned" Internet user category said:

> *"I've known my friends for a long time and I know if they think a site is Ok then it more than likely will be – they would warn me about a site if anything bad had ever happened to them on it"*

Privacy Risk Perception and Cognitive Biases

From the interviewees' responses, the picture that emerges is one in which increase in risk perception leads individuals to engage in risk handling behaviour if they think the risks can be reduced by such behaviour whereas, when risk reaches a certain threshold or it can no longer be quantified, risk perception turns into a perception of ambiguity. In these situations interviewees reportedly abstain from disclosing information as well as from risk handling behaviour, particularly respondents in the older age groups. Interviewees in the younger age groups seemed to have a higher threshold for perceiving ambiguity than the older age group. Reportedly, the younger age groups would usually attempt to submit inaccurate information to obtain the perceived benefit of information disclosure but if this were not possible or if other types of risk handling behaviour did not suffice then abstinence would ensue. A young "circumspect" Internet user actually went through with information disclosure in a couple of ambiguous situations and regretted it:

> *"I've taken crazy risks twice before, where I really didn't know if I would be in trouble or not and both times I've immediately regretted it and rung my bank and cancelled my credit card"*

Conversely, the older generation simply abstained from disclosing information as soon as risk increased beyond the threshold. An "alarmed" male internet user between the ages of 35-44 remarked:

> *"...you can get what you want in different ways and compromising your security is too important to risk. I don't believe in having endless email accounts to protect data – you don't need any of that, just simply find another way preferably offline – there's no point in complicating life – at least not yet – we do not rely on the digital world enough yet that it is the only way of acquiring something and hopefully by the time we do start depending on the digital world to provide commodities it will be established enough that it will be a lot safer to do so..."*

Drennan et al. (2006) also support these findings. They argue that risk awareness leads to suspicion, which subsequently leads to privacy active behaviour. They found that a high level of risk perception leads to a variety of risk handling behaviours such as buying well known major brands, brand loyal behaviour, seeking more information, performing wider searches, and avoiding purchase altogether. However, an important finding of theirs was that privacy-active behaviour that was hypothesized to increase the likelihood of online subscription and purchasing was not found to be significant. It is argued in this work that this is a result of ambiguity influencing user's willingness to disclose personal information. When the perception of ambiguity exists, users refrain from online interaction regardless of the amount of privacy risk handling behaviour they have conducted in the environment.

Representativeness and Availability Bias

An "alarmed" female Internet users in the 55+ age category indicated that she was becoming more aware of the risks involved in transacting online as a result of hearing about all the informational privacy breaches through media sources. She admitted that recent privacy breaches reported on the media have increased her concern for her privacy. This indicates she too is prone to availability bias when assessing her risk of informational privacy breach. She may also be prone to representativeness bias when assessing which online entities to submit her personal information to online, i.e. if she has heard of a privacy breach taking place in a company she will not interact with them.

Anchoring and Adjustment

From Table 5.8 above two interviewees were influenced by the look and feel of the site when first visiting a website. They admitted that if they went on a site and it looked good and everything worked as it should then they would more than likely interact with that site and submit their credit card details to that site. This is evidence of an anchoring and adjustment bias taking place. The interviewees were happy to interact with sites that "looked professional". Even though the female "circumspect" interviewee took other measures to minimise risk, like submitting details of a credit card that had a limited amount of credit available on it, the male "unconcerned" Internet user admitted to basing his perception of the sites trustworthiness completely on its look and feel. However, he did add this caveat:

> *"I am extremely touchy though, if I sense anything suspicious about the look of the website I simply leave. Zero tolerance is my motto."*

Other Heuristic Biases

Perhaps one of the most interesting findings from the interviews is that seventeen interviewees felt that the notion of 'self-reliance' is necessary for establishing an acceptable level of informational privacy and thus reducing online privacy concerns. This concept of self-reliance was subjective to each individual and mostly consisted of keeping oneself abreast of potential threats to privacy, relying on one's own assessment of every online situation when deciding whether to interact at any given time or not, and generally using common sense to assess the risks to online privacy. This concept of common sense or self-reliance echoes a similar concept to which Sultan et al. (2002) refer as being 'Internet savvy.' This self-reliance seemed to instil in individuals a feeling of internal control over online situations which empowered them to be able to interact confidently online with minimal concerns about privacy. As one female interviewee, in the "circumspect" Internet user category, put it:

> *"I take precautions like I do in real life, I will walk down Grafton Street at 2pm as I know it is relatively safe, but at 2am it's a different story and if I chose to go there at that time of night, I need to be aware of the potential consequences. It is exactly the same for the World Wide Web."*

In addition, another male interviewee, from the "alarmed" Internet user category and in the 35-44 age group, went as far as to say that everyone needs to rely on themselves to protect their online privacy in order to avoid a surveillance state and paternalistic policies, where government controls all online transactions under the guise of 'protecting its citizens'. According to the theory of bounded rationality, as already argued in this dissertation, individuals make imperfect rational decisions when faced

with uncertain situations. If individuals rely completely on themselves for informational privacy protection, this self-reliance mechanism has the potential to introduce bias into their decision making processes when faced with uncertainty and ambiguity.

5.2.4 Summary of Findings from the Interviews

One key purpose of the interviews was to help ascertain whether ambiguity and ambiguity aversion are negatively correlated. The interview findings do support this conclusion, through the relation of both constructs with risk taking and risk handling behaviour, in that those who have the greatest aversion for ambiguity (i.e., the subjects who were classified as concerned and alarmed) also reported experiencing privacy breaches less frequently (Figure 5.7), likely because of a lower propensity to take risk or, at least, a greater propensity to handle them carefully. That is, it appears that ambiguity and ambiguity aversion are indeed negatively correlated in that individuals who are averse to ambiguity systematically avoid ambiguous situations, ending up perceiving the online context in which they interact as less ambiguous. As noted earlier, this finding is important as it permits us to conclude that the positive sign of the estimated coefficient of ambiguity aversion in the regression model for the willingness to disclose personal information is consistent with our RPC model.

In what follows, we summarize other important findings from the interviews:

- All interviewees admitted to refraining from submitting personal information in the presence of ambiguity, consistent with H4.
- Age has a positive impact on both perceived ambiguity and ambiguity aversion, supporting the conjecture we put forth in formulating H4.c and H5.e. In particular,

there was a distinct difference in the perception of ambiguity between the different age groups, with older interviewees appearing more prone to perceive ambiguity in a given situation, and ambiguity aversion was strongest among the older age groups.

- The importance an individual places on trust has a positive impact on the intensity of the individual's risk handling behaviour. That is, when facing a not trusted online counterparty, an individual who deems trust to be of a high importance tends to undertake risk handling behaviour, to see if trust can be built, rather than disengage (suggesting that trust and risk handling behaviour are complements rather than substitutes). To the extent that the importance placed on trust is a valid proxy for risk aversion, this is consistent with H5.d.

  Risk handling behaviour takes place when individuals believe the risks of the online situation are quantifiable and can be reduced by such behaviour. That is, consistent with H5.e, risk handling behaviour does not take place in the presence of ambiguity (in such case individuals perceive the privacy risks to be unquantifiable and prefer to refrain from disclosing personal information online). On a related note, the interviews confirmed that an individual's level of education and their familiarity with ICTs has a positive impact on an individual's propensity to engage in privacy risk handling behaviour. This is broadly in line with the RPC model in that education and familiarity with ICTs reduce limits to rationality and therefore perceived ambiguity (H5.f).

- Evidence of cognitive biases was found directly in the responses of nine interviewees. In fact these interviewees directly indicated their reliance on heuristics when making decisions concerning their informational privacy. Table 5.9 gives a breakdown of interviewees' biases found from discussions with them:

Table 5.9 Breakdown of heuristic biases among interviewees

	unconcerned	circumspect	wary	alarmed
Biases				
Anchoring and adjustment	1	1		
Representativeness bias		2	3	
Availability bias		1		1

Notes: Anchoring and adjustment refers to evidence that interviewees based their decisions on first impressions of a website or the initial look and feel of the site. Representativeness and availability bias refer to the tendency for the interviewees to make decisions based on what they hear from the media and how recently they have heard it.

Overall, this means that, consistent with the RPC model, individuals do not undertake risk handling behaviour 1) when their trust propensity is high and 2) in ambiguous circumstances. This indicates that individuals do not see the need for risk handling behaviour when they either do not perceive risk is sufficiently high to warrant such behaviour (high trust propensity) or conversely they perceive so much risk that risk handling behaviour is deemed pointless (the risks are so high that they are perceived as unmanageable and the situation is, as a consequence, perceived as essentially ambiguous).

5.3 Summary and Implications of Overall Findings of the Survey

The survey and the attendant regression analysis of the responses, outlined in this chapter, provided evidence that the willingness to disclose personal information in an online interaction is positively influenced by the *perceived benefit* of the online interaction and negatively influenced by *perceived risk*, consistent with both the traditional and the revised privacy calculus model.

Also, in accordance with the privacy calculus model, we found in the online questionnaire that risk handling behaviour (self-reported) intensity is positively impacted by *perceived privacy risk* and, consistent with the realistic auxiliary assumption that risk handling behaviour is costly, by the *benefit* of disclosing personal information online. The individual's *preference for control* in online situations is highly significant in explaining risk handling behaviour (self-reported) intensity, coherent with the privacy calculus model (both the traditional and our revised version thereof). We also found that an individual's reported risk handling behaviour intensity is negatively impacted by the individual's propensity to trust and by the individual's ambiguity aversion (because the individual, in the presence of ambiguity, disengages), consistent with the revised privacy calculus model.

In the regression analysis of the questionnaire results and the follow-up semi-structured interviews, we found that, consistent with the circumstance that we allow for behavioural biases, individuals that have perceived a privacy breach in the previous six months experience a weaker perception of control over their personal information (availability bias) and that familiarity with ICT relaxes rationality limits, hence increasing both the willingness to disclose personal information and the intensity of the self-reported risk-handling behaviour.

One key purpose of the interviews was to help ascertain whether ambiguity and ambiguity aversion are negatively correlated. The interview findings do support this conclusion, through the relation of both constructs with risk taking and risk handling behaviour, in that those who have the greatest aversion for ambiguity (i.e., the subjects

who were classified as concerned and alarmed) also reported experiencing privacy breaches less frequently (Figure 5.7), likely because of a lower propensity to take risk or, at least, a greater propensity to handle them carefully. That is, it appears that ambiguity and ambiguity aversion are indeed negatively correlated in that individuals who are averse to ambiguity systematically avoid ambiguous situations, and end up perceiving the online context in which they interact as unambiguous. As noted earlier, this finding is important as it permits us to establish that the positive sign of the estimated coefficient of ambiguity aversion in the regression model for the willingness to disclose personal information is consistent with our RPC model.

5.4 Conclusions

In this chapter, we describe and examine the findings of the questionnaire and of the twenty semi-structured interviews carried out two months after the online questionnaire was completed. The results of both the questionnaire and the interviews are largely supportive of the RPC model. An important finding from both the questionnaire and the interviews is that, in the face of ambiguity, both the willingness to disclose personal information and the propensity to engage in privacy risk handling behaviour decrease. This would indicate that privacy risk handling behaviour takes place only in the presence of uncertainty of the "quantifiable" sort, i.e. risk, in an effort to reduce that risk to an acceptable level. In the presence of ambiguity or "unquantifiable" risk, risk handling behaviour is seen as pointless. An important contribution of the analysis of the semi-structured interviews is that it clarifies the relation between (perceived) ambiguity and ambiguity aversion, showing that risk handing behaviour carried out by ambiguity-adverse subjects (i.e., systematic avoidance of ambiguous situations) leads them to

perceive the internet as a relatively unambiguous environment. This, in turn, implies that the estimate of the relation between willingness to disclose personal information and ambiguity aversion, obtained using results from the questionnaire, is consistent with the RPC model.

6 ADR in New Software Product Development (NSPD)

In this chapter, having completed the preliminary empirical analysis and testing of the RPC model in chapter 5 and before we provide details on how the implications of the RPC model guided the design of the RiposteTrEx system in chapter 7, we explain how the ADR methodology was used to guide the development of the new software product entitled RiposteTrEx, for the purpose of gaining further and deeper insight into the validity of the RPC Model and to pave the way for its refinement, while helping to align the privacy risk management features of the software to the needs of the users. In doing so, the ADR methodology proposed by Sein et al (2011) is adapted to settings in which the product being developed is an IS for use outside the organization, instead of the (intra-)organizational IS considered by Sein et al (2011), and therefore settings appropriate to the NSPD environment of our ADR project. To the best of our knowledge, this is the first time in which the ADR methodology has been applied in a NSPD environment.

6.1 Choosing ADR for New Software Product Development (NSPD)

We found (both retrospectively and, at the more advanced stage of the project, going forward) that fitting the project into the ADR structure was relatively easy, though the methodology had to be adapted somewhat. Typically, ADR deals with two challenges: (1) it addresses a problem situation encountered in a specific organizational setting by intervening and evaluating; and (2) it constructs and evaluates a software product that

addresses the class of problems typified by the encountered situation (Sein et al., 2011). When ADR, as in our case, is used in a NSPD environment (i.e., for producing new software products), the challenges differ slightly from those outlined by Sein et al (2011). In such an environment, ADR (1) addresses a need or service requirement encountered in a specific "real-world" or practical setting that has not yet been met by information technology and (2) constructs and evaluates a software product that addresses the need or requirement typified by the encountered setting, which is external to the organization, until and after the software product goes to market. The ADR process must continue, for a short time and on a less intense level, after the software product initially goes to market as it is generally accepted, in agile software development, that the first version of a software product often does not fully meet requirements in terms of functionality and user expectation. The feedback from the first release can be used to test feature designs and help improve marketing and customer support (Jiang, Scheibe and Nilakanta, 2011).

In this research, we interpret ADR as complementing the NSPD process in the following ways: (1) by providing a structured learning method that focuses on the building, operation and evaluation of a commercial software product during the entirety of its turbulent development cycle, (2) by facilitating the embedding of formalized research insights into the product during this turbulent development cycle, and (3) by assisting the validation of the software product by end-users before and after commercialisation, respectively, in a way that can be directly related to the validation of the research insights, thereby generating a positive feed-back loop between research and application. That is, ADR facilitates the effective and simultaneous building of a

software product and the development of its underlying theory. In this way, it provides for the possibility of engaged scholarship in turbulent environments such as NSPD.

As part of the ADR element of this study, the RPC Model is tested by examining the findings of focus groups that have been carried out on users of the privacy risk management electronic postal system entitled RiposteTrEx. In particular, this work seeks to establish whether the feedback from the users of the privacy risk management technology, gathered during the focus groups, is coherent with the feedback that would be expected under the RPC model. Analysis of the feedback will focus primarily on features of RiposteTrEx that were developed based on the RPC Model and special attention will be paid to the risk handling strategies and behaviour enabled by the privacy risk management technology embedded in the product.

Table 6.1 shows a breakdown of the full software product development cycle for RiposteTrEx mapped into the four stages (which are described in section 4.5 of this dissertation) of the ADR methodology, and gives details about the tasks/activities undertaken during each one of the four stages, including those related to data collection and analysis, as well as the duration of each stage and the amount of hours that were required to carry out the activities. In the following sections, we will describe the stages and the relevant principles of the ADR approach which were followed within each stage of the RiposteTrEx product development project.

Table 6.1 Breakdown of ADR Methodology for the RiposteTrEx Development Cycle

Stage	Timeframe	Tasks/activities	Duration
Problem formulation (Stage 1)	Aug 2010 – April 2011	Data collection and documentation through online questionnaire, semi-structured interviews and meetings with key stakeholders (senior public service personnel and prospective users)	7 months
		Seven days of research and development work per month	49 days
Building, Intervention, and Evaluation (BIE) (Stage 2)	Dec 2010 – June 2011	Iterative prototype development, testing & evaluation On-going articulation of system requirements for privacy enhanced e-postal systems.	7 months
		Seven or of research and development work per month	52 days
Reflection and learning (and on-going BIE) (Stage 2&3)	July 2011 – December 2011	On-going iterative development, testing & evaluation On-going articulation and formalisation of system requirements for privacy enhanced e-postal systems, largely based on the traditional privacy calculus (PC) model and survey of the literature, as validated by preliminary testing (based on questionnaire data and semi-structured interviews) Submission of research to workshops for academic feedback. First set of focus groups with a cross section of the public	6 months
		Four or five days of research and development work per month	28 days
Formalisation of learning (and on-going BIE) (Stage 2&4)	Jan 2012 – September 2012	On-going iterative development, testing & evaluation Analysis of second set of focus groups. Generalisation of system requirements for privacy enhanced e-postal systems (including on-going articulation of new design principles, based on RPC Model and survey of the literature, as validated by further testing, aided by regression analysis, based on questionnaire data and semi-structured interviews) Bug reporting and fixing	9 months
		Five days of research and development work per month	45 days
Outcomes and reiteration (Stages 2-4)	September 2012 – December 2012	Software product transition to production stage of the product lifecycle. Conclusion of iterative development, testing & documentation Provision of on-going support for pilot projects and wrap up meetings for the first release cycle. Start-up of the next development cycle for version 2 of the product using the data gathered during the NSPD cycle.	4 months
		Five days research and development work per month	20 days
Total days of research project			194 days

6.1.1 ADR Stage 1: Problem Formulation

The RiposteTrEx project was triggered by a problem envisaged by the managing director, Liam Church, of Escher Group Holdings Plc. regarding how citizens' personal data online will need to be increasingly protected from third party exposure but available to the individual citizen in future electronic interactions with government. This insight was the product of his career-long experience of working closely with various public sector organisations and NPOs and in particular with NPOs worldwide. Based on this insight, the company developed a prototype software infrastructure, to safeguard citizens' personal information when electronically but which also makes a citizen's data readily available to him/her for their own personal use. Further details of the motivation for building the RiposteTrEx product can be found in (Church and Moloney, 2012). He consequently successfully sold a licence for this product to An Post, the Irish NPO, resulting in funding to further develop the prototype to the 'proof of concept' stage. As a result of this funding and after almost 2 years of in-house conceptualisation and research, the RiposteTrEx project for commercialisation started in earnest in 2010.

At the beginning of the RiposteTrEx commercialisation project and during the latter stage of the problem formulation process, an IS researcher (the Author of the present thesis) was assigned to the project, working closely with the project team, to provide the team with insight from the IS literature (formalized knowledge) and learn from the teams experience, expertise and experiential knowledge of their chosen field. As recommended by Sein et al. (2011), this stage of the project revolved around two key

principles, i.e. those labelled 'Practice-Inspired Research' and 'Theory-Ingrained Artefact'.

Even though the problem formulation stage within Escher Group started around April 2010, practice-inspired research commenced when the Author, i.e. IS researcher, joined the team in August 2010. She was called upon to generalise the problem and to help inform the design of a software product aimed at resolving the class of problems which the specific problem represented. That is, for the RiposteTrEx case study outlined in this research, the specific problem of interest was the set of privacy risks faced by perspective users of the RiposteTrEx product and the class of problems of interest were those arising in the development of a software product for providing private electronic postal mail. By embedding the researcher in the world of the practitioner at such an early stage, an interface between the scientific world of the researcher, marked by theoria, and the practical world of the practitioner, marked by praxis, was created (Mårtensson and Lee, 2004; Costello, Conboy and Donnellan, 2011). This encouraged praxis and theoria throughout the rest of the project stages, with the ultimate aim of producing a theory-ingrained artefact. The project aimed to develop what can be defined, according to Gregor's (2006) taxonomy of theories for informing the design of artefacts, a Type V theory or, equivalently, a set of design principles or a design theory.

In late August 2010, inspired by the second principle, i.e. that the project should produce a 'theory-ingrained artefact', a weeklong brainstorming session took place at the company headquarters to kick-off both the development effort for the software product and the collaboration between industry and academia. At this meeting, senior

software developers and designers, security experts, an IS researcher, and consultants, senior management, and senior public servants came together to conceptualise the proposed product and to tackle the expected challenges to be faced by the project team. Following the brainstorming week, interaction among participants continued through the use of Computer Mediated Communication (CMC) channels where everything relating to the product, such as documentation, the development environment and prototype testing environments, was shared across four countries, Ireland, the US, South Africa and Singapore (the four locations where Escher Group has development teams).

6.1.2 ADR Stage 2: Building, Intervention, and Evaluation (BIE)

This setting up of the project facilitated the commencement of the second stage of the ADR methodology, i.e. the Building, Intervention and Evaluation (BIE) stage. For a new software product, this stage differs slightly from the corresponding stage outlined by Sein et al. (2011). This stage is carried out as an iterative process in the target environment. Therefore, in NSPD, it must interweave the building of the software product with intervention and evaluation in a *real-world setting*, external to the organization (extra-organizational), as opposed to doing this in the organisational (intra-organizational) setting described by Sein et al. (2011). The outcome is the realized design of the software product (Moloney and Church, 2012). During BIE, the problem and the software product are continually evaluated, and the design principles are articulated for the chosen class of systems, which the software product represents.

This initial BIE stage for RiposteTrEx lasted seven months, during which time a number of iterations of the BIE cycle took place. Senior management, the development team, the product testers and the IS researcher worked together to define, refine, develop and deploy prototypes which tested various features of the system and observed how users (in-house testers) responded to the features and iterated, until finally all features of the product were implemented, tested and deemed to be functioning correctly (the first Beta version of the product). After the seventh month, the software product had reached the 'proof of concept' stage of the development cycle. At this point, a demonstration of its functionalities was given to the governmental body (An Post) that had commissioned the project and a series of focus groups with end-users were conducted. This demonstration and the focus groups determined whether the software product would be further developed. Fortunately, the product feedback was, for the most part, positive[18]. Over the following eighteen months, considerable reworking of the product was nonetheless carried out, until a second set of focus groups, at the first release stage, was carried out in August and September of 2012, which again resulted in further reworking of the product. This reworking embodied the three principles that, according to Sein et al. (2011), should guide product development at the BIE stage. The first one of these is the principle of 'reciprocal shaping' between the software product and the organizational context. The second one is the principle that the different project participants should play 'mutually influential roles'. The third one is that there should be 'continuous and concurrent evaluation' of the product, as it is being developed.

[18] The first set of focus groups were conducted by an independent research company to which the author has no connection and therefore can only report that the findings were sufficiently positive to warrant a continuation of the development project of the product.

Sein et al. (2011), in formulating the principle of reciprocal shaping, emphasized the reciprocal influences exerted by the two domains that are relevant in IS development for organizations, i.e. the information system and the (intra-)organizational context. Within NSPD, as already noted, the two domains consist of the software product and the external (extra-organizational) context where the need or requirement satisfied by the software product arises. Using the feedback from the online questionnaire, the semi-structured interviews and the second set of focus groups carried out for the first release of the product, the ADR team engaged in recursive cycles of decision-taking and used a combination of the user feedback and design constructs to shape their interpretation of the real-world environment. They then used this increasing understanding of the real-world environment to influence the selection of design constructs for the product.

The third principle, i.e. 'authentic and concurrent evaluation', emphasizes a key characteristic of both ADR and agile software development: evaluation is not a separate stage of the research process that follows building. Therefore, in the RiposteTrEx project, decisions about designing, shaping, and reshaping the software product and intervening in (extra-organizational) real-world settings were interwoven with on-going evaluation. Accordingly, the BIE stage of the project continued after the proof of concept stage was complete. In fact, it overlapped with stages 3 and 4, as shown in Table 6.1. On-going iterative development, testing and evaluation of the software product took place right up to the final testing (via focus groups) of the product before it went live for its first two pilot (in the autumn and winter of 2012).

6.1.3 ADR Stage 3: Reflection and Learning

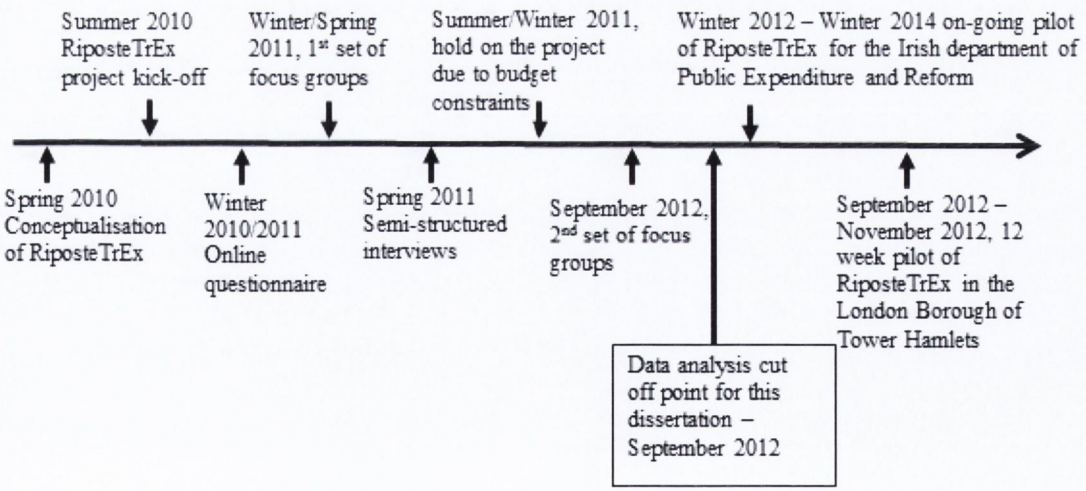
As explained by Sein et al (2011), the reflection and learning stage moves conceptually from building a solution for a particular instance to applying that learning to a broader class of problems. For RiposteTrEx, this stage was continuous and interweaved with stage four. In fact, conscious reflection on the problem framing, the theories chosen, and the emerging product occurred through all four stages of the ADR process. It was critical to constantly reflect and learn from the development process of the new software product in order to ensure that all contributions to knowledge were identified and rigorous. The research process was regularly adjusted based on early evaluation results to reflect the increasing understanding of the software product and to constantly develop the product with a view to the problem it needed to solve. The principle of 'guided emergence' directed this stage. This principle makes the NSPD cycle dynamic and causes the lines between the different stages of the ADR method to begin to merge. This principle emphasizes that the ADR team should be sensitive to signals that indicate the need for on-going refinement and react accordingly by continually updating and refining the system requirements and, thus indirectly, the new design principles for the specific class of systems they are made to address (Sein et al., 2011).

6.1.4 ADR Stage 4: Learning Formalisation

The objective of the fourth stage of ADR is to formalize the learning opportunity afforded by the project under consideration. Accordingly, the situated learning from the RiposteTrEx project was developed into general solution concepts for the design of electronic postal systems. We did this by outlining in the present work and in a recently

published conference paper, i.e. Church and Moloney (2012), the design accomplishments realized in the development of the software product and the attendant organizational outcomes, as instances of formalized learning. This fourth stage drew on the seventh and last principle put forth by Sein et al (2011), i.e. the principle labelled 'generalised outcomes'. Generalization is challenging because of the highly situated nature of ADR outcomes that include organizational change along with the design and development of a software product. Sein et al. (2011) suggests three levels for this conceptual move to generalisation: (1) generalization of the problem instance, (2) generalization of the solution instance, and (3) derivation of design principles from the design research outcomes. All three levels were attempted during the RiposteTrEx project and were addressed by papers that were either published at conferences (Church and Moloney, 2011; Church and Moloney, 2012; Church, Moloney and Bannister, 2013) or that are currently works in progress (Church and Moloney, 2013; Moloney and Coyle, 2014). Figure 6.1 shows the timeline of the ADR project for RiposteTrEx.

Figure 6.1 Timeline for the RiposteTrEx ADR project



6.2 Conclusion

This chapter explained how the ADR methodology formulated by Sein et al. (2011) can be adapted for use in settings in which the product under development is an IS for extra-organizational use, which is the relevant setting in the case of the IS product, i.e. RiposteTrex, considered in our application of this methodology. We also outlined the key steps of the product development cycle of this product and explained how they map into the stages of the adapted ADR methodology.

7 Engineering and Testing the Revised Privacy Calculus (RPC) Model

In this chapter, having motivated the choice of the ADR methodology being the overarching methodology for this research in chapter 6, we provide details on how the implications of the RPC model were used to guide the design of the RiposteTrEx system, which is at the heart of the ADR project underpinning this dissertation. We demonstrate how users' acceptance of the latter, assessed through a series of focus groups, was used to draw inferences on the validity of the model. The RPC Model was used to guide the design of the RiposteTrEx system in such a way that not only would the system safeguard informational privacy so as to meet minimum regulatory requirements, but would give the users the possibility of managing their own privacy risk in a manner that users would find as beneficial as possible, so as to maximize their

online interaction, subject to given constraints in terms of the cost of developing and running the system.

One key advantage of using the RPC model as a guide in deriving the system requirements, rather than the traditional formulation of the PC model, is that it clarifies the link between possible users' biases, risk taking/handling behaviour and decisions concerning information disclosure and online engagement. This allowed us to use results and ideas put forth by the behavioural economics literature (and authors who, like Acquisti and his co-authors, straddle the IS and economics domain), such as those on "nudging" (discussed in the relevant section of chapter 2), and apply them to improve the welfare of decision makers affected by such biases in an IS domain.

For exogenously given system objectives and resource constraints (e.g., on the development and running costs of the system)[19], the implications of the RPC Model on how to achieve the former subject to the latter were first mapped to a set of requirements for the RiposteTrEx system, analogous to normative implications of the model under the given system objectives and realistic resource constraints. The system requirements were then mapped to a set of system features, namely system functionalities (e.g., privacy management tools) and specific system design principles. The following sections provide details of this mapping process. We then present the findings of focus groups that were conducted to assess the extent to which users believe that the system requirements have been met and the users' general satisfaction with the system, with special emphasis on the level of acceptance of the features aimed at

[19] The overall objectives and resource constraints in terms or development and running costs of the system were specified by the NPO. They were given in the somewhat informal and iterative manner that is typical of many innovative development projects.

meeting the RPC model-derived system requirements. This is followed by a reflection on the findings and by an attempt to outline general privacy design principles for electronic postal systems.

7.1 Defining the System Requirements for RiposteTrEx

We now provide a detailed description of the system requirements derived for RiposteTrEx during the design and development phase of the NSPD lifecycle. The main objective of the RiposteTrEx system is to provide a means for formal private online correspondence between citizens, businesses, and local and national government, by using an electronic postal system as an infrastructure that transfers and stores users' personal information, maintaining levels of informational privacy that users deem acceptable so as to regularly use the system to interact. The product must also adhere to the current data protection legislation and the forthcoming data protection regulation of the EU.

Under this set of general objectives of the ReposteTrEx project, the implications of the RPC Model (especially the ones that were supported the most by the preliminary empirical testing reported in chapter 5) were first (Stage 1) mapped to a set of requirements for the RiposteTrEx system, outlined in Table 7.1, and then (Stage 2), after having synthetized from these requirements a smaller set of more general requirements, to a set of system features, including system functionalities (e.g., privacy management tools) and technical design principles, outlined in figure 7.1. The following

sections provide details on the mapping process, especially how the system requirements were mapped to system features.

Table 7.1 Mapping the RPC Model Implications to System Requirements (Stage 1)

Empirical findings	Constructs	System requirements
Willingness to disclose personal information is positively affected by the following constructs:		
	Perceived benefit	Possibility to increase the level of information disclosure for higher levels of perceived benefit;
	Familiarity with ICTs	Provide learning methods to increase familiarity with the system, targeted at users with low familiarity with ICT.
Willingness to disclose personal information is negatively affected by the following constructs:		
	Risk perception and risk aversion	Reduce risk perception; Possibility to lower the level of information disclosure for higher levels of perceived privacy risk and higher levels of privacy risk aversion.
	Ambiguity aversion (and perceived ambiguity)	Reduce ambiguity (especially system-originated ambiguity) Possibility to lower the level of information disclosure for higher levels of perceived ambiguity and higher levels of ambiguity aversion.
	Age and education	Higher default (but adjustable) level of privacy protection for users of older age and with higher education.
	Importance placed on trust (and lack of trust)	Possibility to lower the level of information disclosure for higher levels of importance placed on trust and/or low trust; Leverage trusted brand of NPOs to increase trust perception of trustworthy counterparties.
Reported risk handling behaviour intensity is positively impacted by the following constructs:		
	Benefit perception	Increased range of feasible risk-handling behaviour strategies in situations when benefit perception is high and risk perception is
	Risk perception	

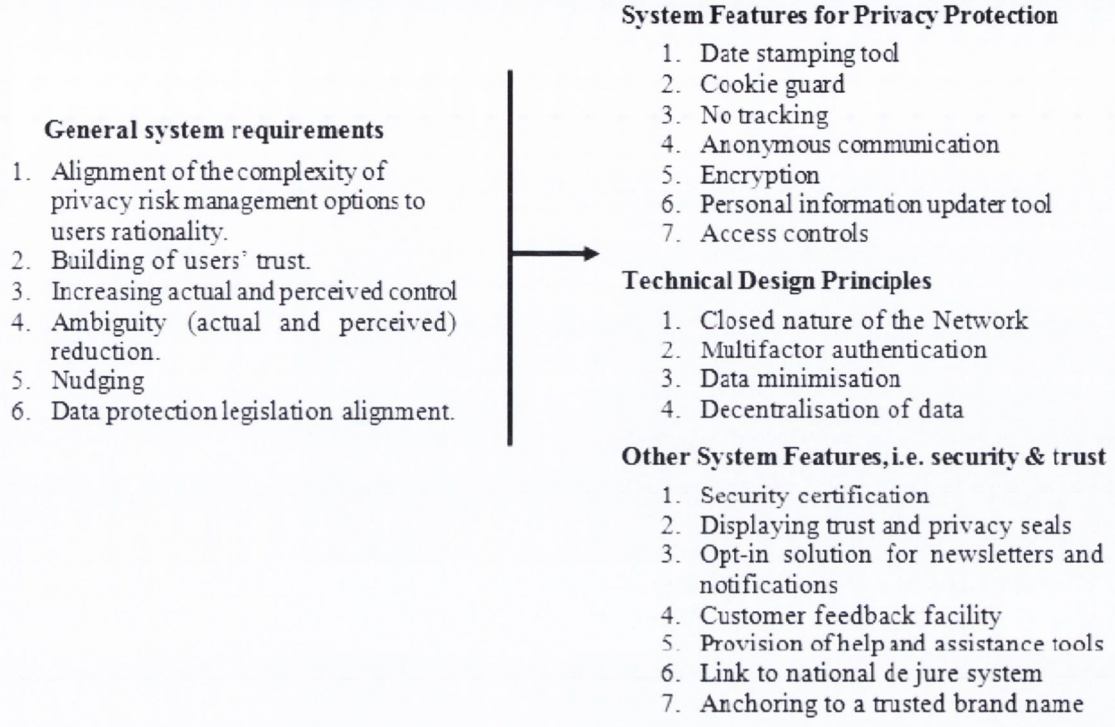
		high.
	Importance placed on trust	Increased range of feasible risk-handling behaviour strategies in situations when importance placed on trust is high and/or trust is low
	Education Familiarity with ICTs	Provide assistance tools to increase knowledge of the system targeted at users with lower education and lower familiarity with ICTs
Reported risk handling behaviour intensity is negatively impacted by the following constructs:		
	Propensity to trust	Reduce range of feasible risk-handling behaviour strategies for subjects whose propensity to trust is high and/or when trust is high (it is not worth sustaining the cost of making these strategies available to these subjects and in these situations)
	Ambiguity aversion (and ambiguity)	Lower range of feasible risk-handling behaviour strategies for subjects whose ambiguity aversion is very high and in situations of high ambiguity (it is not worth sustaining the cost of making these strategies available to these subjects and in these situations)

From undertaking a synthesis of the requirements outlined in the third column of the table above, a set of five general system requirements (all subject to realistic cost and resource availability constraints) were derived:

1. Align the complexity of privacy risk management options available to users to their limits to rationality, widening privacy risk management options for expert users (providing dedicated privacy management tools) while ensuring as high as possible privacy protection by default for inexpert users;
2. Build user trust (mainly through increasing information transparency);
3. Maximise users' actual and perceived control over their personal information;
4. Remove/reduce actual ambiguity (mainly through data minimization and the elimination of secondary use of personal information once submitted online) and perceived ambiguity (mainly through training/education);
5. Nudging users into desirable choices beyond limits to rationality, e.g. cognitive error and biases.
6. Data protection legislation alignment.

These are now motivated and discussed in detail in the next subsections. In doing so, we outline the system features for privacy protection, which include primarily the functionalities described in Appendix H and the technical design principles described in Appendix I, as well as other features described in Appendix J, and explain the role played by such system features in meeting the system requirements. Figure 7.1 outlines the relationship of these features, principles and functionalities.

Figure 7.1 The mapping of general system requirements onto system features, functionalities and technical design principles (stage 2)



7.1.1 Alignment of the complexity of privacy risk management options to users' rationality

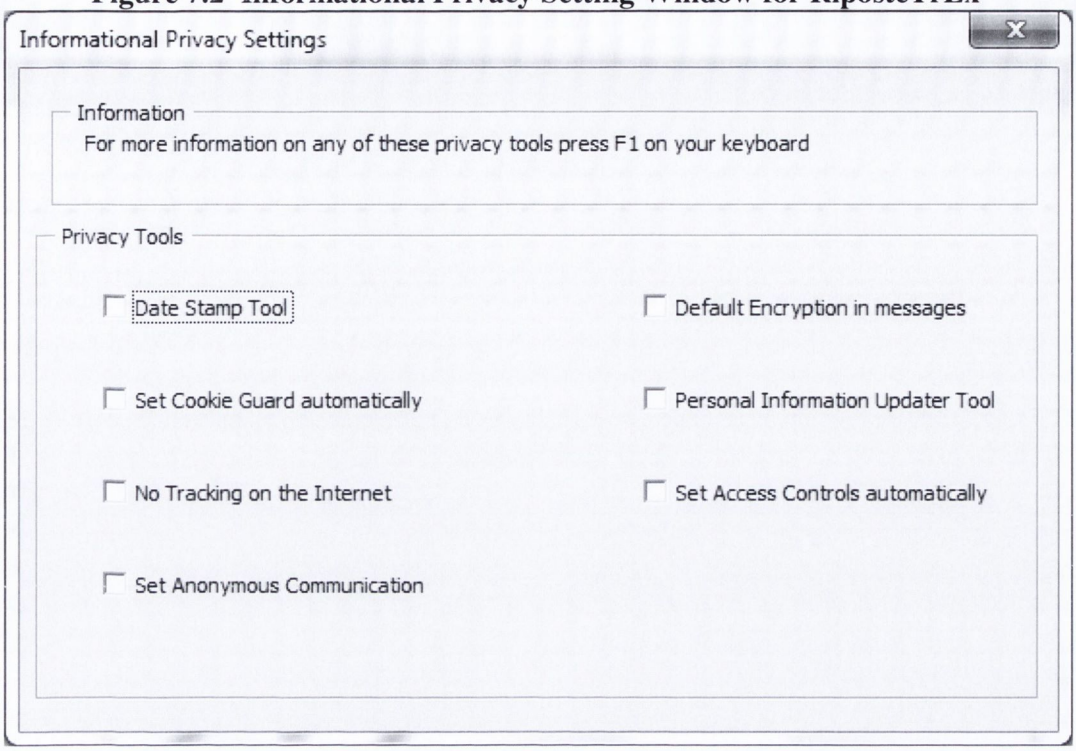
Within EUT-consistent versions of the PC model, IS users prefer wider risk management options, so as to be able to set the risk-expected reward trade-off in the desired fashion. In the revised version of this model, however, limits to rationality might render users unable to appreciate the usefulness of certain risk management options and, as emphasized by the literature on "nudging" reviewed in chapter 2, might even cause them to perceive ambiguity in situations in which they are offered the possibility of availing of options that they do not understand, resulting in

disengagement. That is, too many and too sophisticated risk management options for all users might not only be costly but also counterproductive.

For this reason, all the privacy settings and tools (available from the user's profile) are set to maximum protection of personal information *by default* and we require that, if users of the product (RiposteTrEx) wish to make their profile public within the system (disabling default privacy settings), they must actively seek out how to do so. This way, we allow for unfamiliarity with ICT and other limits to rationality that might render the user unable to choose the level of privacy protection before resorting to disengagement. The more expert users (those who actively seek to regulate their own privacy settings via their profile), instead, are given a choice of which privacy protection tools to enable and so as to allow for different levels of rationality within this class of users (e.g., fully expert users may wish to disable them all and make their privacy risk taking and risk handling behaviour decisions themselves whereas less confident users might disable only some of them). Overall, we cater for variation in limits to users' rationality by ensuring that the system has the capability of delivering maximum protection of personal information for users who are more prone to perceive digital settings as ambiguous, while allowing non competent users to set privacy levels in a way that best suits their attitudes and preferences towards privacy risk.

Figure 7.2 shows the set of Informational privacy tools that (expert) users in the RiposteTrEx system can choose to disable. Each of these privacy tools are described in Appendix H.

Figure 7.2 Informational Privacy Setting Window for RiposteTrEx



Notes: The more expert users can pick and choose the different privacy tools they wish to enable in the "Informational Privacy Settings" dialog box which appears when users indicate that they wish to set their profile to public. Users which select a private profile have all these settings enabled automatically.

7.1.2 Building users' trust

Increasing users' trust is important to increase willingness to interact online as it reduces risk perception, in that trust is an antecedent of perceived risk within the PC model. To build users' trust in a cost-effective way, RiposteTrEx relies on mechanisms such as opportunities for structured customer feedback, the provision of help and assistance tools and, most importantly, increased information transparency.

As far as customer feedback and the provision of help and assistance tools, these are described under the relevant headings in Appendix J.

As far as information transparency is concerned, it can be defined as giving users access to the information an organisation has collected about them, and how that information is going to be used (Awad & Krishnan, 2006). The semi-structured interviews found that the greatest cause of privacy concern was the fear that personal information would get used for other reasons than those for which it was originally collected. Thus, by increasing information transparency within the system, the privacy concerns of individuals should be alleviated. The RiposteTrEx system seeks to increase information transparency through a combination of the following:

- Allowing users access to the information that they have submitted to the system and recording all entities that have access to that information, also through the use of the PI Updater tool (Appendix H);
- Providing optional storage facilities for personal information (Appendix I);
- Displaying a trust or privacy seal throughout the system (Appendix J);
- Opt in or out solutions for newsletters and similar (marketing, etc.) notifications which, if perceived as invasive, might reduce trust in the system (Appendix J);
- Being embedded within a national de jure system (Appendix J);
- Anchoring to the trusted brand name of the Post Office throughout the system (Appendix J).

7.1.3 Increasing (actual and perceived) control

According to the PC model, greater control over personal information is, for privacy risk-averse users, desirable. In turn, increasing users' perceived control is important to increase their willingness to interact online as it reduces risk perception, in that perceived control is an antecedent of perceived risk within the PC model.

To maximize, in a cost-effective way, users' control over their personal information, RiposteTrEx relies on a combination of specific tools and more general design principles. The tools, both described in Appendix H, are:

- The Personal Information (PI) Updater Tool;
- IBE Encryption.

The relevant design principles, described in Appendix I, are the following:

- Closed nature of the network and multifactor authentication;
- Data minimization
- Decentralization of data, optional storage and system interoperability

To maximize, in a cost-effective way, users' perceived control and align it to the effective control, i.e. to mitigate the effect of biases that might lead to under-estimate the level of control in the system, RiposteTrEx relies on a combination of the following (described in Appendix J):

- Customer feedback
- Provision of help and assistance tools

7.1.4 Ambiguity (actual and perceived) reduction

The findings of the semi-structured interviews showed that older users perceive ambiguity in virtually all interactions online. They find it difficult to judge between what is a low threat to their informational privacy and what is a high threat. Subsequently, systems should provide options for these users to automate all informational privacy features that protect from harm, i.e. automate antivirus software updates and software updates from trusted organisations like Microsoft and IBM, thus reducing ambiguity regarding how to protect their personal information. By default, all personal information of users is private in RiposteTrEx and if users do not feel confident about changing their privacy settings, their personal information is protected from the start. The knowledge of having default privacy (factory) settings may reduce the uncertainty and ambiguity about unknown and immeasurable risks when interacting online.

Based on the results of the semi-structured interviews, secondary use of personal information was the main cause of ambiguity perception among the respondents. The RiposteTrex system sought to reduce this ambiguity through ensuring the system complied with the data protection regulations of the EU and through the use of two system tools (Appendix H):

- The Personal Information (PI) Updater tool
- The date stamping tool.

Moreover, as explained in Appendix J, the user can opt in or out of receiving newsletters and similar (marketing, etc.) notifications which, if perceived as invasive,

might increase perceived ambiguity, possibly leading to withdrawal and non-engagement.

7.1.5 Nudging

As noted, one key advantage of using the RPC model as a guide in deriving the system requirements, rather than more restrictive EUT-consistent versions of the PC model, is that it clarifies the link between users' possible biases, risk taking/handling behaviour and decisions concerning information disclosure and online engagement, thereby allowing us to use ideas on "nudging" drawn from the behavioural economics literature (and from the IS literature that is building on it) to improve the welfare of decision makers affected by such biases. A key requirement of the system is therefore the capability to carry out such "nudging", in a manner that, based on implications of the RPC model, should benefit IS users.

As far as alleviating the negative effects of representativeness bias is concerned, we rely on the very fact that the system is conceived to be run by an NPO. As explained in the literature review, representativeness bias, when used to form the basis for judgement, gives rise to a cognitive bias to the extent that an individual categorizes a situation based on a pattern of previous experiences or consolidated beliefs about that situation. Representativeness, as a method for forming beliefs, is about reliance on stereotypes (Kahneman & Tversky, 1972). Traditionally, the stereotype of NPOs is that of a trusted and neutral entity within society (US Postal Service Office of Inspector General, 2011). It was hoped that this stereotype of NPOs being trusted and ambivalent within society would work in favour of the RiposteTrEx system, in that NPOs have been the legal

guardians of private communication for centuries in the physical world and could also potentially fulfil that role in the digital world, though the fundamental aim of the system is to build up users' trust due to the genuine (i.e., objectively assessed) advantages provided by its functionalities and overall design. That is, though the long run aim is to build up users' trust on rational grounds, and we believe this should be possible because we designed the system in a manner that the PC model says should be beneficial to users, we acknowledge that the pursuit of such aim might be jeopardized by users' cognitive error and biases, if these are left unaddressed, and hope that positive stereotypes concerning the trustworthiness of the NPO will help in this respect, by nudging less expert users away from harmful effects of representativeness bias and towards the system.

Following a similar line of reasoning, in order to reduce the negative impact of availability bias and leverage on it to increase users' engagement with the system, we rely on the traditional image of the NPO as a reliable entity with a track record of reliability and no privacy breaches. As explained in the literature review, this bias occurs when individuals give preference to information and events that are more recent, or that were observed personally, and therefore are more memorable when making decisions. This is because memorable events tend to be more magnified and are likely to cause an emotional reaction (Sheffrin, 2002). The positive track record in terms of absence of privacy breaches is well known to many people in Ireland and forms the basis for the traditional image of reliability. The RiposteTrEx project intends to remind users of this track record and image of the NPO to encourage uptake of the system while trust in the system is built through users' engagement with it.

The anchoring-and-adjustment heuristic describes situations in which individuals use a number or a value as a starting point, known as an anchor, and adjusts that starting point until an acceptable value is reached (Epley & Gilovich, 2005). Some anchors are self-generated by participants and other anchors are provided by an external source (Epley, 2004). As suggested by Tversky and Kahneman adjustments are typically insufficient and are often too close to the original anchor (Epley, 2004). IS Research has established that *initial* perceived ease of use is an important factor influencing user acceptance and continued usage behavior of information technologies (Davis, 1989). These findings would seem to support the presence of anchoring and adjustment bias in individual's initial assessment of a technology's ease of use. If a user initially perceives a technology to be easy to use, the likelihood of continued use increases (Venkatesh, 2000). Therefore, in developing the RiposteTrEx system, another research project was undertaken between Escher Group and researchers at the Dundalk Institute of Technology (DKIT) who conduct research into User Interface Design for products that are in use by the elderly population in an assisted living environment. The research project was initiated by Escher Group to ensure the first experience a user has of the RiposteTrEx product is as easy as possible. Moreover, as previously explained, the privacy policy (which includes the cookie policy) for the RiposteTrEx system is clearly accessible on the homepage of the system to inspire confidence in the NPO's ability to protect personal information and to give a positive anchor for first time users. Figure 7.3 shows where the privacy policy can be accessed and Figure 7.4 shows the cookie policy pop-up which loads when accessing RiposteTrEx through a Browser.

Figure 7.3 Privacy policy of RiposteTrEx

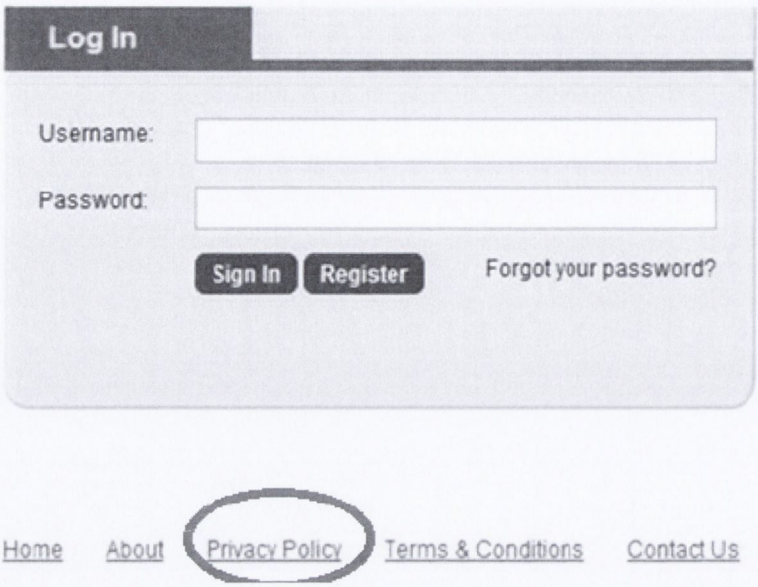
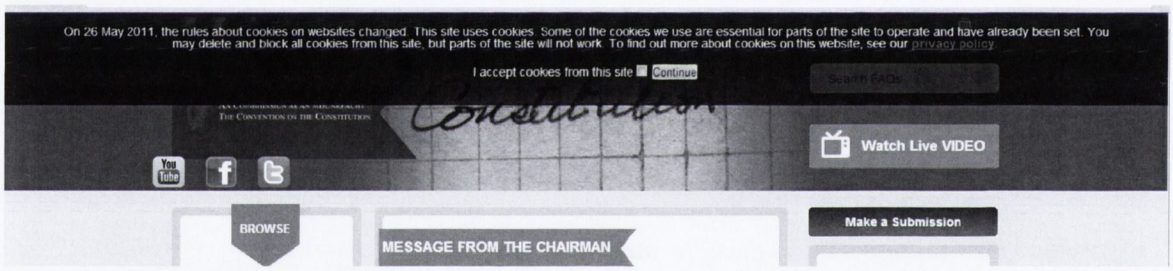


Figure 7.4 Cookie policy pop-up for RiposteTrEx



7.1.6 Data protection legislation alignment

The EU directive 2009/136/EC requires all organisations which process personal information to have a privacy policy and cookie policy accessible to their customers (European Commission, 2009). A privacy policy which also contains a cookie policy is available within the RiposteTrEx system both on the login page and on a user's profile page. It details the ownership and use of personal information by the system at the various stages of transferral and storage of personal information. It also explains how,

from a user's profile page, users can regulate their level of informational privacy based on a series of privacy protection tools available to them.

7.2 Description of the Focus Groups

When the first version of the product was due to be rolled out in pilot form for the Irish Department of Public Expenditure and Reform (DPER), in December 2012, in August and September 2012, eight focus groups were carried out to test the system's functionality and assess the reaction of the public to the new technology (these are different focus groups from the preliminary ones carried out in 2010, which could not be used because they had been designed before the RPC model was formulated and used in guiding the design of privacy risk management within RiposteTrex). The customer for whom the RiposteTrEx system was originally developed (i.e., the Irish NPO, An Post[20]) commissioned independent professional qualitative research agency to carry out the focus groups in order to avoid any conflict of interest. This prevented the Author from having full control of the design and roll-out of the focus groups. She was, however, allowed to submit a series of questions to be put to the respondents regarding how they felt the system protected their informational privacy and allowed them to manage privacy risk. The research company conducting the focus groups also agreed to comply with the ethical standards that we adhered to for this dissertation and they agreed to hand each participant a one page information sheet detailing the code of ethics being followed by this research (see Appendix G). The initial set of questions that we submitted were too long and would have taken up too much time during the focus

[20] Some aspects of this project are protected under a non-disclosure agreement that the Author has signed and therefore cannot be explained in detail, i.e. legal agreements between Escher Group and their customers.

groups. Therefore, a shorter set of 15 questions, which could take up to 30 minutes of each focus group, was decided upon. It was stressed, moreover, that once the 30 minutes were finished, the interviewers would move on with their own questions. To decide what questions to include, we established that the central aim of the focus groups was twofold:

1. To test the effectiveness of the RPC Model by checking whether the system, or specific features thereof, are well received; this amounts to directly or indirectly testing whether the users find the system requirements (that the features are designed to meet) worth pursuing, for a given level of engineering effectiveness in implementing the system requirements;
2. To test whether the system requirements derived from the RPC Model implications have been engineered effectively, by checking the system requirements have been met.

Table 7.2 shows the final list of questions that were agreed upon between Escher Group and An Post and asked of the focus group participants. The questions in italics test the effectiveness of the RPC Model, i.e. they test directly or indirectly whether the model-derived system requirements are seen as important by users, whereas the rest of the questions test whether the system requirements have been met, i.e. whether they have been engineered effectively. Escher Group was given the full video recordings (90 minutes) of each focus group. We (the Author and Escher Group) did not, however, have any further input into how the participants were asked to assess the product or how the focus groups were conducted.

We did, however, analyse each video recording and placed special emphasis on analysing the allocated 30 minutes within which our questions were asked. We also analysed the full 90 minutes to ensure a thorough analysis of the findings.

Table 7.2 Final list of questions

Questions	Relevant system requirements
Does this system help reduce the risk of your personal information being compromised or abused? (Why) Do you think security in the system is sufficient for safeguarding your information? (Why) Do the risk management options available within the system represent an improvement relative to what currently exists?	Alignment of the complexity of privacy risk management options to users' rationality (widening of privacy risk management options for expert users) and increasing perceived control
Would you store your personal information in this system (Why)? Does elimination of secondary use of personal information reduce ambiguity about how your information is used once it is submitted online? Is a closed system good?	Ambiguity reduction (especially by eliminating secondary use of personal information) and increasing perceived control
Do you trust the system? (Why) Is it clear how your personal information is privately transferred and stored in the system? Do you think your data will get used for other reasons than the ones stated in the video? If there was an independent auditor checking the system on a regular basis, would this improve your trust in the system? Do you trust An Post given their history of safeguarding personal information in the postal system without any serious informational privacy breaches occurring?	Increasing user trust (especially through increased information transparency and reliance on positive image and track record of NPO)
Do you think you will have more control over your personal information in this system than in others on the Internet? (Why) Is the customer feedback to the system sufficient? If there were user videos and user training sessions provided by An Post would this encourage you to use the system? Does the system minimise the amount of personal information it requires from you?	Increasing perceived control

The research company had access to a large sample of the Irish population. Thus, the demographics of the participants in the focus groups were evenly spread across age, gender, computer literacy, and rural or urban inhabitants. Two regions (four locations) of the country were involved, the first region was located in the east of the country (urban and rural Dublin) and the second was located in the west of the country (urban and rural Cork). Each focus group consisted of eight participants. The table below describes the demographics of the focus group participants.

Table 7.3 The demographics of the focus group participants

Group	Age	Mode of Access		Knowledge of Computers		Gender	Location
		PC at home only	Mobile and PC at home	*Standard	*Advanced		
1	18-24	50%	50%	50%	50%	50/50 M-F	Region 1
2	25-34	50%	50%	50%	50%	50/50 M-F	Region 2
3	35-44	50%	50%	50%	50%	50/50 M-F	Region 1
4	45-54	50%	50%	50%	50%	50/50 M-F	Region 2
5	55+	50%	50%	50%	50%	50/50 M-F	Region 1
6	18 - 34	50%	50%	50%	50%	50/50 M-F	Rural reg. 1
7	35-54	50%	50%	50%	50%	50/50 M-F	Rural reg. 2
8	18-54	No Internet access at home, using library, office, friends and family PCs		75%	up to 25%	50/50 M-F	Region 1

***Note**: Participants with standard knowledge of computers were capable of sending email and surfing the Internet for information and entertainment purposes. They all had either a Facebook and/or LinkedIn account or both. Participants with advanced knowledge of computers were capable of carrying out online banking, shopping, filing of taxes, and e-bill payment.

7.2.1 Overview of the Focus Groups

Each focus group meeting lasted 90 minutes. The groups were shown a ten minute video of the RiposteTrEx product where a detailed description of the product's functionality was given. The video described how the product provided protection of personal information through the use of encryption and how it ensured all users of the system were authenticated, enhancing the integrity and availability of the personal information, stored and transferred, within the system. Users were told how the system would increase trust by allowing a trusted authority, the NPO, to deploy and run the network, and how control over a user's personal information would increase by allowing the user to have a number of private 'personal' databases within the system to store subsections of their personal information, like financial information or health information. Only the user would have access to the databases containing their personal information and each database would be protected using a specialized form of encryption called Identity-Based encryption (Boneh and Franklin, 2003).

7.2.2 The RiposteTrEx Video Details

During the 10 minute video, the system was introduced as the new electronic communications system from An Post for Irish residents, state and local government and businesses. Users were first presented with a vignette about a completely digital world and how users would interact in this world by using a system called RiposteTrEx. It described a series of scenarios that could happen in everyday life in this digital world. One scenario was online banking and another was interacting digitally with

government. The video went through each step of these scenarios in detail, describing how each step is achieved and how each step protects individuals' personal information.

It then described how the system allows all members of society to communicate privately with one another. It pointed out how the product was an enhancement to email because it would be difficult for anyone to view the contents of RiposteTrEx mail as the contents were encrypted by default. It outlined the motivation for using encryption as being due to the fact that the system simulated the level of information protection enjoyed by individuals with the physical postal system.

It went on to show how users would be able to manage their own personal information and control who has access to it. It argued that with this functionality users would be able to not only store and keep track of their personal information but also to analyse their own information, i.e. analyse their spending habits, compare their bills year on year and so on. Due to its secure nature the system would facilitate online payment of bills and the transfer of sensitive documents. It then discussed how users would be able to avoid spam by selecting for themselves (opt-in) which mailing lists, from authenticated companies, to sign up to.

The video detailed the steps involved in the registration process for the system. This is done through a multifactor authentication process, as explained in appendix I of this dissertation. The security benefits of multifactor authentication were then briefly outlined to the participants and how the NPO is in a good position to carry out multifactor authentication as they can independently verify the physical address of all citizens registering for the system. Then, when the product introduction and explanation

of the registration process was complete, the video described the main functions and tools of the system and their benefits to the user. It explained how storage was available for users to store their personal information within the system if they wished. It emphasised that this storage of personal information was optional and no personal data would be stored without the specific consent of the user. The trusted NPO, An Post, was the guardian of all the personal information stored in the system, just like it was in the physical world. Emphasis was also placed on the fact that personal information was not centrally stored and that an extra level of authentication was needed to access each personal information database of a user.

The video then talked about information transparency and the privacy options (as outlined in this chapter) available to the users. It outlined how users could continually contribute towards improving their e-postal system through the user feedback functionality via a public database stored within the system. The video was finally concluded with a summary of the privacy features (tools previously listed) available in the system for users to protect their personal information. In this section, the video pointed out how the system provided enhanced confidentiality through the (optional) use of IBE encryption and how it ensured all users of the system were authenticated, thus enhancing the integrity and availability of the personal information within the system. Users were told how the system increased trust by allowing a trusted authority, the NPO, to deploy and run the system, and how a user's control over their personal information was increased by allowing the user to have a number of private databases distributed within the system(or downloaded to their local machine[21]) to store sub-

[21] Unfortunately, the ability to transfer personal information to other database management systems was not explained in the focus groups. This may have impacted the participants' attitudes to the system.

sections of their personal documents, like financial information or health information, in separate databases. It was made clear that even the administrators of the system could not access the private databases of the user. Again, this feature replicates the original postal service where postal workers could see the envelopes going through the system but the content of the envelopes was protected. It was also noted that the system was being built according to the security standard ISO 2700 and would eventually undergo auditing for security certification.

7.2.3 Post Video Details

After the video finished, the rest of the allocated 90 minutes (circa 75 minutes due to 5 minutes of introductions and 10 minutes of video) was spent on a general discussion of privacy and the participants' views of the privacy risk management e-postal system being presented were discussed and recorded. The Author's questions (outlined in Table 7.2) took up about 30 minutes of the time in each focus group, which left 30 minutes for the analysis of the system for An Post. Finally, a hypothetical scenario was presented to each focus group and their opinion was sought regarding this scenario, the final 15 minutes of the meetings was used for this scenario.

7.2.4 Analysis Method for Focus Group Data

The same analysis approach used for the semi-structured interviews was used for analysing the data from the focus groups, i.e. the Constant Comparative Method (CMM) (Glaser, 1965). The method was considered appropriate for analysis of the focus groups because, as previously discussed, this dissertation uses both qualitative and quantitative

approaches to data gathering, in such circumstances the CCM is a good fit (Glaser, 1965). In order to best compare the results of all three sets of data, i.e. the semi-structured interviews, the online questionnaire and the focus groups, the CCM method of analysis was used to explore in more depth the tentative hypotheses. The CCM provides a systematic approach to substantiating or disproving hypotheses without losing the richness and contextual basis for interpreting and validating results common in qualitative data analysis (Glaser, 1965).

7.3 Findings from the Focus Groups

As noted earlier, the central aim of the focus groups was twofold:

1. To test the effectiveness of the RPC Model by checking the system (or specific features of the system) is well received, i.e. whether the system requirements are seen by users as worthy of pursuing, for a given level of effectiveness in engineering these requirements into the system;
2. To test whether the system requirements derived from the RPC Model implications have been engineered effectively by checking the system requirements have been met.

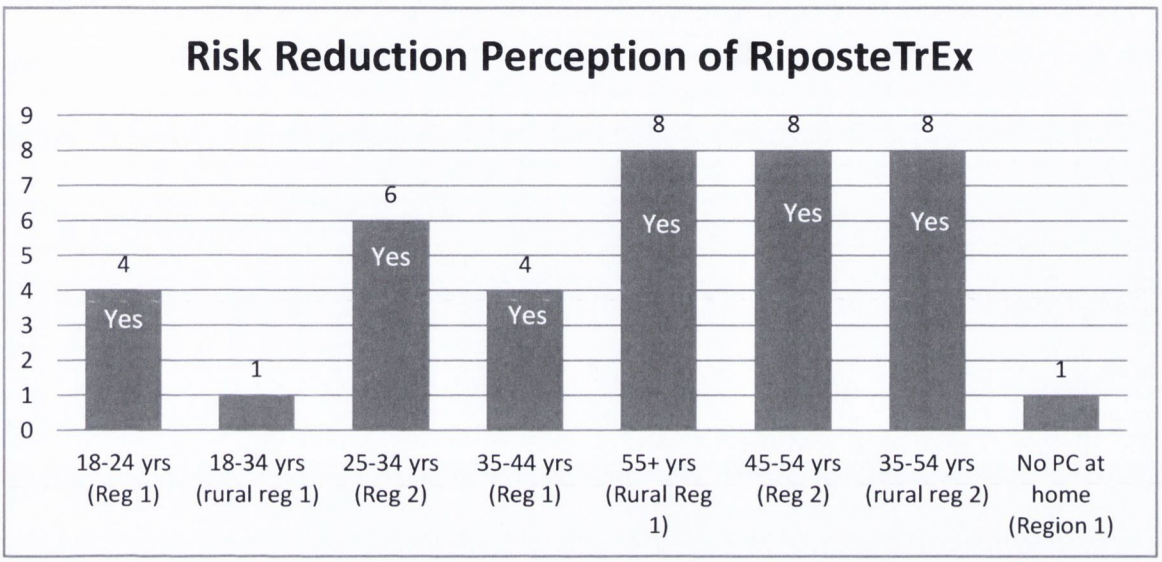
The next two subsections discuss answers to questions pertaining to each one of the aims of the focus groups outlined above.

7.3.1 Effectiveness of the RPC Model as a Theoretical Basis for the System

The graph below gives a snapshot of the groups' acceptance of the product in terms of their perception of whether RiposteTrEx helps them reduce the risk of breach of

informational privacy. The vertical axis of the graph shows how many individuals in each focus group perceived that the system reduced risk. The horizontal axis shows the eight focus groups and the ages and location of the participants.

Figure 7.5 Responses to the question: Does this system help reduce the risk of your personal information being compromised or abused?



Age had the most impact on the acceptance of the system, which is apparent from the graph, whereas there were no appreciable differences in this regard between participants who lived in a rural setting and those who lived in an urban setting.

The 18-24 age group spent most of the time during the focus groups informing the interviewers how they achieve all the functions of the RiposteTrEx system through using their own expertise and knowledge of how to avoid risk when online. They made recommendations on how to eliminate privacy concerns and were, in general, neutral to the RiposteTrEx system. Some participants of this group suggested it was more for the older generation who felt less competent on the Internet and who spent their time interacting with the government and paying bills. The younger participants felt that a lot

of the functionality did not apply to what they did on the Internet, i.e. social networking and research for study and hobbies. The older age group (45-54 and 55+) instead felt the information system showed potential for simplifying their information processing and management efforts online. However, they indicated that some adjustment would need to be made to the RiposteTrEx system before they would agree to use it. The choice of deciding how to use this technology was paramount. In particular, the older age groups agreed that allowing the user to decide whether they wished to retain their personal information in paper format, i.e. *offline,* or whether they wished to go *online* was essential.

The majority of older users (45-54, 55+) tended to like the idea of being able to organise their personal information, compare financial information, i.e. compare budgets and bill payment year on year, and track and control their submission of personal information to various government departments and companies. This seemed to give the participants an increased perception of control over their submitted personal information but, ironically, the same participants tended to be reluctant to store their personal documents in the system for this data analysis to take place.

Likewise, being able to access personal documentation like passports and health records especially when abroad was seen to increase the benefit of submitting/storing personal information electronically in such a system. Having access to a complete set of medical records online, especially for participants who had aging parents or ill children was seen to increase the benefit of the digital world and simplify difficult situations. However, the majority of participants continued to be reluctant or unable to clearly specify the

privacy measures they wished to see in place to satisfy their privacy concerns surrounding the use of this information system in such scenarios.

The terms 'ambiguity' and 'data minimisation' were particularly difficult to explain and to clarify and thus analysing the response of the participants regarding whether the system eliminated perceived ambiguity and minimised the need to submit personal data to the system was difficult. Proof that there would be no secondary use of personal information was also difficult to give and this would need to be clearly shown before users accepted the system was truly using personal information in the way that was stated in the privacy policy. Such proof could be in the form of security certification or privacy seals which, however, are yet to be obtained.

The majority of groups felt that submitting personal information to the government and businesses via a privacy enhanced messaging system like RiposteTrEx would bring some benefits and convenience but the submission and storage of personal information to the system would need to remain optional. This points either to the difficulty of removing deep rooted perceptions of ambiguity or to the need to allow users to decide how their personal information should be used, at least until sufficient trust has built up. That is, while attempts to nudge privacy risk-adverse users towards trusting the system seem to have been somewhat effective, it remains important to build trust over time through beneficial and breach-free system-facilitated interactions.

Overall, the fact that the older generation perceived that the product has the potential to reduce risk when transacting and interacting electronically (that is, that the older the participants the more receptive they were to the technology) is coherent with the RPC

model to the extent that older users value their privacy more and therefore are more averse to privacy risk. Consistent with this model, it might also be explained by the fact that older users might be less familiar with ICT and might therefore find both the especially cautious default privacy setting and the automated privacy risk management functionalities beneficial. The fact that the younger participants found both features redundant provides evidence in support of the choice of widening the range of available risk management options, and therefore in support of the RPC model implications that underpin such choice. The fact that they deem such features essentially as an unwelcome nuisance is also interesting though, in the context of the RPC model, to be expected. In fact, these users do not reject these features for failure to handle their complexity but simply because their presence leads to a waste of time and attention, which can be seen as unnecessary risk handling behaviour costs that these users are unwilling to bear (because they are not very averse to privacy risk).

7.3.1.1 Evidence of Cognitive Bias

Recurring references to well-publicised stories of hacking, including stolen laptops, websites being hacked and credit card details stolen, and referencing cases of privacy breaches suffered by government agencies implied that a lot of the fear regarding protection or personal information was generated by the media. All eight focus groups mentioned the media as a source for stories about threats to informational privacy. This is evidence of bias, based on availability of information, in the decision-making processes of the participants.

7.3.1.2 A Hypothetical Scenario

Due to the fact that some privacy protection and security measures were not yet implemented for the RiposteTrEx system, i.e. the security certification and the privacy and trust seals, the interviewers anticipated some negative feedback from the focus group participants. Thus, a hypothetical scenario was presented to the participants. This hypothetical scenario was also adapted according to the feedback from the focus groups. This gave us the opportunity to test the effectiveness of the RPC Model controlling for the effectiveness of the engineering of the model-derived system requirements. In other words, this scenario gave us the chance to test the effectiveness of the RPC Model without having to consider the fact that the systems requirements might have been poorly implemented or that their implementation might have been poorly explained to users in the focus groups, either way biasing the participants perception of the effectiveness of the system for managing privacy risk.

Each group was presented with a hypothetical scenario depicting a system that had:

1. Both a security certification and a privacy seal to prove the system worked as it was described to work, i.e. no covert data gathering allowed and complete transparency when handling personal information.
2. An Internationally renowned IT company that helped to design and develop it. This company had years of expertise in security implementation and maintenance.
3. Decentralised storage of personal information into private independent personal databases, each requiring password authentication to access them, and each stored within a different instance of a RiposteTrEx system.

4. The users had a choice to selectively sign up for different digital services on offer (i.e. requiring different types of personal information, like financial, health or demographic information) and thus availing of different levels of informational privacy protections.

The last three points were added intuitively by the interviewers having received the strong feedback from the participants about the necessity of optional, decentralised storage of personal information and the need for continued investment in security measures for the system.

The majority of participants (except 18-25 and 18-35 who persisted in arguing that there was no need for such a system) admitted that they would be more inclined to consider using the system in this hypothetical scenario because:

1. Ambiguity concerning the secondary use of their personal information would be reduced by having either a privacy or trust seal and security certification;
2. Trust in the technology would increase, as a result of collaboration with an internationally renowned organisation with expertise in security of IT systems and, thus, trust in the administrators of the technology that was protecting their personal information would increase;
3. Control over personal information submission would increase as a result of users having the *option* to sign up to digital services which require the submission of different subsets of personal information;
4. Additional control over personal information storage would be achieved by allowing users to decentralise storage of their personal information in any way they saw fit and across multiple instances of RiposteTrEx, run by multiple entities not just An Post;

5. As a result of the previous points, the perceived risk in using the system would decrease.

Even though the majority of focus groups admitted to being more inclined to use the RiposteTrEx system described in the hypothetical scenario, all age groups refused to believe that such a scenario was possible or realistic in the current information age. The younger age groups (18-24 and 25-34 years) when faced with this scenario agreed that the hypothetical scenario was an improvement on the existing RiposteTrEx system. However, the majority still indicated they would not use it themselves as they could not see a clear need for it. They continued to believe that the hypothetical RiposteTrEx system would be beneficial to the older generation who were less experienced with Information Communication Technology.

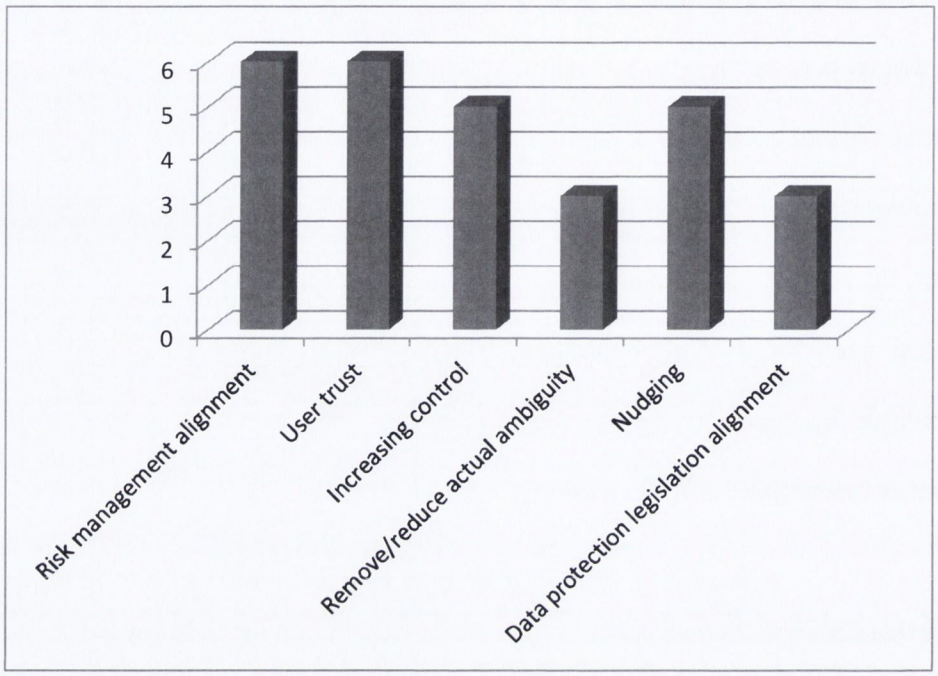
The fact that the hypothetical scenario was supported by the focus groups suggests that, if some outstanding engineering problems were resolved (i.e., if the RPC Model-derived requirements were perfectly engineered into the system), the model would be effective in managing informational privacy risk for users.

7.3.2 Effectiveness of system Requirements implementation

The graph below outlines the overall findings of the focus groups in relation to select system (sub-)requirements and how effectively (according to the participants) they were met in the RiposteTrEx system. The vertical axis of the graph shows how many focus groups perceived that the system was an improvement on what is currently available to them electronically in terms of protecting their personal information. The horizontal

axis shows the system features (outlined in section 7.1) that were assessed by the focus groups.

Figure 7.6 Effectiveness of implementation of system requirements (ambiguity reduction and data protection legislation alignment scoring lowest)



Six of the focus groups believed the widening of privacy risk management options (the provision of privacy protection tools) helped users of the system to better manage their personal information (all groups except 18-34 years and No PC at home). These six focus groups also believed the system increased transparency and thus user trust compared to the options that are currently available to them on the Internet (all groups except 18-34 years and No PC at home). Five focus groups believed the system increased the control that they would have over their personal information (all groups except 18-24 years, 18-34 years and No PC at home). Only three of the focus groups accepted that the system would substantially reduce ambiguity related to secondary use of personal information (groups 55 years+, 45-54 years, 35-54 years). Five focus groups

like the 'nudges' the system provided in terms of default privacy settings being set to maximum (35-44 years, 45-54 years, 55+ years, 35-54 years, no PC at home), however, another form of nudging, i.e. leveraging the trusted brand name of the NPO to counteract the effects of cognitive bias was only supported by 2 focus groups (55+ years and 45-54 years). Finally, three groups believed the system aligned well to the data protection legislation regarding the minimum use of personal information within the system (55+ years, 45-54 years and 35-54 years) the other five groups believed this could be improved in the system.

In each focus group, there was a strong sense that, in order to preserve informational privacy, separation or decentralisation of personal information in an online context was essential. The majority of participants had reservations about storing sensitive personal information[22], like health information and/or passport details, within one single closed network. When it was outlined that the information would be stored separately in different encrypted databases within the network, all participants felt that this was still not acceptable because once the network was compromised, all the databases stored in the system would be at risk and as a result all of their personal information could be threatened. These reservations were repeated to varying degrees in six of the eight focus groups, with the exception of the 55+ years and 45-54 years focus groups. These two groups argued that inevitably the complete digitalisation was going to happen in the future and they were reasonably comfortable with the fact that the Irish NPO, An Post, would be the custodians of such important information.

[22] Sensitive data is an important subset of personal data. Sensitive data is that which reveals racial or ethnic origin, political opinions, religious beliefs, trade union membership, health or sex life details. This information is regarded as sensitive because it could expose the data subject to discrimination as well as infringe on the very fundamentals of privacy. Health information as defined by this article would include past or present information on physical or mental state as well as any abuse of drugs or alcohol (Herold, 2002)

Storing the personal databases on different, standalone closed networks was seen to be essential to the success of such a technology. So, while the division of personal information into numerous databases within a single closed system and the ability to port any documents from the RipostetrEx system to another data management system went some way in relieving participants' concerns about unauthorised use and informational privacy breaches, it did not go far enough. A series of interconnecting closed networks, i.e each individual institution like a hospital or a bank should have its own RiposteTrEx closed system. Each independent closed system would require individual and separate authentication to gain entry. This was the minimal level of security acceptable for storing *sensitive* personal information, such as health records and passport details, in digital format.

It was also agreed by the six focus groups mentioned above (all groups except the 55+ years and the 45-54 years focus groups) that the NPO should not run all closed networks. Banks should be put in charge of storing their customers' financial data and the banks should administer their own closed network and likewise for hospitals and other institutions. Users should be able to decide which RiposteTrEx system they wish to join and submit their personal information to, i.e if they wish to join the bank system and have a database in that system which stores all their financial data, but to keep their health records off line and stored in paper format in their GP's surgery or their local hospital, they should be allowed to do so. The participants felt it essential that they were still allowed the option to stay 'offline' with whatever personal information they wished and they should be allowed to pick and choose which information they wished to submit online. In other words, the idea of *obliging* individuals to interact with the government

and businesses electronically was rejected. This point was particularly important for participants who had elderly relations. They emphasised that it would be too burdensome for these elderly people to start interacting online. This would usually mean that the responsibility would ultimately fall on the participants to help their elderly relations interact with the system. Even though it was stressed by the interviewers that there would be no obligation on the elderly (or anyone) to change the way they interact, this point was mentioned in three of the eight focus groups (no PC at home, 35-54 years and 45-54 years).

7.4 Reflection on the Findings

There were three key findings from the eight focus groups. The first finding was the need to distribute the personal databases across multiple independent instances of the RiposteTrEx system. The second key finding was the need to increase trust in the technology of the RiposteTrEx system concerning its ability to protect personal information within the system and the third finding was the importance of ensuring the submission of any personal information be entirely optional for the user, experienced or inexperienced alike. These findings are now discussed in more detail in turn.

7.4.1 Distributed Personal Databases

Unfortunately, the participants of the focus groups were not told about RiposteTrEx's ability to transfer documents (XML documents) to other database management system or its interoperability functionality. Perhaps as a result of this, participants expressed concern that the entirety of their personal information would be at risk of the

RiposteTrEx system was breached. Re-authenticating with the RiposteTrEx system to access each personal database within the system, despite it being time consuming, was generally a popular choice, given the sensitivity of some of the personal information that could potentially be stored, i.e. medical records and financial data.

Some female participants within the 35-44 age group highlighted the fact that multiple passwords would complicate the system. These women explained that their life was full and they would have very little time to keep authenticating between instances of the systems. They suggested that perhaps the level for authentication used for each of the instances of the personal databases stored within the RiposteTrEx system should be left up to the user to decide. Another reason for leaving this choice up to the user was because the value of personal information is subjective. Users may decide to protect some personal databases more than others.

7.4.2 Trust in the Technology

A second key finding involved the concept of trust in technology. One form of trust was satisfied by the system, institutional trust. The NPO was generally seen as a benign trusted authority that would not threaten users' informational privacy. One exception to this was that the younger age group were inclined to think the NPO might too readily divulge personal information to the government if requested to do so.

Trust in the security of the technology that the NPO was believed could deliver was seen to be insufficient. The majority of the focus groups (except 45-54 and 55+) did not believe that the NPO would have the resources to adequately protect their personal

information in the future. Knowledge that the security system was being designed by a leading private company in the postal industry, Escher Group Ltd, went some way to increase their trust in the system but initial reactions tended to remain (anchoring and adjustment). An example was given in one focus group that Google has many more resources to dedicate to security issues and even they found it challenging and, thus, the NPO with its lack of experience and resources would be wholly inadequate.

7.4.3 Optional Submission of Personal Information

The third key finding was that even though the participants agreed that, for transferring personal information, privacy concern would decrease for users using this system than for users of the Internet currently, they argued that it would introduce another type of concern, concern regarding the obligation of 1) submitting sensitive personal information electronically and 2) interacting with government electronically.

Ironically, a user's perceived control over *submitted* personal information was seen to increase by using the system, but likewise their concern over *having to submit* personal information was also increased, as a result of the user feeling pressured into interacting with government electronically. The decision about whether to start electronic interaction with the government would need to be optional and selective, meaning the user should be allowed to select which type of personal information they are happy to submit electronically to the RiposteTrEx system and which type they would like to remain in paper format.

7.5 Conclusions Drawn from the Focus Groups

The RiposteTrEx project sought to deliver a robustly private communications system that would lead to the creation of widespread trust and confidence in the electronic postal industry. The experiences of the RiposteTrEx project underlines Gurses et al's. (2011) conviction that the menaing of data minimisation needs to be interpreted on a case by case basis, due to the complexity and subjectivity of how best to safeguard personal information while still facilitating digital communication. Upon reflection, it is difficult to achieve a *single solution* to reducing informational privacy concerns. Based on our analysis of the RiposteTrEx system the implementation of the system requirements outlined for RiposteTrEx goes *some* way towards reducing perceived privacy risk and ambiguity in online interactions but it does not eliminate them completely or for every user. Another conclusion from this phase of the project was that the challenge of developing a privacy risk management technology does not seem to lie in *deriving* the system requirements for the product but rather in finding the most appropriate software functionality and tools and configuring those tools in such a way as to implement sufficient privacy protections for all users. This implementation of privacy protection functionality needs to be done on a case by case basis depending on what the information system is trying to achieve.

Gurses, Troncoso and Diaz (2011) argue that engineering information systems according to the principles of Privacy by Design (PbD) requires the development of a general methodology to guide managers and development teams on how to properly interpret the principles for each particular case but they points out such a methodology cannot be reduced to a simple checklist that can be ticked away for compliance reasons.

We make a similar argument for engineering information systems according to our RPC Model. Instead of *developing* a new methodology framed as a somewhat restrictive sequence of steps and actions, we use the rich ADR methodology to guide the NSPD management and development team on how to interpret the implications of the RPC Model for a particular case of engineering informational privacy into a class of systems, i.e. electronic postal systems.

Overall, we found that the challenge lies not so much in improving the RPC Model, but rather in adequately engineering the model normative implications into information systems so that the functionality of the system is 1) not prohibitively slow or complex for users to use every day, 2) is engineered in such a way that it cannot be manipulated by hackers and wrong doers to achieve subversive goals. This dual challenge is formidable as it entails not only implementing appropriate security mechanisms within the system but also convincing people that the system is both secure to an acceptable degree, so that it protects their informational privacy the majority of the time (save for exceptional unforseen circumstances), and easy enough to be used effectively and efficiently.

7.6 Privacy Design Principles Summary and Generalization

To sum up, we have identified six general system requirements, described in section 7.1, and a number of system features that are needed in order to meet the requirements, primarily the set of system functionalities described in Appendix H and the technical design principles described in Appendix I. These features can be seen as reducing down to a means of pursuing two general organizing design principles, which summarize the

two key implications of the RPC model for IS like the software product considered in our ADR project. The first organizing design principle is to allow users to set their own preferred trade-off between privacy risk and expected benefit from digital interactions and safeguard the personal information that they deem most valuable. The second one is that the system should also take into account the limits to users' rationality, delivering maximum protection of personal information for users who are more prone to perceiving digital settings as ambiguous, thus increasing their perception of control over their personal information and helping build their level of trust in the system, without requiring them to carry out difficult risk assessment tasks or to undertake demanding risk handling behaviour. According to the RPC Model, less experienced users (subjects to more binding limits to rationality) should find this beneficial (say, improving of expected utility).

As a further step, we map the set of system requirements and key design features for the RiposteTrEx system to a set of system requirements and design principles for a broader class of IS, so as to offer guidance (based on insight provided by the RPC model) for the development of IS that share objectives broadly comparable to those of RiposteTrEx. To derive the principles, we reformulate the system objective in more general terms as the provision of services for the online interaction between individuals and between the latter and organizations, by using an electronic infrastructure that transfers and stores users' personal information, maintaining levels of informational privacy that users deem acceptable so as to elect to regularly use the system to interact. The main difference between this and the earlier formulation of the system objective (given in the introduction of section 7.1), which applies more specifically to

RiposteTrEx, is that we do not require the system to be based on an electronic postal system linked to a national de jure system.

Under this more general objective, we can retain the key organizing design principles, which follow directly from the implications of the RPC model and the specified system objective, i.e.

- the system should allow users to set their own preferred trade-off between privacy risk and expected; benefit from digital interactions and to choose the personal information to safeguard (that they deem most valuable);
- system design should take into account the limits to users' rationality, delivering maximum protection of personal information for users who are more averse to privacy risk and more prone to perceive digital settings as ambiguous.

We may also retain the five system requirements, as enumerated just below Table 7.1, and most of the associated system features. More specifically, we may retain all system functionalities (Appendix H) and all technical design principles (Appendix I). It is only some of the other system features described in Appendix J that would not be relevant, most importantly the link to a national de jure system (which may or may not be available for non-postal systems or privately run systems) and the anchoring to the trusted brand of the national post (which may be however replaced by another type of trusted brand).

Table 7.4 outlines the mapping process for how the privacy design principles for privacy risk management information systems were derived from the set of general system requirements for RiposteTrEx.

Table 7.4 The mapping process for how the organising (privacy) design principles for privacy risk management information systems were derived

General System Requirements	System Features for Privacy Protection	Organising (Privacy) Design Principles
1. Alignment of the complexity of privacy risk management options to users rationality. 2. Building of users' trust. 3. Increasing actual and perceived control 4. Ambiguity (actual and perceived) reduction. 5. Nudging 6. Data protection legislation alignment.	1. Date stamping tool 2. Cookie guard 3. No tracking 4. Anonymous communication 5. Encryption 6. Personal information updater tool 7. Access controls Technical Design Principles 1. Closed nature of the network 2. Multifactor authentication 3. Data minimisation 4. Decentralisation of data Other System Features, I.E. Security & Trust 1. Security certification 2. Displaying trust and privacy seals 3. Opt-in solution for newsletters and notifications 4. Customer feedback facility 5. Provision of help and assistance tools	1. Allow users to a. Set their own preferred trade-off between privacy risk and expected benefit from digital interactions b. Safeguard the personal information that they deem most valuable 2. The information system should take into account the limits to users' rationality to deliver maximum protection of personal information for users who are more prone to perceiving digital settings as ambiguous.

7.7 Conclusion

This chapter described the system requirements derived as normative implications from the RPC model (under given objectives and constraints) and their mapping to system features intended to ensure that the product, i.e. ReposteTrEx, meets such requirements. The results of focus groups aimed at ascertaining users' acceptance of the product were also reported, and used to infer the efficacy of both the RPC model (which served as a theoretical guide in setting system requirements) and of the engineering process (which sought to achieve the system requirements). During the focus groups, it was found that, while the RiposteTrEx system managed to reduce risk perception regarding the threat to informational privacy concerns of individuals, it did not fully eliminate ambiguity with regard to secondary use of personal information once the information got submitted to the system. Once again, familiarity with ICTs seems to play an important role, having an influence on participants' willingness to use the system, in that the younger participants (who were very confident about their ICTs familiarity) were not interested in using the system, whereas the older and less confident age groups were more inclined to see its benefits. This might suggest that such a system, if implemented nationally, could help towards increasing digital inclusion among the older population but might not be well received by the younger ones. Overall, our results point to the difficulty to engineer in fully the normative implications of the RPC model rather than to any fundamental weakness of the model itself.

8 Conclusions, Contributions and Future Work

In this dissertation, within an overall ADR framework, we have put forth a Revised Privacy Calculus (RPC) model which takes into account limits to rationality in the informational privacy decision-making processes (privacy calculus, PC) of individuals when faced with ambiguous digital scenarios, we have tested this model using an online questionnaire and twenty semi-structured interviews and, finally, we have investigated whether this RPC model can be usefully engineered into a privacy risk management information system.

In this chapter, we review the work completed in this dissertation, draw together our overall conclusions based on this work and offer recommendations for the design of privacy enhanced electronic postal systems and other IS. In the first section, we outline the contributions that this work has made to the field of IS. We then discuss the limitations of the work and we set out possible directions for future research. Finally, a few concluding remarks are given.

8.1 The Main Results Restated

This research has made 3 contributions to the body of IS knowledge. The first contribution is methodological in that the dissertation describes the study of a case entailing the application of a recently formulated design science research methodology, namely ADR, in a novel extra-organisational setting, namely a NSPD setting. The

second main contribution of this research is theoretical in nature, in that, by considering heuristic biases and bounded rationality, we were able to redefine the PC model in a manner that more closely fits the decision making process of individuals when dealing with electronic information disclosure in uncertain or ambiguous situations. Finally, the third main contribution of this research is applied in nature in that we provided preliminary privacy design principles to guide further development of privacy risk management information systems and other IS. These three central contributions are discussed in further detail in the following subsections.

8.1.1 Methodological Contribution: Using the ADR methodology for Engaged Scholarship

As outlined above, one of the main contribution of this research is that it adds to the body of methodological research in IS by describing a case study centred on an application of a novel design science research methodology, namely ADR. We provided one of the first applications in the IS literature of this methodology and one of the very first case studies of its application. In fact, due to ADR being a relatively new approach to conducting Design Science Research in IS, few case studies, which provide details of how software design and development can be facilitated using this methodology, currently exist. During the case study, we demonstrated how learning was achieved, within the over-arching ADR project, by employing a multi-method research approach. As part of this multi-method approach, various data types were gathered from three different sources, including an online questionnaire, semi-structured interviews and focus groups. This diversity of data types and sources permitted to draw richer and more reliable conclusions on the validity of the RPC model, and therefore allow us to more

confidently view this model as a valid conceptual basis to derive design principles for electronic postal systems.

Additionally, the case study was conducted in the context of NSPD for extra-organisational deployment, a novel setting not previously considered by the literature. In this context, in line with Sein et al (2011), we demonstrated how the ADR methodology provides a new approach to the challenge of engaged scholarship. We found that the ADR methodology was particularly well suited to support engaged scholarship in the NSPD environment in a number of ways.

The first anecdotal finding was that, after the project was retrospectively re-structured according to the guidelines provided by the ADR methodology, a significant improvement seemed to occur in a number of important respects pertaining to the organization of the project, for example greater emphasis on the key milestones of the project and significantly reduced time between each testing cycle. However, this result did not happen easily. It became clear, early in what we previously referred to as the advanced research stage, that the 'stages' of an ADR project (see Figure 1.2 and Table 6.1) need to be more cyclical and iterative in nature than anticipated. As new features were being added to the IS under development right up to the final stages of the project, stage 2 frequently needed to be revisited. As such, de facto, stage 2 continued up until the end of the project and stages 3 and 4 were also iterative in nature and alterations to the outcomes in all three of these stages were constantly being made.

Occasionally, the knowledge building goals of the Author were subordinated to the practice and change-related goals of the industry partner (Escher Group). Yet, once

these transitional issues were resolved, all parties agreed that the resulting project outcomes were more rewarding than before the implementation of the ADR methodology. This is seen to be because of the heightened efficacy and efficiency in achieving the research and practical aims of the project which were a consequence of the adoption of the research methodology. Escher Group, moreover, found it beneficial that the Author had published the project outcomes in academic conferences and book chapters. They felt it added credibility to their new product and showed their dedication to developing new software products grounded in the latest research, best practices and state of the art technology.

The ADR method provided Escher Group with an explicit and coherent set of concepts and procedures for transforming their product ideas into reality. By articulating and exploring opinions in an open environment with colleagues and researchers, ideas were more easily captured, developed and transformed into design constructs. This type of analysis has been emphasised by Lester and Piore (2004) as aiding the innovation process. Moreover, senior management and the RiposteTrEx NSPD team witnessed first-hand the benefits of collaborating with academia for improving their product offering. Consequently, the company is now engaging more enthusiastically with research institutions in the region. They are currently members of a consortium collaborating with a group of local research institutes to establish an applied research centre. This centre will explore similar ADR projects for the mutual benefit of industry and academia.

From a more general epistemological point of view, the ADR methodology facilitated dyadic learning, i.e. when one member of a dyad develops knowledge then the other

member develops that same knowledge also. The NSPD team in Escher Group learned a great deal about engaged scholarship during the project and the Author learned a lot about NSPD. This type of knowledge sharing breaks down barriers and facilitates increased collaboration among industry and academia. The Author gained a diverse and multifaceted understanding of the ICT industry thanks to the interaction with experienced management and development teams involved in the project. The tacit knowledge of the project members, built up over decades in the industry, provided a useful perspective to the research project. The Author also found that the ADR methodology, when used in such contexts, helps to broaden the scope of the research endeavour, focusing less narrowly on the scholarship of discovery and expanding the academic research mission to more fully embrace the scholarship of application and dissemination (Small and Uttal, 2005).

8.1.2 Contribution to Theory: A Revised Privacy Calculus Model

The results of the online questionnaire, combined with insights from the theory of bounded rationality and results from the behavioural sciences (especially behavioural economics and psychology), form the basis for the second main contribution of this dissertation, i.e. a redefinition of the PC (Privacy Calculus) Model. In particular, by considering heuristic biases and bounded rationality, we were able to redefine the PC model in a manner that, as demonstrated by the empirical findings outlined in chapter 5, more closely fits the decision making process of individuals about electronic information disclosure.

Our findings support Drennan et al. (2006) in that they argue that risk awareness leads to suspicion, which subsequently leads to what they call "privacy active behaviour" similar to our "risk handling behaviour". They too found that a high level of risk perception by individuals leads to a variety of privacy active behaviours such as buying from well-known major brands, seeking more information about an online counterparty before engaging with them, performing wider searches to gather more information about a subject before engaging, and avoiding purchase altogether. Unlike in our study, however, they do not check for a possibly distinct role of ambiguity nor for whether risk-handling behaviour increases in both risk perception and perceived benefit, which is an important implication of the PC model, both in the traditional and our revised formulation.

8.1.3 Applied Contribution: Preliminary Privacy Design Principles and Features

Finally, the third main contribution of this research is applied in nature in that we have provided preliminary privacy design principles to guide product development teams on how to effectively and efficiently develop privacy risk management-enhanced IS, with special emphasis on electronic postal systems. This is a significant contribution in that privatization and the influence of information and communication technologies (ICTs) are changing the way NPOs carry out their business. There has been rapid growth in postal electronic services in recent years with 85 electronic postal services having been introduced globally in 2010 alone, compared to 33 in 2007 (UN News Centre, 2013), to the point that arguably the challenge faced by NPOs now is no longer whether they should digitalize their service offerings but how best to digitalize them. An essential requirement of these systems is that they safeguard the personal information that they

transfer and store within the system. By using the RPC Model to develop the preliminary privacy design principles for e-postal systems, a theory-engrained solution for facilitating this digitalization (and for adding value by building in privacy enhancements) has been presented.

By following the (preliminary) privacy design principles and adopting the system features outlined in this thesis, other NPOs embarking on their own process of digitalisation in a manner that meets the system requirement derived from the RPC model under the given general objective, which is essentially to render online interaction as appealing as possible to as wide a portion of the population as possible. While the solutions provided in this thesis will not solve all the challenges faced by NPOs in digitalising their service offerings, it is a step in the right direction and a positive case study of one such road to digitalisation experienced by a NPO.

As explained by Gurses, Troncoso and Diaz (2011), a 'technologically enhanced' approach to informational privacy protection has three important advantages. Firstly, it does not focus solely on modifying the behaviour of those collecting personal information. Instead it explicitly recognises that there is a need to restrict what the technology can do and make it more difficult for private companies and governmental agencies to engage in unlawful or overly intrusive behaviour. The second advantage of this approach is that it is proactive and preventative, rather than reactive and punitive. As it focuses on preventing unwanted forms of collection and on limiting what companies can do and in principle, it should also reduce the number of abuses and the need for costly complaints procedures. The third advantage is that it forces both producers and users of technology to regard the collection of personal information and

the legality of doing this as inseparable, and therefore encourages them to regard privacy enhancements as a positive aspect of the technology. Our approach can be seen as having been technologically enhanced in a systematic theory-engrained way and, therefore, should offer the advantages identified by these authors in a possibly amplified and more reliable way.

It could be argued that our preliminary set of privacy design principles is similar in content to existing principles such as the Fair Information Practice (FIPs) and the principles of PbD. However, we argue that a significant difference between our set of principles and existing sets of principles is the fact that we seek to leverage user biases to help users make better (less biased) decisions. This principle alludes to the use of a gentle type of privacy nudging to be carried out for users that are prone to heuristic driven bias. This idea is gaining traction with a number of IS researchers active in the field of field of "privacy economics" (Acquisti, 2009; Balebako et al., 2011; Wang et al., 2013). In addition, previous sets of privacy principles have been critiqued in the past for being too vague (in terms of engineering specifications) to help the engineering effort needed by new software development teams when engineering informational privacy into (new) information systems (Williams, 2009; Gurses, Troncoso and Diaz, 2011; Van Lieshout et al., 2011). Van Lieshout et al (2011) argue that the use of the PbD principles to engineer privacy into ICT systems is still rather underexplored and requires substantial conceptual and empirical work to be done to ensure it is designed and engineered effectively. They warn that the implementation of the PbD principles is not easily realized (Van Lieshout et al. 2011). This is due to the fact that engineering systems with privacy in mind requires integrating privacy requirements into the typical systems engineering activities of a product development project. This requires the

elicitation and analysis of 1) the concept of privacy, 2) the functional requirements of the system being developed; and 3) the development of designs that fulfil those requirements. It also includes implementing those designs, and testing that functional and privacy requirements are fulfilled by such implementations. Our privacy principles have been designed and described so as to overcome, to the extent possible, such limitation, by providing as detailed guidance on the engineering process to IS designers and engineers as possible.

Some avenues of future research naturally flow from the RPC Model. An important step on the research agenda is to validate the Model and the Privacy Design Principles more rigorously. Validation questions include:

1. Can the RPC Model be extended for use when examining informational privacy in mobile and social networking contexts?
2. Does the RPC Model hold across cultures and nationalities (i.e., not just in an Irish sample)? Can the RPC Model be used by researchers across the entire IS community to determine the informational privacy decision-making processes of various categories of users regardless of their culture, and/or race?
3. Do the design principles effectively guide developers to produce privacy enhanced IS products in product groups other than electronic postal systems, i.e. can they be applied to other classes of systems apart from electronic postal systems? We conjectured, at the end of chapter 7, that they can but some testing is required. For example, health information is subject to specialised data protection regulations in many countries, are the privacy design principles sufficiently robust to meet these stringent requirements?

4. If the answer to the previous question is no, then can the privacy design principles be adapted to suit other disciplines such as the medical discipline?

During the course of a research study research on the periphery of the study may necessitate further investigation. For example, in this dissertation, we define privacy risk as the degree to which an individual believes that a potential for loss is associated with the release of personal information to an entity (Featherman, 2003; Malhotra, Kim and Agarwal, 2004).

8.2 Limitations and Future Research

Some avenues of future research naturally flow from the RPC Model as well as some limitations of the work undertaken as part of the research that underpins this thesis. An important next step, from this point of view, would be to validate a broader range of implications of the RPC model under a wider variety of circumstances. Validation questions include:

1. Can the RPC Model be extended for use when examining informational privacy in mobile and social networking contexts?
2. Does the RPC Model hold across cultures and nationalities (i.e., not just in an Irish sample)? Can the RPC Model be used by researchers across the entire IS community to determine the informational privacy decision-making processes of various categories of users regardless of their culture, and/or race?
3. Do the design principles effectively guide developers to produce privacy enhanced IS products in product groups other than electronic postal systems, i.e. can they be applied to other classes of systems apart from electronic postal

systems? We conjectured, at the end of chapter 7, that they can but some testing is required. For example, health information is subject to specialised data protection regulations in many countries, are the privacy design principles sufficiently robust to meet these stringent requirements?

4. If the answer to the previous question is no, then can the privacy design principles be adapted to suit other disciplines such as the medical discipline?

On a more abstract note, we observed that our definition of privacy risk is not derived from an explicit characterization of the decision maker's preferences, but rather is borrowed from the literature since preferences have not been fully specified in this dissertation, as it is common in the IS literature. It should be, in principle, possible to find a specification of preferences, e.g. a particular utility function, which implies this definition of privacy risk. Identifying such a specification would be an interesting endeavour for future research, though perhaps of greater interest in the economics than in the IS domain. Also, we used the concept of *control preference* as a proxy for risk aversion. We are, however, conscious that this might be a very context-specific proxy, which might not fully capture the individual's risk aversion. Investigating less context-specific proxies for risk aversion could also be of value for this line of research.

Though we explicitly examined the effect of three heuristic driven biases and perceived ambiguity on individuals' informational privacy decision making processes in uncertain online contexts, there are many more cognitive biases considered by the behavioural economics and psychology literature which may also help to explain the process individuals go through when deciding which information to disclose and which

informational privacy protection measures to take. For instance, Acquisti (2004) argues that individuals are affected by hyperbolic discounting; this cognitive bias is relevant in our context because there is evidence that, in online settings, individuals tend to prefer immediate gratification and discount future risks and/or costs in a manner that later leads to regret (Acquisti, 2004). In future research we will extend the RPC Model to explicitly allow for this possible bias. It is also worth noting, however, that in the context of our survey, we would not have been able to test for the effect of this bias on willingness to disclose personal information and risk handling behaviour as it requires data on situation specific behaviour that, as noted before, is not available to us.

Another worthwhile extension would be to include risk handling behaviour as an explanatory variable of willingness to disclose personal information, thereby allowing for the possibility that the choice of whether to disclose information depends on the possibility to deploy risk handling behaviour. Again, testing this effect will require situation specific data on IS users choices and behaviour that in the context of our survey is not available. So we leave this investigation to future empirical work, along the lines of Drennan et al (2006).

The can be argued, as we noted in chapter 3 of this work, that the privacy calculus approach to the concept of privacy neglects the 'absolute' value of privacy. However, this approach is not strictly inconsistent with the RPC model, as the model can be made consistent, in principle, with the view that privacy is an absolute by admitting an infinitely large privacy risk aversion. However, this approach is not in line with the spirit of the model. It entails an essentially different approach to conceptualising privacy. A worthwhile endeavour for future research would be to explore, in depth,

whether such views can be in some way reconciled and whether an appropriate extension of the RPC model may accommodate this.

It is worth emphasizing once again that all variables, except the demographic ones, measure individuals' *attitudes* as our survey questions essentially captured variation of attitudes and typical self-reported behaviour across subjects. Therefore, they cannot be used to capture variation of behaviour across circumstances (per subject or classes thereof). As already noted, Smith et al. (2011) acknowledge that this is a common limitation of empirical studies in the literature on informational privacy. We sought to partially address this by carrying out semi-structured interviews and in part by using ADR as our overarching methodological framework but we hope to continue to address this problem more directly in future research. We also hope that it will be possible, through observation of the RiposteTrEx (volunteering) users' behaviour, to collect direct data on it.

The number of responses from the questionnaire was reasonably large (420 responses out of 2,500 questionnaires). The fact that the semi-structured interviews echoed the findings of the questionnaire was also reassuring. Nonetheless, the same sample of the population was used for both the online questionnaire and the semi-structured interviews. This is a potential limitation in that effects of priming from the online questionnaire could have resulted in biased responses from the semi-structured interviews. In order to counteract any priming effects, the time between the submission of the final responses to the online questionnaire and the commencement of the semi-structured interviews was over two months in length. Nonetheless, residual priming effects cannot be rules out. Given resource and time limitations, it was impossible for us

to avoid this problem entirely and we therefore leave this task to future research. Future research could also employ a more diversified sample, drawn from a wider range of socio-economic and demographic backgrounds, so as to be representative of a wider population. From this point of view, a useful extension would be to form an International sample in that, even though the concept of privacy is present in all cultures and societies, its precise characterization shows substantial variation across cultures, due to its subjectivity (Goold, 2009).

Also, we were not allowed to participate in the focus groups which tested the effectiveness of system's functionality in regard to its ability to protect personal information. As a result of this, there was no product expert present at the focus groups. We believe this had an impact on the responses of the participants. Whenever concern about a particular functionality of the system arose during the 90 minutes of each focus group, there was no one with sufficient system expertise and knowledge to provide facts about the actual functionality of the product. This led to ambiguity about the effectiveness of the system. In the future, Escher Group plans to conduct their own round of focus groups, this time ensuring a product expert is present during the session to give details about the exact functionality of the system. As a result of the focus groups not yielding strong acceptance of the product, it was only possible to put forth a preliminary set of privacy design principles for electronic postal systems. Thus, at least one further stage (and possibly more) of validation needs to be completed before the privacy design principles can be finalised.

From an engineering point of view, the NSPD team's objective to design and develop an electronic postal system which would allow users to dynamically manage their

informational privacy settings has been achieved to an extent but further work on the system is needed. As noted by Jiang, Scheibe and Nilakanta (2011), it is generally accepted, in agile software development, that the first version of a software product often does not fully meet requirements in terms of functionality and user expectation. The feedback from the first release can be used to test feature designs and help improve marketing and customer support (Jiang, Scheibe and Nilakanta, 2011).

The development of the Personal Information Updater Tool (described in chapter 7) introduced into the RiposteTrEx system a user-centric approach to data minimization by allowing the user to consent to, and revoke consent to use personal information by interested parties. This tool, however, provides the user with a somewhat limited ability to revoke the use of their personal information once submitted, in that the interested parties receiving the user's personal information are not bound by any legal contract or obligation to refrain from passing on the user's personal information to third parties if they so wish. Research into how consent and revocation of consent to use personal information is passed onto third parties would be an interesting avenue to explore in the future.

Other research questions, which straddle theory and its engineering, worth pursuing are:

1. How feasible is it that electronic postal systems (partially) replace the physical postal system? What challenges are preventing this transformation from taking place? Are they privacy-related?
2. Is the concept of informational privacy changing? Does an individual's attitude to informational privacy change throughout their life time? Is it a generational

thing? Does privacy risk aversion change across time and circumstances, including cultures and societies?

3. Is the concept of privacy dying? Is it valued as much today as it was three decades ago?

In addition to investigating the research questions above, we are currently preparing a number of papers based on this work for publication. Five conference papers, a journal publication and 2 book chapters have so far been completed from the work described in this dissertation as well as a number of working papers. These works are briefly discussed in Appendix K of this work.

8.2.1 Implications of the Methodological Constraints within the Dissertation

As noted in chapter 5 of this dissertation, some constructs were weakly measured by the questionnaire. The constructs for cognitive biases such as availability and representativeness bias, anchoring and adjustment, and unwillingness to disclose personal information in ambiguous circumstances were particularly weakly measured. We believe that this limitation was the result of a poorly designed survey instrument. At the time that the questions for the survey instrument were being designed, the objectives and the results that we wished to gather from the survey were poorly defined. These, unfortunately, only became clear after the survey had been conducted. This resulted in an effort to extract information from results gathered by a survey instrument that had not been constructed specifically for our research questions. We view the realization (i.e. the limitations of the survey instrument) as part of the scientific and, from the point of view of the RiposteTrEx project, organizational learning achieved through the ADR

project. This is consistent with this methodology, which contains a substantial iterative element.

Planned future research, as part of a continuation of this project, is to redesign the survey to better suit our research questions, namely those implied by the objective of making inference on the revised PC model.

In addition to this, we would like to extend our research by examining how to characterize the heuristics people use to make decisions that involve sacrificing privacy, rather than just identifying biases as we have done here. Herbert Simon's work (1969) stimulated two streams of research in psychology and bounded rationality. The first stream is the heuristics and biases school of thought for which Kahneman and Tversky (1972) are known, and the other stream led to the development of the fast and frugal heuristics for which Gigerenzer and Goldstein (1996) are known. Both streams have had a significant impact on the behavioral economics discipline when examining how people form judgments and make decisions. The challenge, which we would like to address in future research, and building on the insights of these two schools of thought, is how to characterize more satisfactorily the heuristics people use to make decisions involving privacy sacrifices.

Similarly, from the survey results, the *Education* construct exerted a negative influence on the willingness to disclose personal information, suggesting either a cultural bias in relatively educated subjects towards an emphasis on privacy by, or a greater awareness of privacy risks among, the educated subjects, or both. Unfortunately, our sample did not contain enough variation in the level of education to elicit indications in this respect

and therefore, just like for the relation between ambiguity and ambiguity aversion, the survey questions would need to be redesigned and the survey re-run with more focused questions to address this problem. As noted earlier, we plan to undertake such additional research work in the near future, as part of the ongoing ADR project that was initiated as part of the research undertaken for this dissertation.

A number of other issues resulting from errors in the survey design will hopefully be resolved when the survey instrument is revised. For instance, the survey provided for limited situation specific data collection, which we intend to correct through more intensive use of focus groups and by attempting to innovatively design the survey instrument so as to allow for situation-specific data to be gathered.

Additionally, a number of individuals who volunteered to be interviewed after the survey could be seen as non–representative interviewees. For instance, one volunteer was a researcher of terrorist groups who clearly had privacy concerns as a result of his profession. Due to the small number of interviewees, 20 in total, these non-representative participants could have skewed the results somewhat. Indeed, the sample size for interviews, due to all participants being self-selected could have affected the analysis of factors influencing decision making. The main purpose of the interviews was to ascertain whether the constructs that were weakly measured by the questionnaire were in fact adequately captured by the survey instrument, i.e. availability and representativeness and anchoring and adjustment, as well as unwillingness to disclose personal information in ambiguous circumstances. The interview findings do support the conclusions of the survey analysis. In this respect the indications of the interviews are relatively clear. We, therefore, are inclined to conclude that in spite of weaknesses

in the measurement of some constructs, the overall findings support the main implications of the RPC Model.

The focus groups showed a clear distinction between age groups with respect to the intention to use the technology under investigation (RiposteTrEx). The older the participants, the more inclined they were to see a use for such a technology. The older age groups felt that submitting personal information to the government and businesses via a privacy enhanced messaging system like RiposteTrEx would bring positive benefits and convenience. However, even these groups stressed that the submission and storage of personal information to the system would need to remain optional. This points either to the difficulty of removing deep rooted perceptions of ambiguity or to the need to allow users to decide how their personal information should be used, at least until sufficient trust has built up. That is, while attempts to nudge privacy risk-adverse users towards trusting the system seem to have been somewhat effective, it remains important to build trust over time through beneficial and breach-free system-facilitated interactions.

Additionally, the majority of focus groups, even the younger participants, admitted to being more inclined to use the RiposteTrEx system described in the hypothetical scenario described during the interviews. This suggests that some

outstanding engineering problems could be resolved (i.e., if the RPC Model-derived requirements were fully engineered into the system), the model would be effective in providing guidance on how to manage informational privacy risk for users. As the system matures and new ways of building the RPC derived requirements into the system are found, another round of focus groups will be conducted to ascertain whether the system is increasingly meeting the needs of its users in addition to increasing users' trust through systematic protection of their personal information.

8.2.2 Future Related Research Projects and Collaborations

In November 2012, Liam Church, the managing director of Escher Group Plc, Gary Coyle, Head of Escher Group UK, Gus Kostakis, Head of Escher Group US and the Author were invited to meet with David Williams, the Inspector General for the United States Postal Service in his offices in Washington DC. During this meeting, we outlined and discussed the new privacy enhanced electronic postal system, RiposteTrEx, and reported our findings from both the eight focus groups conducted during the ADR project and a recently completed 12 week pilot project of RiposteTrEx that was conducted by Gary Coyle (Escher Group's Head of UK operations), in the London borough of Tower Hamlets (Moloney and Coyle, 2014), which the Inspector General found to be interesting.

Consequently, in January 2013, the research department of the USPS Office of the Inspector General (OIG) carried out a similar investigation to ascertain the level of interest among the US public for reforming the U.S postal service and introducing an electronic postal system similar to RiposteTrEx (USPS Office of the Inspector General, 2013). Their findings differed from our focus group findings for the RiposteTrEx System with regard to user acceptance of such a system among the younger population. They found that younger respondents had the most open views about what the Postal Service can and should be doing in the digital age, while older respondents appeared to be less comfortable with the Postal Service changing its traditional role (USPS Office of the Inspector General, 2013). Further investigations need to be conducted to ascertain the reasons for this diversity in attitudes between the US survey participants and the focus group participants in Ireland. It may simply be the case that, culturally, different attitudes exist in both countries but it is necessary to conduct further investigations before coming to any conclusions.

Additionally, the author has been invited, by the research department of the USPS OIG, to present the empirical findings of her research from this dissertation to a Webinar series on Trust Frameworks jointly hosted by Dr Karen Sollins from the Massachusetts Institute of Technology in Boston. The paper outlining the empirical findings is a work in progress paper, Moloney and Poti (2013). These webinars are being put together so that researchers at the OIG and MIT can more closely examine Trust and Trust Frameworks, and gain insight into their position in the overall identity/privacy landscape. The ultimate aim of the webinars is to write an academic paper on the current state of the art with respect to Trust and Trust Frameworks including technical,

business, social and regulatory aspects of each framework. The series of Webinars are taking place from July – September 2013.

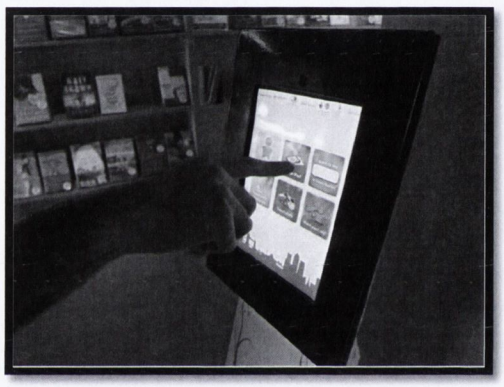
We (the Author and Escher Group) are also currently collaborating with the research department of the USPS OIG in writing a paper on the future of the postal service. The paper is entitled "*The Post Office of the Future: The New Hot Spot*" and is due to be published by the OIG later this year (2013). The paper provides suggestions on how NPOs across the globe can leverage their resources to generate profit and sustain employment in the digital age (USPS Office of the Inspector General, 2013).

8.2.3 Related R&D Prospects: Pilots and Applications of RiposteTrEx

RiposteTrEx is still considered a new software product. Development for version 2.0 of the product is on-going. However, as briefly stated previously, a live instance of RiposteTrEx 1.0 is currently being piloted by an Irish government department, the Department for Public Expenditure and Reform. Escher Group has provided the department with a website for the Irish Constitutional Convention which is currently taking place in Ireland over two years, from the beginning of 2013 until the end of 2014. The Constitutional Convention Website is a live instance of the RiposteTrEx system. Even though from the homepage (https://www.constitution.ie/) the website looks like a simple information providing website, there was a requirement for the website to facilitate the private transfer and storage of messages between participating members of the public and parliamentarians. When authenticated members log into the website, they can send private messages to each other using the RiposteTrEx system.

In September 2012, phase 1 of a proof of concept pilot project (conducted over a 12 week period) for rolling out RiposteTrEx in the borough of Tower Hamlets in central London, was set up in partnership with Tower Hamlets Council. This first phase consisted of locating 4 ruggedized iPad kiosks in three local libraries and the local mosque. The objective of this pilot, based on the needs of the citizens of Tower Hamlets according to their town council, was to encourage citizens, especially those generally excluded from digital society, to communicate digitally with their local council.

Figure 8.1 Ruggedised iPads located in 3 local libraries and in a local mosque



The preliminary results of the pilot were interesting. Over 10,000 communications occurred on the system in 12 weeks. Only 4 of these communications needed to be deleted as a result of abuse. This suggests that, when given the opportunity, citizens are interested in participating electronically with their local government.

The most encouraging finding of the pilot was that 14% of users of the kiosks had never previously been on the Internet. Another positive finding was that 45% of respondents would naturally see these kiosks as being located in their local Post Office and part of the national postal system. For more information on this pilot study see Moloney and Coyle (2014)

Over the last year, Escher Group has applied for and received membership to the European Large Scale Project (LSP) entitled *"The electronic Simple European Networked Services"* (The eSENS Project, 2013). Escher Group was the founding members of the Irish National Consortium for the eSENS project. The project was launched within the ICT Policy Support Programme (ICT PSP), under the Competitiveness and Innovation Framework Programme (CIP) of the European Commission (2007). The aim of the eSENS project is to develop an infrastructure for interoperable public services in Europe. It aims to support the creation of a Digital Single Market by facilitating the delivery and usage of electronic public services (The eSENS Project, 2013).

The reason for Escher Group entering this LSP was that we were looking for parallel markets in which to sell the RiposteTrEx system and we saw this as a chance to learn from experts in the fields of e-procurement, e-health, e-justice and digital identity. We hope that by gaining knowledge in these e-government fields and by participating in cross-border pilot studies, we can adapt RiposteTrEx for use in these fields.

8.3 Conclusion and Final Remarks

This chapter provided an overview of this dissertation and of its findings and contributions, classifying the latter as contributions on the methodological, theoretical and applied front. It then offered a discussion of the limitations of the research work undertaken and suggested possible extensions and avenues of future research. This thesis was an attempt to explore the complex concept of informational privacy and its implications for IS users in online settings. In seeking to understand how to improve

privacy risk management options for users of electronic postal systems like RiposteTrEx, and IS users more generally, we strived to allow for this complexity as much as we could, for example by formulating the privacy calculus model in a manner that explicitly allows for users' cognitive biases and for a distinct role of ambiguity as well as by following the ADR methodology to guide the development of the privacy risk management features of RiposteTrEx. The model remains, however, somewhat stylised and far from able to capture this complexity in full, even though it was largely supported by both the survey and the focus groups and proved useful in the development of the privacy-related features of RiposteTrEx. Likewise, even though the structured approach afforded by the ADR methodology greatly benefited the development of RiposteTrEx, the design and engineering of the privacy-related features of the product and of similar IS remains challenging. Much remains to be done, not least to more satisfactorily account for dimensions of privacy that pertain to the sphere of civil rights, including personal freedom and autonomy, as well as implications for society at large, including the functioning of democracy itself. Of special relevance, in this respect, is the tension between, on the one hand, the needs of the online economy and users' desire to interact online, and, on the other hand, their desire to preserve their personal privacy or, at least, the interest of society to protect it, as a prerequisite of personal freedom and autonomy for all.

9 Bibliography

ABC4Trust Project, 2009. *ABC4Trust.* [Online] Available at: http://abc4trust.de/ [Accessed 23rd March 2011]. This project is unded under the 'Information and communication technologies' (ICT) Theme of the Seventh Framework Programme (FP7).

Ackerman, M.S., Cranor, L.F. & Reagle, J., 1999. Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. In *ACM Conference on Electronic Commerce*. Colorado, 1999. Association of Computing Mchinery (ACM).

Acquisti, A., 2004. Privacy in Electronic Commerce and the Economics of Immediate Gratification. In *in Proceedings of the 5th ACM Electronic Commerce Conference*. New York, 2004. ACM Press.

Acquisti, A., 2009. Nudging privacy: The behavioral economics of personal information. *IEEE Security and Privacy*, 7(6), pp.82-85.

Acquisti, A. & Grossklags, J., 2003. Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior. In *In: Proceedings of the Second Annual Workshop Economics and Information Security (WEIS 2003).* College Park, Maryland, US, May 29-30, 2003., 2003.

Acquisti, A. & Grossklags, J., 2005. Privacy and rationality in individual decision making. *IEEE Security and Privacy*, 1, pp.26-33.

Acquisti, A. & Grossklags, J., 2005. Uncertainty, Ambiguity and Privacy. In *The 4th Annual Workshop on Economics and Information Security (WEIS 2005).* Harvard University, Cambridge, MA, USA, 2005.

Acquisti, A. & Grossklags, J., 2008. What Can Behavioral Economics Teach Us About Privacy? In *Digital Privacy: Theory, Technologies, and Practices.* Boca Raton, Florida: Auerbach Publications.

Agosta, L., 2010. *Empathy in the context of philosophy.* London; UK: Palgrave and MacMillan.

Agre, P.E. & Rotenberg, M., 1997. *Technology and Privacy: The New Landscape.* London : MIT Press.

Altman, I., 1975. *The Environment and Social Behavior.* London: Monterey, CA: Brooks/Cole.

Altman, I. & Chemers, M., 1980. *Culture and Environment.* Monteray, California: Brooks/Cole Publishing Company.

Ambrose, P.J. & Johnson, G.L., 1998. A Trust Based Model of Buying Behavior in Electronic Retailing. In *AMCIS 1998 Proceedings.*, 1998.

Anand, P., 2002. *Foundations of Rational Choice Under Risk.* 3rd ed. Oxford, UK: Oxford University Press.

Antón, A.I., Earp, J.B. & Young, J.D., 2010. How Internet Users' Privacy Concerns Have Evolved Since 2002. *IEEE Security & Privacy*, vol 8((1)), pp.pp 21 - 27.

Arendt, H., 1998. *The Human Condition, Chicago, University Press Chicago.* Chicago: University Press Chicago.

Avison, D., Baskerville, R. & Myers, M., 2001. Controlling action research projects. *Information Technology and People*, 14(1), p.28–45.

Awad, N.F. & Krishnan, M.S., 2006. The Personalisation Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalisation. *MIS Quarterly*, 30(1), pp.13-28.

Balebako, R. et al., 2011. Nudging Users Towards Privacy on Mobile Devices. In *The 2nd International Workshop on Persuasion, Influence, Nudge & Coercion through mobile devices*. Vancouver, Canada, 2011.

Barber, B., 1983. *The Logic and Limits of Trust*. New Brunswick, New Jersey: Rutgers University Press.

Barnes, S.B., 2006. A privacy paradox: Social networking in the United States. *First Monday*, 11(9).

Baskerville, R. & Myers, M.D., 2004. Special issue on action research in information systems: making IS research relevant to practice – foreword. *MIS Quarterly*, 28(3), p.329–335.

Belanger, F. & Crossler, R.E., 2011. Privacy in the Digital Age: A review of information privacy research in information systems. *MIS Quarterly*, 35, pp.1017-1036.

Belanger, F., Hiller, J.S. & Smith, W.J., 2002. Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes. *Journal of Strategic Information Systems*, 11(3/4), pp.245-70.

Bellman, S., Johnson, E.J., Kobrin, S.J. & Lohse, G.L., 2003. International Differences in Information Privacy Concerns: A Global Survey of Consumers. *The Information Society*, 20, pp.313-24.

Benbasat, I., 1984. An Analysis of Research Methodologies. In P.R.L. James I. Cash, ed. *The Information Systems Research Challenge*. Boston, MA: Harvard Business School Press.

Benbasat, I. & Zmud, R.W., 1999. Empirical research in information systems: the practice of relevance. *MIS Quarterly*, 23(1), p.3–16.

Benbasat, I. & Zmud, R.W., 2003. The Identity Crisis within the IS discipline: Defining and Communicating the Discipline's core Properties. *MIS Quarterly*, pp.183-94.

Bennett, C.J., 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*. Ithaca, NY: Cornell University.

Bennett, C.J., 2008. *The Privay Advocates: Resisting the Spread of Surveillance*. Cambridge, Massachusetts: The MIT Press.

Bernstein, R.J., 1978. *The Restructuring of Social and Political Theory*. New York, NY: Harcourt Brace Jovanovich.

Bhattacherjee, A., 2002. Individual Trust in Online Firms: Scale Development and Initial Test. *Journal of Management Information Systems*, 19(1), pp.211 - 242.

Boeije, H., 2002. A Purposeful Approach to the Constant Comparative Method in the Analysis of Qualitative Interviews. *Quality & Quantity*, 36, p.391–409.

Boneh, D. & Franklin, M., 2003. Identity-Based Encryption from the Weil Pairing. *SIAM Journal of Computing*, 32(3), pp.586-615.

Bonoma, T.V., 1985. Case Research in Marketing: Opportunities, Problems, and a Process. *Journai of Marketing Research* , 22, pp.199-208.

Boyarchenko, N., 2012. Ambiguity Shifts and the 2007

Brandimarte, L., Acquisti, A. & Loewenstein, G., 2012. Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science*, pp.1-8.

Brown, S.D. & Lightfoot, G.M., 1998. Insistent emplacement: Heidegger on the technologies of informing. *Information Technology and People*, 11, pp.290-304.

Brunt, D., 2006. Data Protection Technical Guidance Note: Privacy enhancing technologies (PETs). *Information Commissioner's Office*.

Budnitz, M., 1998. Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate. *South Carolina Law Review*, 49(1), pp.847-86.

Burkert, H., 1997. Privacy-Enhancing Technologies: Typology, Critiique, Vision. In P.E. Agre & M. Rotenberg, eds. *Technology and Privacy: The New Landscape*. Cambridge, MA: MIT Press, 125-142.

Burrell, G. & Morgan, G., 1985. *Sociological Paradigms and Organisational Analysis*. Aldershot: Gower Publishing Company Limited.

Butler, T. et al., 2008. Designing a core IT artefact for Knowledge Management Systems using participatory action research in a government and a non-government organisation. *Journal of Strategic Information Systems* , 17, p.249–267.

Camenisch, J. et al., 2011. *Future Challenges in Security and Privacy for Academia and Industry*. Lucerne, Switzerland: Springer.

Camenisch, J. & Pfitzmann, B., 2007. Federated Identity Management. In M. Petkovic & W. Jonker, eds. *Security, Privacy and Trust in Modern Data Management*. Springer Berlin Heidelberg New York.

Camerer, C.F. & Lowenstein, G., 2003. Behavioral Economics: Past Present and Future. In C. Camerer, G. Lowenstein & M. Rabin, eds. *Advances in Behavioral Economics*. Princeton, NJ: Princeton University Press. pp.3-51.

Casey, T. & Embree, L.E., 1990. *Lifeworld and Technology*. Washington, D.C, USA: University Press of America.

Cass, K., 1998. The world wide web's shadow of opportunity: a Heideggerian perspective of authenticity in the information age. *Information Technology & People*, 11, pp.326-37.

Castaneda, J.A. & Montoro, F.J., 2007. The effect of Internet general privacy concern on customer behavior. *Electronic Commerce Research*, 7, pp.117-41.

Caudill, E.M. & Murphy, P.E., 2000. Consumer Online Privacy: Legal and Ethical Issues. *Journal of Public Policy and Marketing*, 19(Spring), pp.7-19.

Cavoukian, A., 1998. *Data Mining: Staking a Claim on Your Privacy*. [Online] Available at: http://www.ipc.on.ca/images/resources/datamine.pdf [Accessed 19th April 2011].

Cavoukian, A., 2006. *Privacy by Desigh: the 7 foundational principles, Implementation and Mapping of Fair Information Practices*. [Online] Available at: http://www.ipc.on.ca/images/Resources/pbd-implement-7found-principles.pdf.

Cavoukian, A., 2010. Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the information Era. In G.O.M. Yee, ed. *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards*. Chicago, Il, USA: IGI Global. pp.170-208.

Chellappa, R.K., 2008. Customers' Trust in Electronic Commerce Transactions: The Role of Perceived Privacy and Perceived Security. *unpublished paper*.

Chellappa, R.K. & Sin, R.G., 2005. Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology & Management*, 6(2), pp.181-202.

Church, L. & Moloney, M., 2011. Providing Public Services Through Digital Postal Networks: A Position Paper. In *11th European Conference on eGovernment – ECEG 2011*. Ljubljana, Slovenia, 2011.

Church, L. & Moloney, M., 2012. Public Value Provision: A Design Theory for Public e-Services. In *Annual Services Research and Innovation Institute Global Conference*. San Jose, California, USA, 2012. Services Research and Innovation Institute and IEEE.

Church, C. & Moloney, M., 2013. Design Principles for Public Service Provision in Information and Communication Technologies. In B.J. Kelvin, ed. *Technology Development and Platform Enhancements for Successful Global E-Government Design*. IGI GLobal.

Church, L., Moloney, M. & Bannister, F., 2013. The Sealed Letter: Safeguarding the Public System of Privacy Protection in a Digital World. In *The 46th Hawaii International Conference on System Sciences*. Manoa, Hawaii, 2013.

Cohen, J.E., 2001. Privacy, Ideology, and Technology: A Response to Jeffrey Rosen. *Georgetown Law Journal*, 89.

Cook, T. & Campbell, D., 1979. *Quasi-Experimental Design*. Chicago, US: Rand McNally.

Corritore, C.L., Kracher, B. & Wiedenbeck, S., 2003. On-line Trust: Concepts, Evolving Themes, a Model. *International Journal of Human-Computer Studies*, 58(6), pp.737 - 758.

Costello, G., Conboy, K. & Donnellan, B., 2011. Dialogical Action Research as Engaged Scholarship: An Empirical Study. In *The Thirty Second International Conference on Information SYstems*. Shanghai, China, 2011. Association for Information Systems.

Covello, V.T., 1992. Trust and Credibility in Risk Communication. *Health Environment Digest*, 6(1), pp.1-4.

Cross, N., 2001. Keynote speech: Design/Science/Research: Developing a Discipline. In *5th Asian Design Conference*. Seoul, Korea, 2001.

Crotty, M., 2003. *The Foundations of Social Research: Meaning and Perspective in the Research Process*. London: Sage Publications.

Culnan, M.J., 1993. How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. *MIS Quarterly*, 17, pp. 341-363.

Culnan, M.J..a.B.J.R., 2003. Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social Issues*, 59(2), pp.323-42.

Dasgupta, P., 1988. Trust as a Commodity. In D. Gambetta, ed. *Trust: Making and Breaking Cooperative Relations*. New York: Basil Blackwell Ltd.

Davis, F., 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), pp.319-39.

Davis, M., 2010. *Towards a Political Economy of the Internet*. [Online] Available at: http://vimeo.com/channels/129520 [Accessed 6 May 2011].

Decew, J.W., 1997. *In Pursuit of Privacy: Law, Ethics and the Rise of Technology*. New York: Cornell University Press.

DePaolo, B.M., C. Wetzel, W.S. & Wilson, M.J.W., 2003. Verbal and Nonverbal Dynamic of Privacy, Secrecy and Deceit. *The Journal of Social Issues*, 59, pp.391-410.

Deutsch, M., 1962. Cooperation and Trust: Some Theoretical Notes. In M.R. Jones, ed. *Nebraska Symposium on Motivation*. Lincoln, Nebraska: University of Nebraska Press.

DeVault, M., 1999. *Liberating method: Feminism and social research*. Philadelphia, USA: Temple University Press.

Dhillon, G.S. & Moores, T.T., 2001. Internet Privacy: Interpreting Key Issues. *Information Resources Management Journal*, 14, pp.33-37.

Dillman, D.A., 2000. *Mail and Internet Surveys: The Tailored Design Method*. New York, NY: John Wiley and Sons.

Dineva, T. & Hart, P., 2004. Internet privacy concerns and their antecedents - measurement validity and a regression model. *Behaviour & Information Technology*, Volume 23(Issue 6), pp.pages 413 - 422.

Dinev, T. et al., 2006. Privacy Calculus Model in E-Commerce: A Study of Italy and the United States. *European Journal of Information Systems*, 15(4), pp.389-402.

Dinev, T., Hart, P. & Mullen, M.R., 2008. Internet privacy concerns and beliefs about government surveillance – An empirical investigation. *Journal of Strategic Information Systems*, 17, p. 214–233.

Dommeyer, C.J. & Gross, B.L., 2003. What Consumer Know and What They Do: An Investigation of Consumer Knowledge, Awareness, and Use of Privacy Protection Strategies. *Journal of Interactive Marketing*, 17, pp.34-51.

Douglas, M., 2003. *Risk and Blame: Essays in cultural theory*. London: Taylor & Francis e-Library.

Drennan, J., Mort, G.S. & Previte, J., 2006. Privacy, Risk Perception, and Expert Online Behavior: An Exploratory Study of Household End Users. *Journal of Organisational and End User Computing*, 18(1), pp.1-22.

Earp, J.B., Antón, A.I., Aiman-Smith, L. & Stufflebeam, W., 2005. Examining internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management*, Vol 52((2)), pp.pp. 227-237.

Egelman, S., Tsai, L., Cranor, L.F. & Acquisti., A., 2009. Timing is everything?: the effects of timing and placement of online privacy indicators. In *Proceedings of the 27th international conference on Human factors in computing systems, CHI '09*. NY, USA, 2009.

Epley, N., 2004. A tale of Tuned Decks? Anchoring as adjustment and anchoring as activation. In *The Blackwell handbook of judgment and decision making*. Oxford, England: Blackwell Publishers. p.240–256.

Epley, N. & Gilovich, T., 2005. The Anchoring-and-Adjustment Heuristic. *Psychological Science*, 17(4), pp.311-18.

Erbas, N. & Mirakhor, A., 2007. The Equity Premium Puzzle, Anbiguity Aversion, and Institutional Quality. *IMF Working Paper: work in progress, Washington DC: International Monetary Fund.*

Escher Group, 2013. *Riposte - Rock solid messaging*. [Online] Available at: http://www.eschergroup.com/riposte/ [Accessed 11 June 2013].

Escher Group, 2013. *RiposteTrEx™ - A revolutionary communication and transaction platform*. [Online] Available at: http://www.eschergroup.com/digital_postbox/ [Accessed June 2013].

European Commission, 1995. DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. *The Official Journal of the European Communities*, 281(23), pp.P. 31 - 50.

European Commission, 2002. DIRECTIVE 2002/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. *Official Journal of the European Communities*, 201(37), Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0037:EN:PDF.

European Commission, 2009. Directive 2009/136/EC of the European Parliament and of the Council. *Official Journal of the European Union*, p.20. Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF [Accessed 29 April 2013].

European Commission, 2010. *A Digital Agenda for Europe (COM(2010) 245 final/2)*. [Online] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=com:2010:0245:fin:en:pdf [Accessed 30th April 2011].

Fay, B., 1987. An Alternative View: Interpretive Social Science. In M.T. Gibbons, ed. *Interpreting Politics*. New York, NY: University Press.

Featherman, M..a.P.P., 2003. Predicting E-Services Adoption: A Perceived Risk Ffacets Perspective. *International Journal of Human-Computer Studies*, 59, pp.51-474.

Federal Trade Commission, 2010. *Protecting Consumer Privay in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*. [Online] Available at: http://ftc.gov/os/2010/12/101201privacyreport.pdf [Accessed 13 May 2011].

Fishbein, M. & Ajzen, I., 1975. *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley.

Floridi, L., 2005. The Ontological Interpretation of Informational Privacy. *Ethics and Information Technology*, Vol. 7((4)), pp.pp. 1-16.

Foddy, W., 1994. *Constructing Questions for Interviews and Questionnaires*. Cambridge, UK : Cambridge University Press.

Forrester Research, 2010. *North American Technographics® Benchmark Survey, Q2 2010 (US, Canada)*. [Online] Available at: http://www.forrester.com/North+American+Technographics+Benchmark+Survey+Q2+2010+US+Canada/-/E-SUS787 [Accessed 14 April 2012].

Fried, C., 1968. Privacy [a moral analysis]. In Schoeman, F.D. *Philosophical Dimensions of Privacy: An Anthology*. New York: Cambridge University Press. pp.333-45.

Fried, C., 1990. Privacy: A Rational Context. In M.D. Erman, M.B. Williams & C. Guitierrez, eds. *Computers, Ethics & Society*. New York: Oxford University Press.

Galliers, R.D. & Land, F.F., 1988. The Importance of Laboratory Experimentation in IS Research. *Communications of the ACM*, 31(12), pp.1504 - 1505.

Gambetta, D., 1988. *Trust: Making and Breaking Cooperative Relations*. New York: Basil Blackwell ltd.

Gavison, R., 1980. Privacy and the Limits of Law. *Yale Law Journal*, 89, pp.421-71.

Gefen, D., 2000. E-Commerce: The role of familiarity and trust. *The International Journal of Management Science*, 28(6), p.725–737.

Gellman, R., 2012. *FAIR INFORMATION PRACTICES: A Basic History*. [Online] Available at: http://bobgellman.com/rg-docs/rg-FIPShistory.pdf [Accessed 6 Noverber 2012].

George, J.F., 2002. Influences on the Intent To Make Internet Purchases. *Internet Research: Electronic Networking Applications and Policy*, 12, pp.165-80.

George, J.F., 2004. The Theory of Planned Behavior and Internet Purchasing. *Internet Research: Electronic Networking Applications and Policy*, 14, pp.198-212.

Ghauri, P. & Gronhaug, D.K., 2010. *Research Methods in Business Studies*. New Zealand: Prentics Hall.

Ghirardato, P. & Marinacci, M., 2001. Risk, ambiguity, and the separation of utility and beliefs. *International Centre for Economic Research Working Papers*, Applied Mathematics Series.

Gibbons, M.T., 1987. Introduction: the Politics of Interpretation. In M.T. Gibbons, ed. *Interpreting Politics*. New York: New York: University Press.

Gilovich, T., Griffin, D. & Kahneman, D., 2002. *Heuristics and Biases: The Psychology of Intuitive Judgement*. Cambridge, UK: Cambridge University Press.

Glaser, B.G., 1965. The Constant Comparative Method of Qualitative Analysis. *Social Problems*, 12(4), pp.436-45.

Glaser, B.G. & Strauss, A.L., 1967. *The Discovery of Grounded Theory*. Chicago, USA: Aldine Publishers.

Good, N.S., Grossklags, J., Mulligan, D.K. & Konstan, J.A., 2007. Noticing Notice: A Large-Scale Experiment on the Timing of Software License Agreements. In *in Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI 2007)*. San Jose, California, USA, 2007.

Good, N. et al., 2006. User Choices and Regret: Understanding Users' Decision Process about Consensually Acquired Spyware. *A Journal of Law and Policy*, 2(2), pp.283-44.

Goold, B.J., 2009. Building it in: the role of privacy enhancing technologies (PETs) in the regulation of surveillance and data collection. In Goold, B.J. & Neyland, D. *New Directions in Surveillance and Privacy*. Cullompton, Devon, UK: Wilan Publishing. pp.18-38.

Greenberger, B.D. & Strasser, S., 1986. Development and Application of a Model of Personal Control in Organizations. *Academy of Management Review*, 11(1), pp.pp 164-177.

Greenspan, A., 2002. *The History of Money: Remarks by Chairman Alan Greenspan*. [Online] Available at: The Federal Reserve Board. Retrieved from: http://www.federalreserve.gov/boarddocs/speeches/2002/200201163/default.htm [Accessed 28th February 2008].

Gross, R. & Acquisti, A., 2005. Information Revelation and Privacy in Online Social Networks. In *In Workshop on Privacy in the Electronic Society (WPES)*. Alexandria, VA, USA, 2005.

Guiso, L., Sapienza, P. & Zingales, L., 2007. Trusting the Stock Market. *ECGI - Finance Working Paper No. 170/2007 Available at SSRN: http://ssrn.com/abstract=811545*.

Gurses, S., Rizk, R. & Gunther, O., 2010. Sns and 3rd party application privacy policies and their contruction of privacy concerns. In *In the proceedings of the European Conference on Information Systems*. Pretoria, South Africa, 2010.

Gurses, S., Troncoso, C. & Diaz, C., 2011. Engineering Privacy by Design. *In the proceedings of the Computers, Privacy and Data Protection Conference*, pp.Brussels, Belgium.

Hann, I.H., Hui, K.L. & Lee, S.Y.T., 2008. Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach. *Journal of Management Information Systems*, 24(2), pp.13-42.

Harding, J., 2013. *Qualitative Data Analysis from Start to Finish*. London, UK: Sage Publishers.

Harrell, M.C. & Bradley, M.A., 2009. *Data Collection Methods Semi-Structured Interviews and Focus Groups*. [Online] Available at: http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR718.pdf [Accessed 6th April 2013].

Harris Interactive, 1999. IBM Multi-National Consumer Privacy Survey [online]. *Report by Harris Interactive Inc for Privacy & American Business*, 17(Hackensack, New Jersey).

Harris Interactive, 2002. *Privacy On and Off the Internet: What Consumers Want*. Hackensack, New Jersey: Privacy & American Business.

Hart, K., 1988. Kinship, Contract, and Trust: The Economic Organisation of Migrants in an African City Slum. In D. Gambetta, ed. *Trust: Making and Breaking Cooperative Relations*. New York: Basil Blackwell Ltf.

Herold, R., 2002. European Union (EU) Data Protection Directive of 1995: Frequently Asked Questions. *Computer Security Institute (www.gocsi.com)*.

Hevner, A. & Chatterjee, S., 2010. *Design Research in Information Systems*. Integrated Series in Information Systems ed. New York: Springer.

Hevner, A.R., March, S.T. & Park, J., 2004. Design Science in Information Systems Research. *MIS Quarterly*, Vol. 28((1)), pp. pp. 75-105.

Hirschheim, R. & Klein, H., 2003. Crisis in the IS field? A critical reflection on the state of the discipline. *Journal of the Association for Information Systems*, Vol. 4((1)), pp.pp. 237-293.

Hoffman, D.L., Novak, T.P. & Schlosser, A., 2000. The Evolution of the Digital Divide: How Gaps in Internet Access May Impact Electronic Commerce. *Journal of Computer-Mediated Communication*, 5(3).

Holt, J.C., 1973. *Magna Carta*. Cambridge, UK: Cambridge University Press.

Horne, D.A. & Horne, D.R., 2002. Database Marketing: When Does Good Practice Become an Invasion of Privacy? In K. Evans & L. Scheer, eds. *Marketing Theory and Applications*. Chicago: American Marketing Association. pp.480-86.

Hui, K.L., Teo, H.H. & Lee, S.Y., 2007. The Value of Privacy Assurance: An Exploratory Field Experiment. *MIS Quarterly*, 31, pp.19-33.

Hull, G., Lipford, H.R. & Latulipe, C., 2011. Contextual gaps: Privacy issues on facebook. *Ethics and Information Technology*, 13(4), pp.289-302.

Idhe, D., 1990. *Technology and the lifeworld: from garden to earth*. Indiana University Press.

IETF RFC 3161, 2001. *IETF RFC 3161 Time-Stamp Protocol (TSP)*. [Online] Available at: http://www.digistamp.com/technical/references/ietf-rfc-3161-time-stamp-protocol-tsp/?q=1 [Accessed 12 November 2012].

Introna, L.D., 1997. Privacy and the Consumer: Why we need privacy in the information society. *Metaphilosophy*, 28(3), pp.259-75.

Jarvenpaa, S.L. & Leidner, D.E., 1999. Communication and Trust in Global Virtual Teams. *Organization Science* , 10(6), pp.791-815.

Jarvenpaa, S.L. & Tiller, E.M., 1999. Integrating Market, Technology, and Policy Opportunities in E-Business Strategy. *Journal of Strategic Information Systems* , 8(3), pp.235-49.

Jarvenpaa, S.L., Tractinsky, J. & Vitale, M., 2000. Consumer trust in an Internet store. *Journal of Information Technology and Management*, 1(1/2), pp.45-71.

Jiang, Z., Scheibe, K.P. & Nilakanta, S., 2011. The economic impact of public beta testing: the power of word-of-mouth. In *Thirty Second International Conference on Information Systems*. Shanghai, China , 2011.

Joe, V.C., 1971. Review of the Internal-External Control Construct as a Personality Variable. *Psychological Reports*, 26, pp.619-40.

Johnson, C.A., 1974. Privacy as Personal Control. In *Man-Environment Interactions: Evaluations and Applications: Part 2*. Washington, DC: Environmental Design Research Association.

Johnston, C., 2012. *Google paying users to track 100% of their Web usage via little black box*. [Online] Available at: http://arstechnica.com/gadgets/2012/02/google-paying-users-to-track-100-of-their-web-usage-via-little-black-box/ [Accessed 1 May 2012].

Jones, B.D., 1999. Bounded Rationality. *Annual Review of Political Science*, 2, pp.297-321.

Jones, D. & Gregor, S., 2007. The Anatomy of a Design Theory. *Journal of the Association for Information Systems*, Vol 8((5)).

Kahneman, D. & Tversky, A., 1972. Subjective probability: A judgment of representativeness. *Cognitive Psychology*, 3, pp.430-54.

Kahneman, D. & Tversky, A., 1979. Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, 48, pp.263-91.

Kahneman, D. & Tversky, A., 1982. The simulation heuristic. In *Judgment under uncertainty: Heuristics and biases*. Cambridge, UK: Cambridge University Press. pp.201-10.

Kaplan, B. & Duchon, D., 1988. Combining qualitative and quantitative methods in information systems research: a case study. *MIS Quarterly*, 12, p.571–586.

Kling, R. & Scacchi, W., 1982. The Web of Computing: Computer Technology as Social Qrganization. In M.G. Yovitis, ed. *Advances in Computers*. New York, NY: Academic Press.

Klopfer, P.H. & Rubenstein, D.I., 1977. The Concept Privacy and Its Biological Basis. *Journal of Social Issues* , 33(3), pp.52-65.

Knight, F.H., 1921. *Risk, Uncertainty, and Profit*. Boston, MA: Hart, Schaffner & Marx; Houghton Mifflin Company.

Kuner, C., 2007. *European Data Protection Law: Corporate Compliance and Regulation*. 2nd ed. Oxford, UK: Oxford University Press.

Kuneva, M., 2009. *Online Data Collection, Targeting and Profiling (Kepnote Speech)*. [Online] Available at: http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm [Accessed 2 Oct 2009].

Kvale, S., 1996. *InterViews: an introduction to qualitative research interviewing*. Thousand Okas, CA, USA: Sage Publications.

Langer, E.J., 1975. The Illusion of Control. *Journal of Personality and Social Psychology*, 32, pp.pp 311-328.

Laufer, R.S. & Wolfe, M., 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journa of Social Studies*, Volume 33(Issue 3), pp.pages 22-42.

Lee, A.S., 2004. Thinking about Social Theory and Philosophy for Information Systems. In J. Mingers & L. Wilcocks, eds. *Social Theory and Philosophy for Information Systems*. London: John Wiley & Sons.

Leedy, P.D. & Ormrod, J.E., 2005. *Practical Research: Planning and Design*. Upper Saddle River, New Jersey: Pearson Merrill Prentice Hall.

Lee, M.k.O. & Turban, E., 2001. A Trust Model for Consumer Internet Shopping. *International Journal of Electronic Commerce*, 6(1), pp.75-91.

Lefcourt, H.M., 1972. Recent Developments in the Study of Locus of Control. In B.A. Maher, ed. *Progress in Experimental Personality Research*. New York: Academic Press.

Lessig, L., 2000. Code is Law: On Liberty in Cyberspace. *Harvard Magazine*, pp.Available at: http://harvardmagazine.com/2000/01/code-is-law-html.

Levenson, H., 1973. Multidimensional Locus of Control in Psychiatric Patients. *Journal of Consulting and Clinical Psychology*, 41, pp.397-404.

Levenson, H., 1974. Activism and powerful others: distinctions within the concept of internal-external control. *Journal of Personality Assessment*, 38, pp.377- 383.

Levy, S., 2001. *Crypto: Secrecy and Privacy in the New Code War*. London: Penguin Books.

Lewin, K., 1946. Action research and minority problems. *Journal of Social Issues*, 2, pp.34-46.

Lieberman, J.K., 1981. *The Litigious Society*. New York: Basic Books.

LI, X. & Keshelashvili, A., 2006. Perceived Benefit and Threat in Internet Use. In *56th Annual Conference of the International Communication Association*. Dresden, Germany, 2006.

Lilly, P., 2013. From 2008 to 2010, Google's Street View team collected personal data without consent. *Maximum PC*.

Lindlof, T.R. & Taylor, B.C., 2002. *Qualitative Communication Research Methods, 2nd Edition.*. 2nd ed. Thousand Oaks, CA: Sage.

Liu, C., Marchewka, J.T., Lu, J. & Yu, C.-S., 2005. Beyond Concern - A Privacy-Trust-Behavioral Intention Model of Electronic Commerce. *Information & Management*, 40, pp.289-304.

Locke, J., 2007. *Locke's Second Treatise of Civil Government*. [Online] Available at: http://www.sparknotes.com/philosophy/locke/ [Accessed 26th June 2007].

Loewenstein, G.F. & Haisley, E.C., 2008. The Foundations of Positive and Normative Economics. In Mackay, W. *chapter 9: The Economist as Therapist: Methodological Ramifications of 'Light' Paternalism*. Oxford, UK: Oxford University Press.

London Economics, 2010. Study on the Economic Benefits of Privacy-Enhancing Technologies (PETs). *Report prepared for The European Commission DGJustice, Freedom and Security*.

Luhmann, N., 1988. Familiarity, Confidence, Trust: Problems and Alternatives. In Gambetta, D. *Trust: Making and Breaking Cooperative Relations*. New York: Basil Blackwell ltd.

Lu, Y., Tan, B. & Hui, K.L., 2004. Inducing Customers to disclose personal information to internet businesses with social adjustment benefits. In *Proceedings of the 25th International Conference on Information Systems*. Washington, DC, 2004.

Lyytinen, K., 1987. Different Perspectives on Information Systems: Problems and Solutions. *ACM Computing Surveys*, 19, pp.5-46.

MacCarthaigh, M., 2012. Review of Developments, Structure and Management in the Public Sector 2012 Political change (State agencies and state enterprises). *The Journal of the Institute of Public Administration of Ireland*, 60(4).

Machlis, G.E. & Rosa, E.A., 1990. Desired risk: Broadening the social amplification of risk framework. *Risk Analysis*, 10(1), pp.161-67.

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(4), pp.336-55.

March, S.T. & Smith, G.F., 1995. Design and natural science research on information technology. *Decision Support Systems*, Vol. 15, pp.pp. 251-266.

Margulis, S.T., 2003. On the Status and Contribution of Westin's and Altman's Theories of Privacy. *The Journal of Social Issues*, 59, pp. 411-429.

Markowitz, H., 1952. Portfolio Selection. *The Journal of Finance*, 7(1), pp.77-91.

Markus, M.L., Majchrzak, A. & Gasser, L., 2002. A Design Theory for Systems That Support Emergent Knowledge Processes. *Management of Information Systems Quarterly*, 26(3), pp.179-212.

Marrow, A.F., 1969. *The Practical Theorist: The Life and Work of Kurt Lewin*. New York: Basic Books, Inc.

Marshall, C. & Gretchen, R.B., 1999. *Designing Qualitative Research*. 3rd ed. London, UK: Sage Publications.

Mårtensson, P. & Lee, A.S., 2004. Dialogical Action Research At Omega Corporation. *MIS Quarterly*, 28(3), pp.507-36.

Mathiassen, L. & Nielsen, P.A., 2008. Engaged Scholarship in IS Research. *Scandinavian Journal of Information Systems*, 20(2), pp.1-18.

Mayer, R.C., Davis, J.D. & Schoorman, F.D., 1995. An Integrative Model of Organisational Trust. *Academy of Management Review*, 20(3), pp.709-34.

Maynard, M., 1994. Methods, Practice and Epistemology: The debate about feminism and research. In M. Maynard & J. Purvis, eds. *Researching Women's Lives from a Feminist Perspective*. London: Taylor and Francis.

McKnight, D.H. & Chervany, N.L., 2001. What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology. *International Journal of Electronic Commerce*, 6(2), pp.35-59.

McKnight, D.H., Choudhury, V. & Kacmar, C., 2002. Developing and Validating Trust Measures for E-Commerce: An Integrative Typology. *Information Systems Research*, 13(3), pp.334-59.

META Group, 2005. Privacy enhancing technologies. *Report v. 1.1*, Available at: http://www.itst.dk/sikkerhed/privacy/filer/privacy-og-privacy-forum/Privacy%20Enhancing%20Technologies.pdf [Accessed 18 September 2010].

Milberg, S.J., Burke, S.J., Smith, H.J. & Kallman, E.A., 1995. Values, personal information privacy, and regulatory approaches. *Communications of the ACM* , 38(12).

Milberg, S.J., Smith, H.J. & Burke, S.J., 2000. Information Privacy: Corporate Management and National Regulation. *Organization Science*, 11, pp.35-57.

Miller, A.R., 1971. *The Assault on Privacy: Computers, Data Banks, and Dossiers*. Ann Arbor: University of Michigan Press.

Milne, G.R. & Boza, M.E., 1999. Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices. *Journal of Interactive Marketing*, 13(1), pp.5-24.

Milne, G. & Culnan, M., 2004. Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices. *Journal of Interactive Marketing*, 18(3), pp.15-29.

Milne, G.R. & Gordon, E.M., 1993. Direct Mail Privacy-Efficiency Trade-Offs Within an Implied Social Contract Framework. *Journal of Public Policy and Marketing* , 12(2), pp.206-15.

Milne, G.R. & Rohm, A., 2000. Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-in and Opt-out Alternatives. *Journal of Public Policy and Marketing* , 19(2), pp.238-49.

Mishra, A.K., 1996. Organizational Responses to Crisis: The Centrality of Trust. In T.R. Tyler & R.M. Kramer, eds. *Trust In Organizations*. Newbury Park: Sage.

Mi-token.com, 2012. *Token independence*. [Online] Available at: http://mi-token.com/ [Accessed 12 November 2012].

Moloney, M. & Church, L., 2012. Engaged Scholarship: Action Design Research for New Software Product Development. *International Conference in Information Systems, 2012*, pp.Orlando, FL, USA.

Moloney, M. & Church, L., 2012. Informational Privacy Preservation through Universal Service Obligations. *Journal of Internet Technology and Secured Systems*, 1(1/2).

Moloney, M. & Coyle, G., 2014. Next Gen e-Government: How Do We Reconcile Data Protection and Government 2.0? In *Emerging Mobile and Web 2.0 Technologies for Connected E-Government*. IGI Global.

Moloney, M. & Poti, V., 2013. A Behavioural Perspective on the Privacy Calculus Model. *Escher Group Working Paer Series*, (available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2310535).

Mongin, P., 1997. Expected Utility Theory. In W.H. J.Davis & U. Maki, eds. *Handbook of Economic Methodology*. London: Edward Elgar Publishers.

Moor, J.H., 1997. Towards a theory of privacy in the information age. *ACM SIGCAS Computers and Society*, 27, pp.27-32.

Moores, T., 2005. Do consumers understand the role of privacy seals in e-commerce? *Communications of the ACM - The disappearing computer*, 48 (3), pp.86-91.

Morgan, G., 1983. *Beyond Method*. Beverly Hills, California: Sage Publications.

Motulsky, H., 1995. *Intuitive Biostatistics*. Oxford, uk: Oxford University Press.

Muth, J.F., 1961. Rational Expectations and the Theory of Price Movements. *Econometrica*, 29(3), pp.315-35.

Myers, M.D., 1999. Investigating Information Systems with Ethnographic Research. *Communications of the Association for Information Systems*, 2(23).

National Institute of Standards and Technology , 2001. *FIPS PUB 140-2*. [Online] Available at: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf [Accessed 12th November 2012].

Needham, R. & Maybury, R., 2001. Access Control. In R.J. Anderson, ed. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Indianapolis, Indiana: Wiley Publishing Inc. pp.51-71.

Newsom, J.T., 2011. *Levels of Measurement and Choosing the Correct Statistical Test*. [Online] Available at: http://www.upa.pdx.edu/IOA/newsom/da1/ho_levels.pdf [Accessed 2011].

Nielsen, J., 1993. *Usability Engineering.*. Boston, US: Academic Press.

Norberg, P.A. & Horne, D.R., 2007. Privacy Attitudes and Privacy-Related Behavior. *Psychology and Marketing*, 24(10), pp. 829-847.

Norberg, P.A., Horne, D.R. & Horne, D.A., 2007. The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors. *The Journal of Consumer Affairs*, 41(1), pp.100-26.

O'Neil, D., 2000. Analysis of Internet Users' Level of Online Privacy Concerns. *Ph.D. in Public Policy*, Georgia Institute of Technology.

OECD, 1980. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. p.Available at: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

Orlikowski, W. & Baroudi, J.J., 1991. Studying Information Technology in Organisations: Research Approaches and Assumptions. *Working Paper Series STERN IS-90-4.*, Centre for Research on Information Systems, Leonard N. Stern School of Business, New York University., p.New York.

Orlikowski, W.J. & Iacono, C.S., 2001. Research commentary: Desperately seeking the "IT" in IT research - A call to theorizing the IT artifact. *Information Systems Research*, Vol. 12((2)), pp.pp. 121-134.

Parent, W.A., 1983. A New definition of Privacy for the Law. *Law and Philosophy*, 2, pp.305-38.

Parr, B., 2010. *Google Settles Buzz Privacy Lawsuit for $8.5 Million.* [Online] Available at: http://mashable.com/2010/09/03/google-buzz-lawsuit-settlement/ [Accessed 7th October 2010].

Pavlou, P., 2003. Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, 7(3), p.69–103.

Pavlou, P.A., 2011. State of the Information Privacy Literature: Where are we now and Where should we go? *MIS Quarterly*, 35(4), pp.977-88.

Pavlou, P.A. & Gefen, D., 2004. Building Effective Online Marketplaces with Institution-Based Trust. *Information Systems Research*, 15(1), pp.37-59.

Pearl, J., 1983. *Heuristics: Intelligent Search Strategies for Computer Problem Solving.* New York : Addison-Wesley.

Persky, S., Kaphingst, K.A., Condit, C.M. & McBride, C.M., 2007. Assessing hypothetical scenario methodology in genetic susceptibility testing analog studies: a quantitative review. *Genetics IN Medicine*, 9(11), p.727–738.

Peters, R.G., Covello, V.T. & McCallum, D.B., 1997. The Determinants of Trust and Credibility in Environmental Risk Communication: An Empirical Study. *Risk Analysis*, 17(1), pp.43-54.

Peter, J.P. & Tarpey, L.Z.S., 1975. A Comparative Analysis of Three Consumer Decision Strategies. *Journal of Consumer Research*, 2, pp.29-37.

Phelps, J., Nowak, G. & Ferrell, E., 2000. Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, 19, pp.27-42.

PICOS, 2007. *Privacy and Identity Management for Community Services.* [Online] Available at: http://www.picos-project.eu/ [Accessed 23 March 2011]. PICOS receives research funding from the 7th Research Framework Programm (FP7) of the EU as part of the Trust & Security Programme.

Pidgeon, N., 1992. Risk Perception. In T.R. Society, ed. *Risk: Analysis, Perception and Management : Report of a Royal Society Study Group.* London: The Royal Society.

Pidgeon, N., 1998. Risk assessment, risk values and the social science programme: why we do need risk perception research. *Reliability Engineering and System Safety*, 59, pp.5-15.

Posner, R.A., 1978. An Economic Theory of Privacy. *AEI Journal on Government and Society*, pp.19-26.

Preston, J., 2004. Judge Strikes Down Section of Patriot Act Allowing Secret Subpoenas of Internet Data. *The New York Times, Technology Section*, 30.

Primelife, 2008. *Primelife*. [Online] Available at: http://www.primelife.eu/ [Accessed 23 March 2011]. The PrimeLife project receives research funding from the European Union's 7th Framework Programme.

Privacy and American Business, 2005. *New survey reports an increase in ID theft and decrease in consumer confidence*. [Online] Available at: http://www.pandab.org/deloitteidsurveypr.html [Accessed 11 November 2009].

Privacy Rights Clearinghouse, 2005. *Chronology of Data Breaches Security Breaches 2005-Present*. [Online] Available at: http://www.privacyrights.org/data-breach/new [Accessed 26 January 2011].

Rachels, J., 1975. Why Privacy Is Important. *Philosophy and Public Affairs*, 4, pp.323-33.

Rapley, T., 2004. Interviews. In Seale, C., Gobo, G., Gubrium, J. & Silverman, D. *Qualitative research practice*. Thousand Oaks, CA.: Sage Publications.

Remenyi, D., Williams, B., Money, A. & Swartz, E., 2000. *Doing Research in Business and Management: An Introduction to Process and Method*. London, UK : SAGE Publications.

Renn, O., 1998. Three Decades of Risk Research Accomplishments and New Challenges. *Journal of Risk Research* , 1(1), p. 49–71.

Renn, O., 2005. Risk perception and communication: Lessons for the Food and Food Packaging Industry. *Food Additives and Contaminants*, 22(10), pp.1061-71.

Renn, O. et al., 1992. The social amplification of risk: Theoretical foundations and empirical applications. *Journal of Social Issues*, 48(4), pp.137-60.

Rothwell, W., Sullivan, R. & McLean, G., 1995. *Practicing Organization Development: A Guide for Consultants*. San Francisco, CA.: Jossey-Bass Pfeiffer.

Rotter, J.B., 1954. *Social Learning and Clinical Psychology*. New York: Prentice Hall.

Rotter, J.B., 1966. Generalized expectancies for internal versus external control of reinforcements. *Psychological Monographs*, 80, pp.1-28.

Rotter, J.B., 1967. A New Scale for the Measurement of Interpersonal Trust. *Journal of Personality*, 35(4), pp.651-65.

Rule, J.B., 2007. *Privacy in Peril*. Oxford: Oxford University Press.

Rule, J.B., 2009. The Limits of Privacy Protection. In B.J. Goold & D. Neyland, eds. *New Directions in Surveillance and Privacy*. Cullompton, Devon: Wilan Publishing.

Sapford, R., 2007. *Survey Research*. London: Sage Publications Ltd.

Saunders, M., Lewis, P. & Thornhill, A., 2007. *Research Methods for Business Students*. Harlow, UK: Pitman Publishing.

Sein, M.K., Henfridsson, O., Purao, S. & Rossi, M., 2011. Action Design Research. *MIS Quarterly*, 35(1), pp.37-56.

Shankar, V., Urban, G.L. & Sultan, F., 2002. Online Trust: A Stakeholder Perspective, concepts, implications and Future Directions. *Journal of Strategic Information Systems*, 11, pp.325-44.

Shankar, V., Urban, G.L. & Sultan, F., 2002. Online Trust: A Stakeholder Perspective, concepts, implications and Future Directions. *Journal of Strategic Information Systems*, 11, pp.325-44.

Sheedy, C. & Moloney, M., 2013. Leveraging the Postal Infrastructure for the Authentication of Individuals towards an Online Service Provision. In *21st Conference on Postal and Delivery Economics 2013*. Dublin, Ireland, 2013.

Sheehan, K.B., 1999. An Investigation of Gender Differences in On-Line Privacy Concerns and Resultant Behaviors. *Journal of Interactive Marketing*, 13, pp.24-38.

Sheehan, K.B., 2002. Toward a Typology of Internet Users and Online Privacy Concerns. *The Information Society*, 18, pp.21-32.

Sheehan, K.B. & Hoy, M.G., 1999. Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns. *Journal of Advertising*, 28, pp.37-51.

Sheffrin, H., 2002. *Beyond Greed and Fear*. New York, United States: Oxford University Press.

Simon, H., 1957. A Behavioral Model of Rational Choice. In *Models of Man, Social and Rational: Mathematical Essays on Rational Human Behavior in a Social Setting*. New York: Wiley.

Simon, H., 1969. *The Sciences of the Artificial*. Cambridge, MA: MIT Press.

Sitkin, S.B., 1995. On the Positive Effect of Legalization on Trust. In R.J. Lewicki, B.H. Sheppard & M.H. Bazerman, eds. *Research on Negotiation in Organizations*. Greenwich.

Sjoberg, L., 2000. Factors in Risk Perception. *Risk Analysis*, 20(1).

Skinner, E.A., 1996. A Guide to Constructs of Control. *Journal of Personality and Social Psychology*, 71, pp.549-70.

Skinner, E.A., Chapman, M. & Baltes, P.B., 1988. "Control, Means-Ends, and Agency Believes: A New Conceptualization and its Measurement During Childhood. *Journal of Personality and Social Psychology*, 54, pp.pp. 117-133.

Slovic, P., 1999. Trust, emotion, sex, politics, and science: surveying the risk-assessment battlefield. *Risk Analysis*, 19(4), p.689–701.

Slovic, P. & Weber, E.U., 2002. Perception of Risk Posed by Extreme Events. In *The Conference on Risk Management Strategies in an Uncertain World*. Palisades, NY, 2002.

Small, S.A. & Uttal, L., 2005. Action-Oriented Research: Strategies for Engaged Scholarship. *Journal of Marriage and Family*, 67(November), p.936–948.

Smith, H.J., Dinev, T. & Xu, H., 2011. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, 35(4), pp.989-1015.

Smith, H.J., Milberg, S.J. & Burke, S.J., 1996. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*, 20, pp.167-96.

Solove, D.J., 2008. The New Vulnerability: Data Security and Personal Information. In Chander, A., Gelman, L. & Radin, M.J. *Securing Privacy in the Internet Age*. Stanford, CA, USA: Standford University Press. pp.111-36.

Spiekermann, S. & Grossklags, J., 2005. E-Privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior. *Communications of the ACM*, 48(3).

Stewart, D.W., 2007. Analysing Focus Group Data. In Stewart, D.W., Shamdasani, P.N. & Rook, D.W. *Focus Groups*. 2nd ed. London: Sage Publications.

Stewart, K.A. & Segars, A.H., 2002. An Empirical Examination of the Concern for Information Privacy Instrument. *Information Systems Research*, 13(1), pp. 36-49.

Stone, E., Gardner, D., Guetal, H. & McClure, S., 1983. A Field Experiment Comparing Information Privacy Values, Beliefs, and Attitudes Across Several Types of Organisations. *Journal of Applied Psychology*, 68, pp.459-468.

Stone, E.F. & Stone, D.L., 1990. Privacy in organizations: Theoretical issues, research findings and protection strategies. In Ferris, G.R. & Rowland, K.M. *Research in personnel and human resource management.* Greenwich, CT: JAI Press. pp.pages 349-411.

Strand, K. et al., 2003. *Community-based research and higher education.* San Francisco, CA, USA: Jossey-Bass.

Sultan, F., Urban, G.L., Shankar, V. & Bart, I., 2002. Determinants and Consequences of Trust in e-Business. *Working Paper, Sloan School of Management: MIT, Cambridge, MA 02142.*

Tang, Z., Hu, Y.(. & Smith, M.D., 2008. Gaining Trust Through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor. *Journal of Management Information Systems*, 24(4), pp.153-73.

Tauber, A., 2010. Requirements and Properties of Qualified Electronic Delivery Systems in eGovernment: an austrian experience. *International Journal of E-Adoption*, pp.45-58.

Taviani, H.T., 2007. Philosophical Theories of Privacy: Implications for An Adequate Online Privacy Policy. *Metaphysics*, 38.

Taylor, S. & Bogdan, R., 1984. *Introduction to qualitative research methods.* New York: John Wiley & Sons.

Taylor-Gooby, P. & Zinn, J.O., 2006. *Risk in Social Science.* Oxford, UK: Oxford University Press.

Teufel III, H., 2009. Privacy Policy Guidance Memorandum. *US Department of Homeland Security.*

Thaler, R.H. & Sunstein, C.R., 2003. Libertarian paternalism. *American Economic Review*, 93(2), p.175–179.

Thaler, R. & Sunstein, C., 2008. *Nudge: Improving decisions about health, wealth, and happiness.* Yale University Press.

The eSENS Project, 2013. *The e-SENS ("Electronic Simple European Networked Services") Project.* [Online] Available at: http://www.esens.eu/home.html [Accessed 11 April 2013].

The eSENS Project, 2013. *The e-SENS ("Electronic Simple European Networked Services") project.* [Online] Available at: http://www.esens.eu/home.html [Accessed 11 April 2013].

The European Commission, 1995. *EU Directive 95/46/EC - The Data Protection Directive.* [Online] Available at: http://www.dataprotection.ie/viewdoc.asp?DocID=89 [Accessed 11 November 2012].

The European Commission, 2007. *Competitiveness and Innovation Framework Programme (CIP).* [Online] Available at: http://ec.europa.eu/cip/ [Accessed 13 January 2012].

The Ponemon Institute, 2010. 2010 Privacy Trust Study of the United States Government. *The Ponemon Institute Research Report.*

The Privacy Office, 2007. Privacy Technology Implementation Guide. *US Department of Homeland Security,* Washington, DC(available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_ptig.pdf).

Tracy, S.J., Lutgen-Sandvik, P. & Alberts, J.K., 2006. Nightmares, demons and slaves: Exploring the painful metaphors of workplace bullying. *Management Communication Quarterly,* 20, pp.148-85.

Trochim, W.M.K., 2006. Experimental Design. *The Web Center for Social Research Methods*, p.http://www.socialresearchmethods.net/kb/desexper.php.

Tsai, J.Y., Egelman, S., Cranor, L. & Acquisti, A., 2011. The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research*, 22(2), pp.254-68.

Turow, J. et al., 2006. The Federal Trade Commission and Consumer Privacy in the Coming Decade. *Journal of Law and Policy for the Information Society*, Federal Trade Commission. Washington, DC (Available at: http://works.bepress.com/joseph_turow/12).

Tversky, A. & Kahneman, D., 1981. The Framing of Decisions and the Psychology of Choice. *Science*, 211(4481), pp. 453-458.

UN News Centre, 2013. *Online features essential for future of postal services – UN report.* [Online] The United Nations Available at: http://www.un.org/apps/news/story.asp?NewsID=41005&Cr=new+technologies # [Accessed 18th February 2013].

Universal Postal Union, 2011. *Universal Postal Union Standards Support and Downloads.* [Online] Available at: http://www.upu.int/en/activities/standards/support-and-downloads.html [Accessed April 2013].

US Postal Service Office of Inspector General, 2011. The Role of the Postal Service in the Digital Age Part 1: Facts and Trends. *Office of the Inspector General Risk Analysis Research Center Report*, 11(002).

USPS Office of the Inspector General, 2013. Post Office of the Future: The Next Hotspot. *Forthcoming.*

USPS Office of the Inspector General, 2013. What America Wants from the Postal Service: A Survey of Internet-connected Americans. *Report Number: RARC-WP-13-009.*

Van de Ven, A.H., 2007. *Engaged scholarship: a guide for organizational and social research.* London: Oxford University Press.

Van Dyke, T.P., Midha, V. & Nemati, H., 2007. The Effect of Consumer Privacy Empowerment on Trust and Privacy Concerns in E-Commerce. *Electronic Markets*, 17, pp.68-81.

Van Lieshout, M., Kool, L., Van Schoonhoven, B. & De Jonge, M., 2011. Privacy by Design: an alternative to existing practice in safeguarding privacy. *Info*, 13(6), pp.55 - 68.

Van Slyke, C., Shim, J.T., Johnson, R. & Jiang, J., 2006. Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, pp.415-44.

Varian, H.R., 1997. Economic aspects of personal privacy. In Administration, N.T.a.I. *Privacy and Self-Regulation in the Information Age.* Washington, DC.

Venkatesh, V., 2000. Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion into the Technology Acceptance Model. *Information Systems Research*, 11 (4), pp.342-65.

Voltage.com, 2013. *It's Time for a New Paradigm in Data Protection.* [Online] Available at: www.voltage.com [Accessed 19 April 2013].

von Neumann, J. & Morgenstern, O., 1947. *Theory of Games and Economic Behavior*. 2nd ed. Princeton, NJ: Princeton University Press.

Wald, M., 2004. Airline Gave Government Information on Passengers. *New York Times, Technology Section*, 18.

Walkey, F.H., 1979. Internal Control, Powerful Others, and Chance: A Confirmation of Levenson's Factor Structure. *Journal of Personality Assessment*, 43(5), pp.532-35.

Walls, J.G., Widmeyer, G.R. & Sawy, O.A.E., 1992. Building an Information Systems Design Theory for Vigilant EIS. *Information Systems Research*, Vol. 3((1)), pp.pp. 25-59.

Walsham, G., 1995. The Emergence of Interpretivism in IS Research. *Information Systems Research*, Vol. 6((4)), pp.pp. 376-394.

Wang, Y. & Kobsa, A., 2009. Privacy Enhancing technologies. In R.S. Manish Gupta, ed. *Handbook of Research on Social and Organizational Liabilities in Information Security*. New York: Information Science Reference.

Wang, Y. et al., 2013. Privacy Nudges for Social Media: An Exploratory Facebook Study. In *Second International Workshop on Privacy and Security in Online Social Media*. Rio De Janeiro, Brazil, 2013.

Warren, S. & Brandeis, L.D., 1890. The Right to Privacy. *Harvard Law Review*, Vol. IV((5)).

Weber, R., 1987. Toward A Theory Of Artifacts: A Paradigmatic Base For Information Systems Research. *Journal of Information Systems*, Vol. 1((2)), pp.pp. 3-19.

Weber, E.U., 2001. Decision and choice: Risk, empirical studies. In N.J. Smelser & P.B. Baltes, eds. *International Encyclopedia of the Social and Behavioral Sciences*. Oxford, UK: Elsevier Science Limited.

Weinberger, C.V., 1973. Records, Computers and the Rights of Citizens. *Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, pp.Department of Health, Education, and Welfare.

Weiss, R., 1994. *Learning from Strangers*. New York: Free Press.

Westin, A., 1970. *Privacy and Freedom*. New York: Atheneum.

Westin, A., 2003. Social and Political Dimensions of Privacy. *Journal of Social Issues*, Vol 59((2)), pp.pp. 431-453.

White, T.B., 2004. Consumer Disclosure and Disclosure Avoidance: A Motivational Framework. *Journal of Consumer Psychology* , 14(1/2), pp.41-51.

Whitley, E.A., 2009. Informational Privacy, Consent and the "Control" of Personal Data. *Information Security Tech. Report*, 14(3).

Whitley, E.A., 2009. *Informational Privacy, Consent and the "Control" of Personal Data*. Informations Systems technical Report 14. London: Elsevier London School of Economics.

Williams, B., 1988. Formal Structures and Social Reality. In Gambetta, D. *Trust: Making and Breaking Cooperative Relations*. New York: Basil Blackwell Ltd.

Williams, M.-A., 2009. Privacy Management, the Law & Business Strategies: A Case for Privacy Driven Design. In *The 2009 International Conference on Computational Science and Engineering*. Vancouver, Canada, 2009. IEEE Computer Society.

Williamson, O.E., 1974. *Markets and Hierarchies*. New York: The Free Press.

Wilson, D.W. & Valacich, J.S., 2012. Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus. In *Thirty Third International Conference on Information Systems*. Orlando 2012, 2012.

Wittgenstein, L., 1922. *Tractatus Logico-Philosophicus*. 57405740th ed. London: C.K. Ogden.

Xu, H., Teo, H.H. & Tan, B.C.Y., 2005. Predicting the Adoption of Location-Based Services: The Roles of Trust and Privacy Risk. In *Proceedings of 26th International Conference on Information Systems*. Las Vegas, NV., 2005.

Xu, H., Teo, H.H. & Tan, B.C.Y., 2010. The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services. *Journal of Management Information Systems* , 26(3), pp.137-76.

Xu, H., Teo, H.H., Tan, B.C.Y. & Agarwal, R., 2009. The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems*, 26(3), pp.135-73.

Yamaguchi, S., 2001. Culture and Control Orientations. In Matsumoto, D. *The Handbook of Culture and Psychology*. New York: Oxford University Press. pp.pages 223-243.

Yu, C.-h., 2011. *Parametric Tests*. [Online] Available at: www.creativewisdom.com [Accessed 11 May 2011].

Zhao, S., 2004. Consociated contemporaries as an emergent realm of the lifeworld: extending Schutz's phenomenological analysis to cyberspace. *Human Studies*, 27, pp.91-105.

Zhao, S., 2006. Do Internet Users have more Social Ties? A Call for Differentiated Analyses of Internet. *Journal of Computer-Mediated Communication*, 11(3), pp.844-62.

Zhao, S., 2007. Internet and the lifeworld: Updating Schutz's Theory of Mutual Knowledge. *Information Technology & People*, 20, pp.140-160.

Zweig, D. & Webster, J., 2002. Where is the Line between Benign and Invasive? An Examination of Psychological Barriers to the Acceptance of Awareness Monitoring Systems. *Journal of Organizational Behavior* , Volume 23, pp.pages 605-633.

10 Appendices

10.1 Appendix A: Informational Privacy Concerns and their Antecedents

This appendix provides a further and more detailed discussion – in addition to the discussion provided in chapter 2 - of three antecedents to informational privacy concern, i.e. online trust, perceived control over personal information and demographics of users, which are the antecedents that have received greatest attention in the empirical literature on online privacy.

10.1.1 Perceived Control

Another likely candidate as an antecedent of privacy concerns is perceived control. Laufer and Wolfe (1977) have suggested that the need and ability to exert control over self, objects, spaces, information, and behaviour is a critical element in any concept of privacy. Stone and Stone (1990) also argue that the loss of control over information is central to the notion of invasion of privacy. Numerous studies on employee monitoring have also acknowledged the importance of personal control in privacy issues in the context of organizations (Zweig and Webster, 2002).

Laufer and Wolfe (1977) noted that control was identified as the psychological concept central to the conceptualization of privacy. As noted in chapter 2, Altman (1975) defined privacy as the selective control of access to the self. Westin (1970) gave a general definition of privacy as an individual's ability to control the terms by which their personal information is acquired and used. Additionally, Fried (1968) argues that privacy is the control that a person has over information about themselves. Altman (1975) argues that a person who successfully manages to control interaction with others is likely to develop more of a sense of competence and self-worth than a person who fails repeatedly to regulate contacts with others. Hence, privacy theorists have applied the term control widely in the privacy literature as the justification for privacy (Johnson, 1974).

Individuals who value their autonomy would prefer exercising direct personal control as they "*would especially feel themselves more self-efficacious when their agency is made explicit*" (Yamaguchi, 2001: 226). However, when exercise of personal control is not possible, people may relinquish their direct control preferences in exchange for security in *proxy* control. Proxy control is an attempt to align oneself with a powerful 'other' in order to gain control through that powerful other. This attempt at gaining control occurs when people do not have enough skills, resources, and power to bring about their desired outcome or to avoid an undesired outcome in the environment by themselves. The third type of control is collective control in which the individual attempts to control the environment as a member of a group or collective (Yamaguchi, 2001). In collective control, responsibility and agency will be diffused among all members of a collective and therefore everyone in a collective is responsible for the outcome.

A key concept in theories of perceived control is the concept of locus of control (LOC). The LOC is derived from social learning theory (Rotter, 1954). It refers to the extent to which individuals believe that they have the ability to affect outcomes through their own actions (Rotter, 1966). Locus, the Latin word for "place", was divided by Rotter into internal and external. People with an internal LOC orientation, typically perceive themselves as having control over their future and believe that their actions produce predicable outcomes. In contrast, an external LOC orientation signifies a belief that outcomes are the result of other powerful other's behaviour or random occurrences, not influenced by anything other than fate, luck, or chance. According to Rotter, the orientation of the LOC stems from family, culture, and experience. Most individuals with an internal orientation have been shown to come from families that rewarded and encouraged effort, education, and responsibility. On the other hand, most individuals with an external orientation come from families with a low socioeconomic status where there is a perceived lack of control over their lives (Levenson, 1973). Initially, Rotter conceptualized the LOC construct as one-dimensional with internal and external LOC at opposite ends of a bipolar axis (Rotter 1966). However, a series of inconsistent findings in the 1960s and 1970s led to calls for revisions to this initial scale (Joe, 1971; Lefcourt, 1972), along with the development of a multidimensional scale of control (Levenson, 1973). Levenson (1973) proposed that the inconsistencies in findings across research studies were due to the treatment of LOC as a one-dimensional construct. She proposed that internality and externality were different dimensions rather than opposite ends of the same dimension. She posited that externality itself was multidimensional and she categorized it as a belief that control is in the hands of either human forces (i.e.

powerful others) or nonhuman forces (i.e. chance and fate). She suggested that for individuals who believed in powerful others, outcomes were predictable and the potential for control (i.e. proxy control) existed; for those who believed in chance or fate, outcomes were unpredictable and controls were not possible. She developed the I, P, and C scales in which "powerful others externality" (P) was assessed separately from "chance externality" (C), and both of these were separate from "internality" (I) (Levenson, 1974). The scale she developed and validated is now a common alternative to the standard Rotter scale. The Levenson scale uses a Likert scale rather than a forced-choice format. Additionally, it is now generally accepted in the psychological literature (Skinner, 1996; Walkey, 1979) that LOC is a multidimensional construct and that internal, powerful others and chance control are theoretically independent constructs (Hoffman, Novak and Schlosser, 2000; Skinner, 1996).

It is important to note at this point that the construct of control has been treated as a *perceptual* construct because it is of greater interest than actual control when predicting behaviour (Skinner, 1996). The conceptualization of perceived control, therefore, differs from the typical usage of the term control in that perceived control is a cognitive construct and, therefore, is subjective (Langer, 1975). Greenberger and Strasser (1986) define perceived control as a psychological construct which reflects an individual's belief in their own ability to effect a change, in a desired direction, on the environment. Skinner et al. (1988) define the control construct more succinctly as the extent to which an agent can produce desired outcomes. It is this notion of control and perception thereof that is relevant to online privacy, in that if individuals perceive they are, in this sense, in control, then their privacy concerns are alleviated.

10.1.2 Online Trust

The concept of trust, including its nature, causes, antecedents and consequences, has been studied by academics across many disciplines, including sociology (Gambetta, 1988; Luhmann, 1988; Williams, 1988), psychology (Deutsch, 1962; Rotter, 1967), organisational behaviour (Mayer, Davis and Schoorman, 1995; Mishra, 1996; Sitkin, 1995), political science (Barber, 1983) and economics and finance (Dasgupta, 1988; Greenspan, 2002; Guiso, Sapienza and Zingales, 2007; Williamson, 1974). Mayer et al. (1995) proposed an integrative definition of trust which attempts to synthesise the various perspectives on it. He defines it as "the willingness of a party, *the trustor*, to be vulnerable to the actions of another party, *the trustee*, based on the expectation that the trustee will perform a particular action that is important to the trustor, irrespective of the ability to monitor or control the trustee" (Mayer et al., 1995, P712).

Luhmann (1988) argues that trust has to be achieved within a familiar world, and changes may occur in the familiar features of the world which will have an impact on the development of trust in human relations. Hart (1988) clarifies his interpretation of trust by positioning it in the middle of a continuum of words. On one end of the continuum there are the words 'belief' and 'faith'. He interprets belief as a feeling that a person or thing will not fail in performance. The feeling varies according to the available evidence or proof. The extreme case of belief is faith, which implies an emotionally charged, unquestioning acceptance of something. On the other end of the continuum, he places the word 'confidence'. This involves less intensity of feeling, and is based on good evidence for being sure of something. Trust stands in the middle of the

two extremes. According to Hart, trust implies depth and assurance of feeling, with inconclusive evidence or proof. He argues that trust is central to social life when neither traditional certainties nor modern probabilities exist, for example in a weak state or relatively lawless zones of public life (Hart, 1988). Luhmann (1988) and Hart (1988) emphasise the importance of personal agency in defining trust. They argue that sociologists often obscure this attribute of trust when investigating how qualities of trust, fairness and cooperation, which belong naturally to intimate social worlds, can be projected on to the modern world of markets and technology. Shankar et al. (2002) define trust or what they term as offline trust as the belief by one party that another party will behave in a predictable manner.

Liu et al. (2005) , like many researchers before them, believe that trust is a complex social phenomenon that reflects technological, behavioural, social, psychological and organisational aspects of interactions among various human and non-human agents. Their viewpoint aligns well with an existing body of research that sees trust as being potentially part of an individual's personality or nature that has developed as a result of their experiences or faith in human nature. This characteristic of an individual's nature has often been called an individual's *propensity to trust*. Trust is represented as a set of specific beliefs which include:

- Integrity;
- Benevolence;
- Ability
- Predictability of the online business.

Corritore et al. (2003) contend that research on online trust can build on the body of work that studies trust in the offline world. They argue that many offline trust findings are applicable to an online environment, since offline and online situations are often similar. Although, it should be noted that an important difference between online and offline trust is that, online trust entails two separate forms of trusting behaviour, trust in the counterparty and trust in the medium or technology. A similarity between offline and online trust, however, is that both are common features of exchanges. In both settings, risk, fear, complexity and transaction costs may restrict exchange. However, cooperation and coordination can enhance exchange. Furthermore, the social rules of interaction between people appear to function in both the offline and online environment. Thus, offline trust research is relevant to the understanding of online trust. Since trust can mitigate fear and perceived risk and complexity in the offline environment, it is likely that it can do the same in the online environment. Similarly, since trust is a form of social capital that can create cooperation and coordination in the offline environment, it most likely can do the same in the online environment. Without trust, it is conceivable that a robust, interactive online environment would not be possible, just as it would not be in the offline world. They define online trust in the context of trust by the individual person towards a specific transactional or informational website as an attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited (Corritore et al., 2003).

Shankar et al. (2002) believe that a company's view of online trust evolves over time. When the first websites were created, the companies that created them viewed online trust as a construct that dealt with website security or information security.

Subsequently, companies' perception of online trust started to include privacy issues such as protecting personal information submitted online and has grown to become a multidimensional, complex construct that has important antecedents and consequences. Tang et al. (2008) found that firms' ability to influence consumer beliefs about trust depends, *inter alia*, on whether firms can send unambiguous signals to consumers regarding their intention to protect informational privacy. They argue that ambiguous signals concerning the protection of informational privacy sent by an organisation can lead to a breakdown of trust between them and their customers, while sending clear and credible signals can lead to enhanced trust and improved social welfare. Jarvenpaa et al. (2000) find that trust affects the attitude and risk perception of individuals, which in turn influences the individual's willingness to buy online. Gefen (2000) echoes Luhmann's belief that familiarity is a precondition for trust. He explores this belief in the context of ecommerce and finds that both familiarity with an online store and its processes and trust in the vendor influences the individuals' intentions to inquire about, and purchase books. Additionally, he finds that while familiarity builds trust, it is primarily individuals' disposition to trust that affects their trust in the online vendor.

Table A1 outlines the characteristics of trust which can be established and consolidated to help to provide an environment of trust between parties on the Internet. If imparting personal information online involves making a trusting decision, this literature could be interpreted as implying that online trust is a prerequisite for imparting personal information. There is sufficient evidence to suggest that individuals differ greatly in their tendency to trust (Ambrose and Johnson, 1998; Gefen, 2000; Lee and Turban, 2001; Malhotra, Kim and Agarwal, 2004) and an individual's propensity to trust is

frequently proposed as one of several key determinants of online trust (Gefen, 2000; Lee and Turban, 2001; Malhotra, Kim and Agarwal, 2004; McKnight and Chervany, 2001). Nevertheless, it must be noted at this point that because of the subjective nature of online trust, it is not possible to measure exactly how much trust is needed in a given scenario to ensure online privacy concerns do not arise.

Table A1 Perceived Characteristics of Trustworthiness

Researcher	Perceptions that convey trustworthiness
Chen and Dhillon (2003)	Competence Integrity Benevolence
Bhattacharjee (2002)	Ability Integrity Benevolence
McKnight et al. (2002)	Competence Benevolence Integrity
Lee and Turban (2001)	Ability Integrity Benevolence
Peters et al., (1997)	Knowledge and expertise Openness and honesty Concern and care
Mishra (1996)	Competence Concern Openness Reliability.
Sitkin (1995)	Competence Benevolence Values
Mayer et al., (1995)	Ability Integrity Benevolence
Barber (1983) Covello (1992)	Knowledge and expertise Openness and honesty Concern and care
Lieberman (1981)	Competence Integrity

Is Trust an Antecedent to Online Privacy Concern?

Various empirical studies have looked at the consequences of online trust for privacy concerns. Phelps et al. (2000) examined factors affecting consumers' informational privacy concerns and found four significant factors, among which trust figures prominently alongside control. A subsequent study conducted by the same authors (Phelps et al., 2001) found that consumers' attitudes of trust toward direct marketing also act as antecedents to privacy concerns (which are, in turn, antecedents to purchase behaviour and the overall purchase decision process). Sultan et al. (2002) highlight the fact that online trust affects an individual's intent to act which in turn can have an impact on their intent to purchase and remain loyal to a given website. Jarvenpaa et al. (2000) find that trust affects the attitude, risk perception of individuals, which in turn influences the individual's willingness to buy online. The view that trust is an antecedent to privacy concern is not, however, universally shared. Milne and Boza (1999), for example, conducted a US-wide consumer survey and found that improving trust and reducing informational privacy concerns are two distinct approaches to managing online consumer information and that neither is an antecedent of the other. They argue that, when managing consumer information, efforts to improve trust between consumers and organisations have proven to be more effective than efforts to reduce informational privacy concern (Milne and Boza, 1999). On a related note, neither Norberg et al. (2007) nor Horne and Horne (2002) find any support for the positive impact of trust on willingness to disclosure personal information, which indirectly weakens the case for interpreting trust as an antecedent of privacy concerns since the latter are typically found to influence personal information disclosure decisions.

Trust and Ambiguity

Online trust can be viewed as the customer's expectation that the online business will treat the customer's information fairly (Shankar, Urban, & Sultan, 2002). Tang et al. (2008) found that firms' ability to influence consumer beliefs about trust depends, inter alia, on whether firms can send unambiguous signals to consumers regarding their intention of protecting privacy. The ambiguity about the amount of control an individual can exercise over his/her own privacy has become increasingly common in highly networked, digitized, and interconnected information societies (Acquisti & Grosslags, 2005). In this context, Varian (1997) noted that an individual has little or no control over the secondary use of his/her personal information, and hence may suffer negative externalities whenever other parties transact using his/her personal data. In such scenarios, ambiguity becomes relevant to the individual's decision making process. Ambiguous signals can lead to a breakdown of consumer trust (Tang et al. 2008).

10.1.3 Demographics

Research has shown that demographic factors affect opinions and attitudes about privacy with age, gender and race being the most influential. In the Harris/Equifax study of 1990, age was the most significant demographic factor explaining attitudes towards privacy. Americans in the 30-49 age group had the highest concerns about privacy and had experienced the most perceived loss of control over informational privacy. The older age group (50+), less likely to be familiar with information technology, expressed the greatest concern and young adults (<30) were the least concerned about informational privacy and the most accepting of businesses using their personal

information, especially in return for some benefit. Bellman et al. (2003) also found that overall concern for informational privacy increased with age. Older consumers were more concerned with the amount of private information being collected, unauthorised access to the data and errors in their data as well as the collection of data of higher sensitivity. Additionally, the Forrester Research's North American Technographics survey (2010), conducted in the second quarter of 2010 suggests that the younger generation (aged between 18 and 29) of Internet users are more relaxed when it comes to protecting their informational privacy than the older generations.

10.2 Appendix B: Immediate and Mediated Antecedents to Privacy Concerns

From Table 2.2 in Chapter 2, it is evident that a small number of informational privacy concerns are reported regularly by respondents. The following concerns have recurred two or more times in each of the surveys examined:

- Collection (unauthorized or otherwise) of personal information;
- Unauthorized secondary use of personal information;
- Improper access to personal information;
- Errors within stored personal information;
- The use of information in an identifiable way or identification theft.

There is a degree of overlapping between the five privacy concerns listed above. They all have to do with the fear of suffering some form of loss once personal information has been submitted online. In other words, a strong thread running through these privacy concerns is a perception that risk is involved in imparting personal information online. Previous studies generally support the positive impact of privacy risk on privacy concerns (Dinev et al. 2006; Dinev and Hart 2004), and the negative impact of privacy risk on willingness to disclose personal information (Malhotra, Kim and Agarwal, 2004; Xu, Teo and Tan, 2005). This suggests that privacy risk perception and privacy risk aversion may be seen as the two key immediate antecedents of privacy concerns, in agreement with the key role played by these constructs in the privacy calculus model. We may then view the privacy concerns antecedents considered by the privacy calculus literature, together with closely related constructs, as antecedents to either perceived

risk or risk aversion as these are the constructs that appear most prominently in our risk-based reformulation of the privacy calculus model and the theories of decision making under uncertainty on which it is based.

For example, perceived lack of control may be seen as an antecedent to both privacy concerns and perceived risk since, as shown Appendix A, the literature on online privacy has provided substantial evidence that perceived lack of control may be seen as an antecedent to privacy concerns. That is, it may be viewed as an immediate antecedent to perceived privacy risk and, because the latter is an antecedent to privacy concern, as a mediated antecedent to the latter. By a similar line of reasoning, preference for control (especially over personal information) may be viewed as an immediate antecedent to privacy risk aversion and, because the latter is an antecedent to privacy concern, as a mediated antecedent to the latter.

As far as trust is concerned, the level of trust in a counterparty of a given transaction, or at least in the environment in which the transaction takes place, should affect the assessment of the likelihood of adverse occurrences and therefore risk perception. That is, transactions with trusted counterparties should be seen by a rational decision maker as less risky. This leads to view trust as an antecedent to perceived privacy risk and, since the latter is an immediate antecedent to privacy concern, to view trust as a mediated antecedent to privacy concern. As noted in Appendix A, there is conflicting evidence and some disagreement in the literature on whether trust may be deemed as an antecedent to privacy concerns. Nonetheless, in this study view trust as a mediated antecedent to privacy concern due to its plausible role as an antecedent to perceived

privacy risk within the privacy calculus model and leave further empirical testing of this conjecture to the empirical analysis conducted as part of this research as well as to future work. Moreover, we view the importance placed on trust by an individual as a positive antecedent of his/her risk aversion, and therefore as a positive mediated antecedent of privacy concern, because previous literature has found that "trust mediates the relationship between privacy concern and willingness to transact online" (Belanger and Crossler (2011), but see also Van Slyke et al (2006)).

As far as demographic factors are concerned, due to the fact that they do not explicitly appear in the privacy calculus model (or at least they do not appear with a clearly defined and formalized role) , we tend to view them as background factors that may play the role of antecedents to one or more of the mediated antecedents, and therefore one or more of the immediate antecedents. For example, it is possible that age or cultural factor affect, say, perceived control, preference for control and propensity to trust, and therefore both perceived risk and risk aversion. In our empirical analysis, we therefore include them primarily as control variables, though we do offer a discussion of their plausible role within the model or possible extensions thereof.

10.3 Appendix C: Sources for the Questions of the Survey

In this appendix, a list of questions for the constructs online privacy (*willingness to disclose*), perceived benefit, online control preference, ambiguity aversion (), privacy concern (*perceived risk*), trust propensity/importance placed on trust, and finally both potential for availability bias and change in risk handling behaviour following a breach represented by *protective actions/risk handling behaviour* will be enumerated. These questions were taken directly from existing questionnaires in the literature. In the first formulation of our questionnaire, some of the questions were modified and in some case we interpreted their meaning in a different way. When this is the case, we report the original question and highlight any change made to it and/or any different interpretation we give to its meaning.

For all questions, except those on risk handling behaviour, the format for the answer used 5-point Likert-scales anchored with "strongly disagree" and "strongly agree", regardless of the format used in the source. For the questions on risk handling behaviour, the format for the answer admitted binary yes/no choices (or, equivalently, 'box-ticking' for yes).

10.3.1 Willingness to disclose

Willingness to disclose was measured by Dinev and Harte (2006) with answers along five-point scales, anchored with "Not at all" and "Very much", to the following questions:

- To what extent are you willing to use the Internet to do the following activities?
    1. Purchase goods (e.g., books or CDs) or services (e.g., airline tickets or hotel reservations) from websites that require me to submit accurate and identifiable information (i.e., credit card information)
    2. Retrieve information from websites that require me to submit accurate and identifiable registration information, possibly including credit card information (e.g., using sites that provide personalized stock quotes, insurance rates, or loan rates; or using sexual or gambling websites)
    3. Conduct sales transactions at e-commerce sites that require me to provide credit card information (e.g., using sites for purchasing goods or software)
    4. Retrieve highly personal and password-protected financial information (e.g., using websites that allow me to access my bank account or my credit card account)

10.3.2 Perceived benefit

Perceived benefit was measured by Li and Keshelashvili (2006) with an index of six items evaluating the advantages and gains from Internet use (a binary yes/no answer to each item was sought):

- Is the internet

1. Useful for individuals to get information?
2. Useful source to answer his/her questions?
3. Online shopping/bill pay/banking offers him/her convenience?
4. Online games/TV/DVDs are sources for entertainment?
5. Online chats allow individuals to talk to people worldwide?
6. Online communication expands personal contacts?

Hann et al. (2005) found two types of benefit, namely financial gain and convenience, to be the most effective in explaining information submission among individuals. They used an index of five items evaluating the advantages of submission of personal information (a binary yes/no answer to each item was sought):

- I submit my personal information most often for
  1. The convenience of being able to bank online
  2. The convenience of being able to shop online
  3. In exchange for something in which I am interested
  4. In situations where I could win something
  5. In exchange for a monetary reward which I can use to buy items online.

10.3.3 Online Privacy Concern (perceived risk)

The following survey questions were used by Dinev and Hart (2004), with answers along seven-point scales anchored with "strongly disagree" and "strongly agree", to measure individuals' "online privacy concern", which we interpret as a measure of perceived risk regarding the use of personal information:

- I am concerned that the information I submit on the Internet could be misused

- When I shop online, I am concerned that the credit card information can be stolen while being transferred on the Internet
- I am concerned about submitting information on the Internet, because of what others might do with it
- I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee
- When I am online, I have the feeling of being watched
- When I am online, I have the feeling that all my clicks and actions are being tracked and monitored

The following survey questions were used by Smith et al. (1996), who used them (with answers along seven-point scales anchored with "strongly disagree" and "strongly agree"), to measure individuals' "online privacy concern" which, as for the questions used for the same purpose by Dinev and Hart (2004) and which were listed above, we interpret as a measure of perceived risk regarding the use of personal information:

- All things considered, the Internet would cause serious privacy problems.
- Compared to others, I am more sensitive about the way online companies handle my personal information.
- To me, it is the most important thing to keep my privacy intact from online companies.
- I believe other people are too much concerned with online privacy issues.
- Compared with other subjects on my mind, personal privacy is very important.
- I am concerned about threats to my personal privacy today.

The following survey questions were used by Malhotra et. al (2004), with answers along seven-point scales anchored with "strongly disagree" and "strongly agree", to measure an individual's risk beliefs, which we interpret as perceived risk regarding the disclosure of personal information.

- In general, it would be risky to give (personal information) to online companies.
- There would be high potential for loss associated with giving (the information) to online firms.
- There would be too much uncertainty associated with giving (the information) to online firms.
- Providing online firms with (the information) would involve many unexpected problems.
- I would feel safe giving (the information) to online companies.

10.3.4 Online Control preference

The following survey questions were used by Malhotra et al. (2004), with answers along seven-point scales anchored with "strongly disagree" and "strongly agree", to measure individuals' (preference for) control in online settings and therefore risk aversion regarding the use of personal information:

- Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
- Consumer control of personal information lies at the heart of consumer privacy.

- I believe that online privacy is invaded when control is lost or unwillingly reduced as a result of a marketing transaction.

10.3.5 Awareness of Privacy Practices (Ambiguity aversion)

The following survey questions were drawn from Malhotra et. al (2004), who used them (with answers along seven-point scales anchored with "strongly disagree" and "strongly agree"), to measure individuals' "awareness of privacy practices", which we interpret as preference for control/disclosure regarding the use of personal information:

- Companies seeking information online should disclose the way the data are collected, processed, and used
- A good consumer online privacy policy should have a clear and conspicuous disclosure
- It is very important to me that I am aware and knowledgeable about how my personal information will be used

10.3.6 Trust Propensity

The following survey questions were drawn from Malhotra et. al (2004), who used them (with answers along seven-point scales anchored with "strongly disagree" and "strongly agree") to measure an individual's trust propensity:

- Based on your online experiences, to what extent do you agree/disagree with the following statements?
  1. In general, online companies would be trustworthy in handling my personal information.

2. In general, online companies would tell the truth and fulfil promises related to personal information provided by me.
3. I trust that online companies would keep my best interests in mind when dealing with my personal information.
4. Online companies are in general predictable and consistent regarding the usage of personal information.
5. Online companies are always honest with customers when it comes to using personal information that I provide.

10.3.7 Risk Handling Behaviour

Drennan et al. (2006) used an index of seven items to understand the 'protective actions' taken by individuals to reduce their online privacy concerns, (a binary yes/no answer to each item was sought):.

- I take the following protective actions:

1. Start buying well known major brands instead of unknown brands;
2. Brand loyal behaviour;
3. Seeking further information before engaging in an online interaction;
4. Wider search habits;
5. Increased use of word of mouth information sources;
6. A preference for congruent rather than incongruent products in a product category;
7. Avoiding purchase altogether.

10.4 Appendix D: Instrument for Deriving a Typology of Internet Users and Online Privacy Concerns

Sheehan's (2002) four-part typology for the classification of individuals according to their privacy tendencies was used to group the participants of the 20 semi-structured interviews according to their level of informational privacy concern, i.e. the latter were classified in the following four categories:

1. The unconcerned Internet user regarding online privacy concerns;
2. The circumspect Internet user regarding online privacy concerns;
3. The wary Internet user regarding online privacy concerns;
4. The alarmed Internet user regarding online privacy concerns.

The interviewees were categorised according to their responses to the questions below.

Awareness

1. You receive e-mail from a company you have sent e-mail to in the past (low concern)
2. You receive e-mail from a company whose web page you recently visited (moderate concern)
3. You receive an e-mail and have no idea how the company got your address (high concern)

Usage

1. A company requests your e-mail address only to send information of interest (low concern)
2. A notice on a web page states that information collected is used by other divisions of that company (moderate concern)
3. A notice on a web page states that information collected on that web page may be sold to other companies (high concern)

Sensitivity

1. You are asked to provide your name to access home page (low concern)
2. You are asked to provide names of newsgroups read to access home page (moderate concern)

3. You are asked to provide your Social Security Number to access home page (high concern)

Familiarity

1. You receive e-mail about a new product from a company you currently do business with (low concern)
2. You receive e-mail about a new product from known company you don't do business with (moderate concern)
3. You receive e-mail about a new product from a company you've never heard of (high concern)

Compensation

1. A web page requires your e-mail address to access the page; upon registration, you will be entered in a contest to win a computer (value: $1000) (low concern)
2. A web page requires your e-mail address to access the page; upon registration, you will receive a 25% discount on future purchases (moderate concern)
3. A web page requires your e-mail address to access the page; upon registration, you will receive a mouse pad (high concern)

Behaviour

1. Reading unsolicited e-mail.
2. Registering (i.e., providing information about oneself) for web sites
3. Providing inaccurate information when registering for web sites
4. Providing incomplete information when registering for web sites
5. Notifying Internet service providers about unsolicited e-mail
6. Requesting removal from e-mail lists
7. Sending highly negative messages to entities sending unsolicited e-mail (e.g., "flaming")

Method Used for Assessing Privacy Level

Concern for privacy in each situation was measured using a 1–7 scale where 1 indicates the participant is not at all concerned and 7 indicates he/she is extremely concerned.

Frequency of adopting specific behaviour was measured using a 1–7 scale where 1 indicated never taking action and 7 indicated always take action

10.5 Appendix E: The Questions asked of the Participants of the Semi-Structured Interviews

The following interview format and questions were used by the Author to guide each semi-structured interview. The questions listed below are deliberately left open, i.e. to be interpreted by the interviewee exactly as they understood the question, to avoid any possibility of priming the interviewees or of unconsciously directing the interviewees to respond to the questions in a particular manner.

10.5.1 Introduction to the interview

1. Give the interviewee the information on the code of ethics being followed by the interviewer for this research.
2. Explain the reason for the interview and how the data will be used.
3. Explain how data the will be protected, i.e. the recordings will not be saved anywhere only on interviewers work computer. The information the interviewer types up from the recordings will not have the interviewees name on it, only the interview number.

10.5.2 Interview Questions

1. Do you often go on the web?
2. What is your main activity on the web?
3. How would you define the concept of privacy?
4. How would you define informational privacy?
5. Do you have privacy concerns?

6. If so, what motivates these concerns?
7. What information are you ok with submitting online?
8. What actions do you take to protect your informational privacy?
9. How did you decide on those actions?
10. Do you think protecting informational privacy requires you to have a certain amount of:
    a. Control over your personal information once submitted online?
    b. Trust in the online counterparty to which you submit your personal information?
    c. Understanding of the Risks involved in submitting personal information online?
    d. Compromise in that you give something away in exchange for a desired benefit?
11. Do you interact with "trusted websites"?
12. If so:
    a. How did you decide in the first instance that it was a "trusted website"?
    b. Do you carry out risk handling behaviour when on a "trusted website"?
13. Have you or a friend ever experienced a privacy breach?
14. Did you take any actions to avoid breaches in the future?
15. What do you think protects your informational privacy more than anything else?

10.5.3 Concluding the Interview

1. Is there anything else you'd like to tell me?
2. It is ok if I contact you later in case I have additional questions?

10.6 Appendix F: Paradoxical Answers to the same Question: Online Privacy to me is...

The following question was asked twice in the online questionnaire, once at the beginning of the questionnaire (question 1) and again at the end (question 14). The first column of the table shows the responses of individuals to question 1 and the response by the same individual to question 14 once they had completed the questionnaire.

Table F1 Comparison of Question 1 and Question 14 from the online questionnaire

Response To Question 1: Online Privacy To Me Is...	Response To Question 14: Online Privacy To Me Is...
The Amount Of Information You Share With People Online. Little Or A Lot, Depends On Your Own Standards.	The Way You Handle Your Personal Info On The Internet And The Way Companies Etc. Handle Your Information.
The Respect Of My Personal Details In Term Of 'Security', The Third Party Should Be Able To Keep It Secret And In Terms Of Commercial Use, It Should Not Sell My Data.	The Problem I Have With Privacy Has More To Do With Selling My Data Than With Security.
Very Important	Probably Not As Important As It Should Be: We Are Generally Rather Ignorant About What Happens Beyond The Screen
An Oxymoron.	Not Just About Websites And Browsing, But Also About Isp And Provider Services, With Which If Anything My Experience Has Been Worse.
Protection Of Personal Information	Feeling Comfortable/Secure While Performing Any Computer Operation
The Expectation That Information I Do Not Explicitly Publish Is Not Seen By Any Unauthorized Third Party.	I Think Perhaps An Important Concern Is The Tracking Of Web Surfing, The Privacy Issues Involved In Google Street View Etc, Privacy Issues Involved In Something As Simple As Searching (Targeted Advertising). This Sort Of Analysis Of Online Activity For Commercial Purposes Affects My Perception At Least Of Privacy. As Well As The Fact That You Know Communications Are Monitored For National Security Reasons.
How Secure The Information I Send And Receive Is	Keeping The Information I Submit About Myself Online Private
Non-Disclosure Of Information Submitted Without The Prior Explicit Approval Of The Person Concerned	Having The Confidence To Use The Service Regularly
Ensuring People Do Not Have Access To My Private Info Without My Permission	Knowing That I Have As Much Control Over My Personal Information As If I Used A Paper Based System And Had The Paper Completely Under My Control
Keeping My Personal Information Controlled In Terms Of Who Is Able To Access It	Until Now I Hadn't Thought Of Privacy As Involving Websites Tracking My Usage Or Behaviour On The Internet.
The Safety Of My Personal Information That I Submit Online To Register For Websites, User Accounts Etc.	Not Having My Digital Whereabouts Tracked.
Not Posting Anything I'm Not Happy For Absolutely Anyone To Know	Before Reading The Survey I Was Thinking Of Privacy In Terms Of Social Media Rather Than Finance - Of Details Of My Life Rather Than

	Identifying Details/Passwords/Financial Information.
Privacy With A Governing Body On Looking	Online Access Of The Details One Has Submitted To The Company.

10.7 Appendix G: The Research Project's Code of Ethics

This appendix outlines the details of the code of ethics that was followed by the Author during all the stages of data collection and analysis, i.e. the information below was presented to all participants of the online questionnaire, the semi-structured interviews and the eight focus groups and the Author was bound by these guidelines during the entire research project, i.e. during data collection, analysis and reporting of the findings.

10.7.1 Research Background

Thank you for taking the time to complete this work. It is being conducted as part of a doctoral degree and it investigates the concept of online privacy. It aims to establish the following:

1. How an individual determines an acceptable level of online privacy.
2. The impact an individual's propensity/tendency to trust has upon their need for online privacy.
3. The importance of controlling personal information once submitted online.
4. What actions, if any, online users take to protect their privacy.

10.7.2 Participation in this Research is Voluntary.

Completion of this questionnaire/interview/focus group is on a voluntary basis. Each participant has the right to withdraw and to omit individual responses without penalty.

10.7.3 Duration of the Questionnaire/Interview/Focus Group

The questionnaire should take approximately 15 minutes. The interview should take about 60 minutes. The focus group should take about 90 minutes.

10.7.4 Debriefing Opportunities

If participants would like further information regarding this questionnaire/interview/focus group or the research project pertaining to this questionnaire/interview/focus group, they can contact the researchers at this email address:

mmolone2@scss.tcd.ie

10.7.5 Anonymity of Participants and Resulting Data

In order to eliminate concern regarding the collection of personal information during this process, anonymity is guaranteed for all participants. All data collected from this questionnaire/interview/focus group will be treated with full confidentiality and, if published, the data will not be identifiably linked to any individual.

This questionnaire/interview/focus group follows the code of research ethics outlined by Trinity College here:

Trinity College Dublin Research Ethics Protocol

(http://www.tcd.ie/about/policies/assets/pdf/TCDGoodResearchPractice.pdf)

An option will be given to all participants at the end of this work to submit their email address if they are willing to participate in follow-up discussions.

10.7.6 Recording of the Interview/Focus Groups

This session is being recorded, provided you do not object to this. If you do not wish to be recorded please inform the researcher before commencement of the session. All information that is recorded during the interview time will be stored securely and not used for any other purposes other than the current research.

10.8 Appendix H: Privacy Protection Functionalities

This appendix provides details on the privacy protection tools and related system functionalities available within RiposteTrEx.

Date Stamping Personal Information

When submitting personal information to a third party, via the RiposteTrEx system, the user has the option to put a date stamp in the header of the RiposteTrEx form being submitted. This option (the default setting) is selected by checking the check-box in the Informational Privacy Setting Window (shown in figure 7.2). Once the date stamp has expired, a message indicates that the data is no longer representative of the user and, as a result, may be incorrect. With regard to transferring these forms over the Internet, outside the bounds of the RiposteTrEx system, this date stamp can only be used when submitting RiposteTrEx forms to the Internet. Directly inputting a date stamp into forms already on the Internet is not possible with this tool. This tool, however, can also be used in conjunction with the PI updater tool, described above, to ensure any personal information passed on to third parties without the explicit consent of the owner of that personal information becomes obsolete after a given amount of time. This system functionality is in compliance with RFC 3161 standard, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). The TSP is a cryptographic protocol for certifying time-stamp tokens using X.509 public key certificates and public key infrastructure (IETF RFC 3161, 2001).

Cookie Guard

RiposteTrEx maintains a list of all cookies used by the system. Upon login, when the "Set Cookie Guard automatically" option is selected in the Informational Privacy Setting Window (shown in figure 7.2), RiposteTrEx blocks all non-essential cookies whereas, when this option is not selected, it provides the user with the list of all the cookies and allows users to either block or allow all non-essential ones. This option is selected (the default setting) by checking the check-box in the Informational Privacy Setting Window (shown in figure 7.2) and can be altered at any time by users who have chosen to make their profile public.

No tracking

When logged into the RiposteTrEx network, users' movements are not tracked within the system by default. However, if a user wishes to browse the Internet through the RiposteTrEx network, their movements may be tracked just like those of any other user of the Internet. RiposteTrEx's "No Tracking on the Internet" functionality, which can be selected by checking the associated checkbox in the Informational Privacy Setting Window (shown in figure 7.2), adds a header to any information requested by websites indicating the users wishes to *not to be tracked.* This functionality relies on the websites complying with legislation to adhere to the wishes of the user.

Anonymous communication

If users of the system wish to send an anonymous message through RiposteTrEx, they can do so in two ways. Firstly, individuals can send and receive mail anonymously through the system by choosing to hide sender information when sending messages. Only the intended recipient receives information about the sender when (s)he opens the mail, but a third party would not be able to establish who sent the mail by looking at the "envelope" of the mail (the data package). The functionality is enabled through the Informational privacy settings windows available in the user's profile (see figure 7.2) by checking the "set Anonymous Communication" checkbox (the default setting). Secondly, a stronger level of anonymity (total detachment from the user's email account) can be achieved by the user through the purchasing of a post-box number. If users of the system do not wish to send an email with their own name from their standard email account, they can buy a post office box email account and send email via that post office box number (this is simply an email account with a post-box number associated to it instead of the user's name). Users can also decide to receive mail to this email account (post-box number email account), much like the physical P.O. box system.

Encryption

The user can choose to have encryption automatically applied to all sent messages by checking the checkbox "Default Encryption in messages" (the default setting) in the Informational Privacy Settings Window (shown in figure 7.2). If this checkbox is not checked, the user can decide for every single message whether encryption is to be

applied. The type of encryption used within the system is called Identity based Encryption (IBE) and is a tried and tested encryption system that allows for encryption keys to get generated on the fly, this helps to reduce the overhead of key management and the risk of keys being compromised. For further details on this type of encryption see (Boneh & Franklin, 2003). This encryption system has been commercialised and can be built into systems for a set fee (Voltage.com, 2013).

Personal Information (PI) Updater Tool

This is an innovative information-sharing management tool that can be activated by the user by checking the checkbox "Default Encryption in messages" (the default setting) in the Informational Privacy Settings Window (shown in figure 7.2). It uses a formal process for acquiring a user's personal information located in the personal database of the user within the RiposteTrEx system. When seeking personal information from the user's personal database, the requester has to formally identify the portion of personal information being requested, i.e. the user's home address for example. The request is then submitted to the user, who either accepts the request or rejects it. If the user accepts the request and allows for the requester to access that piece of personal information, the requester is given access to *only* that section of the user's personal information.

Before access to the user's personal information is granted, the (authenticated) requester must agree to allow updates and/or revocation (of consent) to the user's personal information whenever the user requests it. Stored within every user's personal database, there is a reference table detailing the list of 'requesters' to whom they have allowed access sections of their personal information.

With the Personal Information (PI) Updater Tool, the user can 1) decide who is allowed to access and retain subsets of their personal information and 2) revoke consent to use or store their personal information from the requester whenever they see fit. While this does not eliminate secondary or unauthorised use of personal information, the user now has a list of people who could potentially breach their trust and pass on their personal information to unauthorised third parties. The requesters of the personal information, being aware of the reference list, may be deterred from passing on the personal information entrusted unto them, without the user's explicit consent. This way, users have a more complete overview of who the processors of their personal information are. There is also the possibility of contacting a suspected offender of a breach and resolving the issue more directly.

If a user suspects a breach has occurred, they can revoke their consent to access their personal information by deleting their personal information from the location(s) they believe caused the breach by using the updater tool. The user's updater tool requests deletion of the personal information from the requester's updater tool, which in turn will authenticate the request and delete the information upon confirmation of authentication.

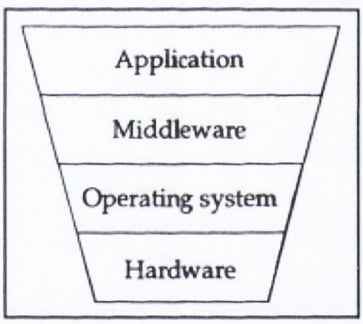
The PI Updater tool also has the functionality to allow users to replicate any changes to their personal information to the requester's copy of their personal information. This tool facilitates the enforcement of the principle of data minimization by ensuring users can update or delete their personal information stored by requesters whenever necessary. Using the PI Updater tool to ensure the user can update their personal information and replicate the changes to the relevant locations within the system also

increases the data quality of the personal information. By increasing data quality, the reliability of, and trust in the system improves (Camenisch et al., 2011).

Access controls

The function of any access control system is to control which principals, i.e. persons, processes, machines, have access to which resources in the system. It controls which files these principals can read, which programs they can execute and how they share data with other principals (Needham & Maybury, 2001).

Figure 10.H.1 Levels of system access control (Needham & Maybury, 2001)



Note: Access controls exist at different levels of a system

Access control works at a number of levels within a system, as shown in the figure above, and usually it is not appropriate to allow users access all of these levels (Needham & Maybury, 2001). However, giving users a certain amount of control over the *application* layer of access control gives users an increased sense of control over who has access to their personal information. Users of RiposteTrEx are allowed to assign 'read access' to their personal information, i.e. read access to their profile and to

their personal databases, to individuals of their choice. This option can be activated by the user by checking the checkbox "Set Access Control automatically" (the default setting) in the Informational Privacy Settings Window (shown in figure 7.2).

10.9 Appendix I: Technical Design Principles

This appendix provides details on the principles adopted in the design of RiposteTrEx, so as to ensure that the system fulfils the requirements identified in chapter 7.

Closed nature of the network and multifactor authentication

The RiposteTrEx network, although run over the Internet, is a closed network. Closed networks require authentication of some kind to gain access to the system (Camenisch and Pfitzmann, 2007). Within closed systems, authentication is used for verifying that agents are genuine.[23] In online settings, it provides access to digital identities or profiles. In this way, only known entities have access to the system and thus to the databases stored within the system. This reduces the risk of unauthorised access to users' personal information stored within the personal databases in the system.

RiposteTrEx uses multifactor authentication to ensure private communication between citizens and between the latter and government. This multifactor authentication is achieved by combining online user registration on the RiposteTrEx system with physical authentication through local post offices. After the user registers on the

[23] Notions of identity and authentication are fundamental concepts in every marketplace or community (Camenisch et al., 2011).

RiposteTrEx network they receive a 4 digit pin code to their physical address. Once the user enters this pin into the RiposteTrEx system, they are authenticated and given access to the system. A detailed description of this multifactor authentication can be found in Sheedy and Moloney (2013). For mobile authentication the RiposteTrEx system uses the Mi-token (tokenless) authentication tool (Mi-token.com, 2012). This is a commercialised tokenless authentication system which, for a set fee, can be built into systems.

When multifactor authentication is required to access a system, the incidences of spam and phishing attacks occurring within that system are reduced as all members of the system are identified and authenticated and thus intruders are detected faster (Camenisch and Pfitzmann, 2007). This increases the reliability of any information sent between members of the system. This in turn increases the integrity of the data within the system (Camenisch and Pfitzmann, 2007).

Data minimisation

This is a well-known and widely adopted principle in the IS literature, especially the PbD literature. Deciding on how to best implement the principle of data minimisation within the RiposteTrEx system was carried out in consultation with the systems Chief Architect, Head of Development, Chief Technology Officer and Chief Cryptographer, along with two external data protection officers. The main tool for ensuring data minimisation is possible in RiposteTrEx is the PI updater tool described in Appendix H. This tool provides a user-centric approach to *consent to*, and *revocation of permission thereof*, the use and storage of personal information by requesters. By providing such a

tool, control over a user's personal information is no longer something that is managed by the administrators of the system on behalf of the user, instead the user has the opportunity to take an active role in the control and management of his/her personal information. Thus, allowing the user to regulate the level of data minimisation they believe appropriate for every situation.

In addition to the protection provided by the PI Updater tool, all personal data that is stored within the system is encrypted within select personal databases and only accessible to the owners (about whom the information relates) of the personal information. Therefore, no personal information is stored *unencrypted* within the system without the knowledge or consent of the owners of that personal information.

The personal data that is transferred through the system is also encrypted while in transit. No copy of the messages transferred through the system is stored within the system. Once a message passes through the system all copies of that message are deleted automatically. Logs recording the history of transactions taking place over the RiposteTrEx network are stored encrypted within the system, expire after 14 days and are consequently deleted. This functionality was guided by the *principle of minimal retention* proposed by (Goold, 2009) and discussed in this dissertation in chapter 2. This functionality was tested to ensure it does not impact on other functions of the system. This is of particular importance for systems being used in an e-government context and which must demonstrate appropriate balancing of data protection compliance, i.e. deletion of personal data that is no longer required, with auditing and accountability obligations.

Having consulted with data protection officers from the Irish Data Protection Organisation, it was agreed that it is both desirable and possible to set the system to delete all logs of messages going through the system after 14 days and to give the user the option of allowing/not allowing back-ups to be made by the systems administrator of their personal databases on a regular basis. This limit of 14 days can be changed by administrators of the system. It is simply the default time limit set in and recommended by the system. It was noted by the data protection officers that there is no legislative precedence preventing the system from deleting logs of messages sent through the system after a period of 14 days and thus 14 days was an appropriate period of time, in normal circumstances, to retain such logs. The system administrators cannot access or view any personal data being stored or transferred within the system. They can, however, view the messages moving through the network but no details about what those messages contain is available to them.

Decentralization of data, Optional Storage and System Interoperability

This is also a well-known and widely adopted principle in the IS literature, especially the PbD literature. Users have the choice of having two or more personal databases stored within the system to ensure their personal information is distributed across different locations and not stored in one single database. The user needs to go through an extra authentication step (challenge response authentication) to access each one of their personal databases.

Not all citizens will be happy to store their personal information within a system which is administered by a government body such as the NPO. Therefore, a requirement of

RiposteTrEx system is also to ensure interoperability of the RiposteTrEx system with other database management systems (DBMS) so that individuals can decide where their personal information is stored, i.e. either downloaded locally on their own personal computer, within the system of a private service provider (SP) like a bank or telecommunications company, with a public/private company like the NPO or with a government department or agency. Consequently, the files and documents storing the user's personal information have been developed using open standards and XML to ensure interoperability between systems and portability from one system to another.

Every DBMS has an independent internal structure and organisation, for example, some systems capitalize field names in their files and documents, some ensure all names are lowercase. These differences make it difficult to port *entire* databases from one DBMS to another. Therefore, rather than porting an individual's entire personal database from the RiposteTrEx system into another DBSM, RiposteTrEx uses XML documents to allow for all files from a RiposteTrEx database to be copied into any other DBMS that can handle XML documents.

Moreover, from the time that users register with the system, they are informed that all storage and transfer of personal information within the system is on a voluntary basis. Users can use a *personal database* facility (an encrypted database for storing personal information within the system) offered by the system *if they wish*. Storage of any type of personal information is voluntary and all personal information can be deleted

whenever the user wishes. Backup copies of the *personal databases* stored by the system are also optional and encrypted by default[24].

[24] Note that when a personal database is "archived", i.e. when a user no longer wishes to store their personal information within the RiposteTrEx network and moves their files from the RiposteTrEx network, any previously backed-up databases are also deleted.

10.10 Appendix J: Other System Features

This appendix provides details on the principles adopted in the design of RiposteTrEx, so as to ensure that the system fulfils the requirements identified in chapter 7.

Security certification (ISO 270001)

The RiposteTrEx system is a new product and therefore has not yet achieved any ISO security certification. However, it has been built adhering to the recognised ISO 27000 series of standards for information security and to other industrial standards such as Federal Information Processing Standard (FIPS) Publication 140-2[25] (National Institute of Standards and Technology , 2001) and the Universal Postal Union's technical standards for Electronic Data Interchange (EDI) and document exchange (Universal Postal Union, 2011).

Once security certification is achieved, perceived trust in, and transparency of, the system should increase for users. It was anticipated that the absence of security certification might cause concern among the participants of the focus groups, so it was explained to them that the system has been built with a view to getting security certification and would eventually undergo auditing for security certification.

[25] This is a U.S. government computer security standard used to accredit cryptographic modules within information systems

Displaying Trust and Privacy Seals

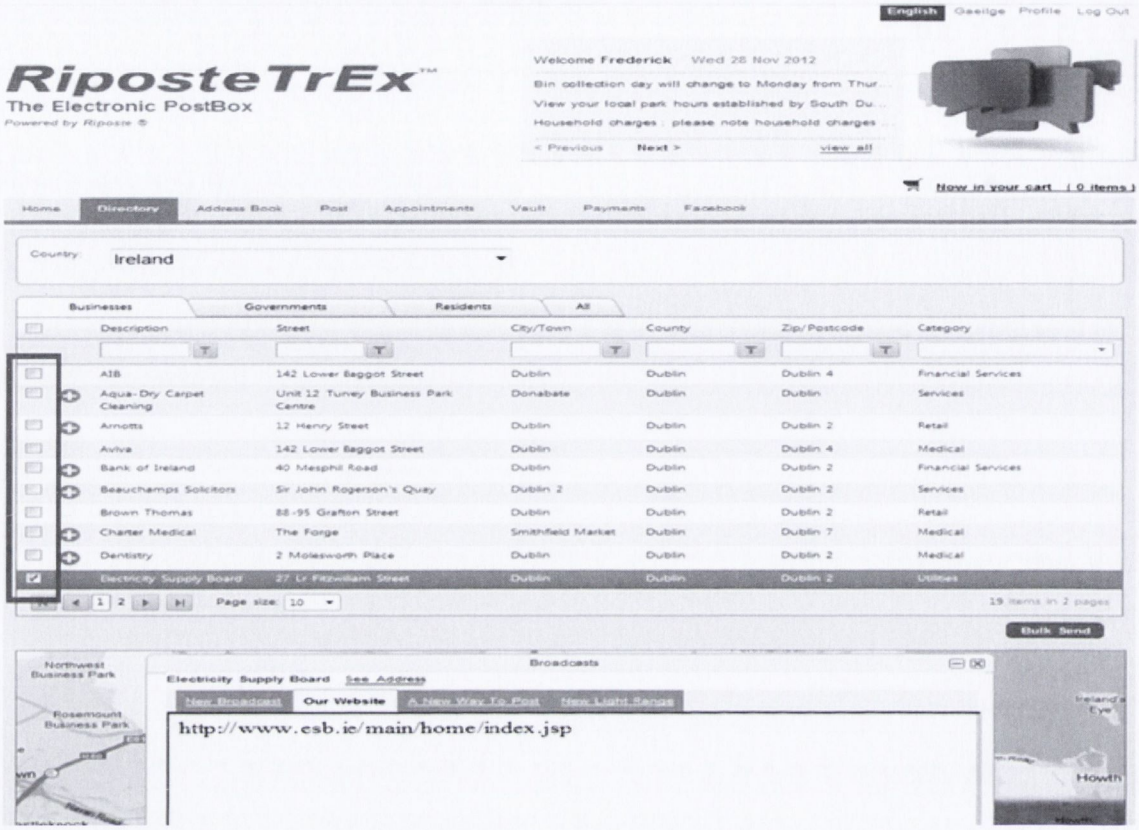
Trust and privacy seals help consumers make a more accurate assessment of the risks of disclosing personal information to online organisations, and therefore displaying them should promote consumer disclosure (Milne & Culnan, 2004). They also provide users with a positive anchor when they are first introduced to the system. Users prone to heuristic driven bias may be positively influenced by such seals and thus make a more positive judgement of the system as a result.

Again, due to the fact that the RiposteTrEx system has been developed only very recently, it does not yet possess any trust or privacy seals as of the writing of this dissertation. The system, however, is designed to make use of such seals when they will become available in order to build trust and help anchor in a positive manner users' belief regarding the reliability of the system.

Opt in solutions for newsletters and notifications

In order to reduce spam, direct marketing is not allowed in the RiposteTrEx system. The system allows all users to "opt-in" to any email newsletters or marketing mail, from other authenticated users of the system, for which they wish to sign up by simply enabling a checkbox in the main address book directory database of the system. In order to send marketing emails, companies must be authenticated with the RiposteTrex system. Users can equally "opt-out" of receiving marketing email by unchecking the same checkbox. (Figure J..2 in Appendix J shows the checkbox system for receiving marketing mail from local businesses).

Figure J.1 "Opt-in" to marketing from companies within the RiposteTrEx network

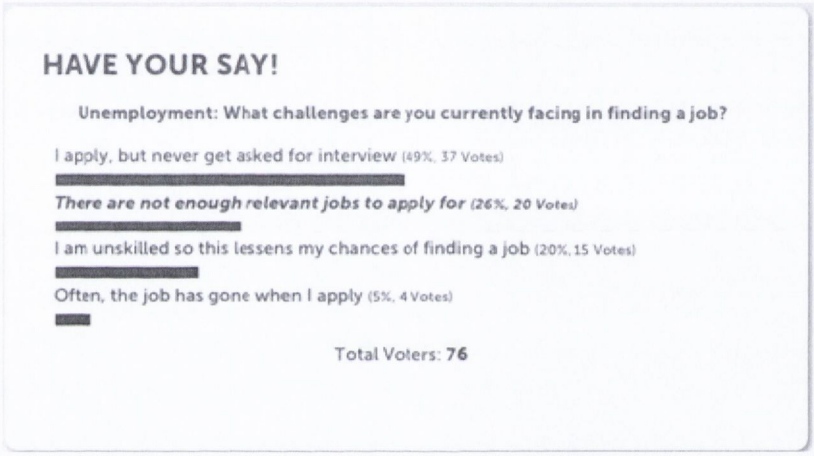


Customer feedback

A form entitled "Have your say" is available to the customer in the 'Contact us' section of the system where customers can submit their ideas and suggestions on how to improve the service provided by An Post. They are also invited to give feedback on their experience with the system. These forms are collected in a database within the system and reviewed regularly by administration staff at An Post. This feature was added so that the user could have an input in how their postal system will be developed and managed. Through participating, it was hoped that trust in the system would increase for the user. Additionally, short surveys are sometimes presented to users from this page. This feature was intended to help An Post survey users on matters of public

interest, such as unemployment in certain locations in Ireland, in a transparent manner conducive to building trust. Figure J.2 shows one such survey conducted over 12 weeks during a pilot of RiposteTrEx that was run from September 2012 until November 2012 in the London borough of Tower Hamlets. For more information on this pilot, see Moloney and Coyle (2014) (forthcoming). This pilot study of RiposteTrEx is beyond the scope of this research but it is briefly discussed in chapter 8, section 8.4.4.

Figure J.2 A short survey on employment issues in the London Borough of Tower Hamlets



Provision of help and assistance tools

It was shown in the online questionnaire and anecdotally in the semi-structured interviews that both familiarity with ICTs and education positively impact users' willingness to disclose personal information. Within the RPC model, this boils down to the effect of lower limits to rationality and perceived ambiguity. Providing extensive training tools for users to learn about the product should help increase their familiarity with the system and educate users regarding how they can protect their personal information online. Providing infrastructure for user forums for more expert and non-expert users may also be a way of encouraging users to help each other understand the

benefits of the system. While no such training materials have yet been made available to the users of the RiposteTrEx system, a team of technical writers are currently undertaking this task and the material should be available with the next release of the product.

Link to a National De Jure System

The RiposteTrEx system is being developed as an electronic national *de jure* postal system. This means that the system is being developed in the context of e-government and therefore operates under particular national laws (Tauber, 2010) and offers special functionalities.[26] As it is typically the case in such systems, it provides services for Non-Repudiation of Submission (NRS) and Non-Repudiation of Delivery (NRD). The former provides public authorities with evidence of the delivery of a mail item having taken place at a certain point in time. The latter provides public authorities with evidence that mail was delivered to a recipient at a certain point in time. This is similar to the conventional postal service in that, if required, official and legal receipt of delivery can be specified. The service does not notify the sender when the mail is opened, only when the mail has been successfully delivered. Implementation guidelines concerning non-repudiation protocols are specified by the ISO/IEC 13888 standard (Tauber, 2010), which is followed in the development of RiposteTrEx. Moreoevr, unlike normal email, the contents of mail sent through the RiposteTrEx system are encrypted by default using secure sockets layer (SSL) encryption.

[26] For de jure or legislated systems, it is typically stipulated by the law that the provider of the system does not tamper with the mail, or the personal data of their customers (Tauber, 2010). In order to maintain credibility and be seen as trustworthy, it must be managed in an impartial and unbiased manner.

Anchoring to the Trusted Brand Name of the Post Office throughout the System

Trust has been shown to be both an antecedent to informational privacy concerns (Belanger et al., 2002), consistent with the RPC model, and an outcome (a negatively affected one) of informational privacy concerns (Chellappa, 2008; Malhotra et al., 2004). Either way, the building of trust is strongly linked to reducing informational privacy risk perception and therefore (because risk perception is, within the RPC model, an antecedent to privacy concern) to the reduction of privacy concerns. In fact, building and maintaining a trusted brand is considered as one way of decreasing privacy concerns for users (Belanger, Hiller and Smith, 2002). Previous research has indicated that NPOs are often seen as trustworthy (The Ponemon Institute, 2010; MacCarthaigh, 2012).

10.11 Appendix K: Research Papers from this Dissertation

This appendix briefly describes the papers that have been published, and work in progress, from this dissertation. In total, 5 papers have been presented in research conferences, 1 paper has been published in a journal and two book chapters are forthcoming and are due to be published either later in 2013 or early 2014.

The first paper from this work was accepted by the 11th European Conference on e-Government, 2011. The paper was written by Church and Moloney (2011). In this paper we (the authors) present RiposteTrEx as a digital postal solution, which was designed to counteract the recent decline of postal services due in part by the decline in physical mail volumes. We argue that our new system helps to restore, in digital form, the full range of traditional universal services afforded by Posts to citizens.

The second paper is Church and Moloney (2012) and was presented at the Annual Services Research and Innovation Institute Global Conference in San Jose, California. In the paper we address the design challenge of developing ICT systems for public e-service provision. We argue that public sector services differ qualitatively from private sector services in that they should provide not just value for money but also *public value*. Therefore, public sector ICTs have unique requirements that are not thoroughly supported by traditional ICTs and their respective design theories. Using public value theory as a theoretical lens, we present a design theory to guide developers of public sector ICTs on how to produce systems which provide public value through private and inclusive systems for public e-services.

The third paper to be published at a conference from this work was written by Moloney and Church (2012) and was presented at the International Conference on Information Systems, 2012. In this paper, we demonstrate the use of the ADR methodology in a NSPD environment. The main argument of this paper is that the ADR methodology facilitates engaged scholarship among IS academics and practitioners in a high pressure environment such is NSPD when using agile development.

The fourth conference paper from this work was presented in January 2013 at the 46th Hawaii International Conference on System Sciences (HICSS). The paper was written by Church, Moloney and Bannister (2013). In this paper we argue that the universal postal service was one of the great social developments of the 19th century and that while such services continue to exist in almost every country in the world today, much of the traffic that they formerly managed has been displaced by various forms of electronic communication. We argue that this transformation brought many benefits but it also involved some losses. One loss was the privacy of the sealed letter. We argue that a system like RiposteTrEx can reinstate the concept of private correspondence, i.e. the privacy of the sealed letter enjoyed for centuries by customers of the postal service, in our digital age.

The fifth conference paper was presented at the 21st Conference on Postal and Delivery Economics, 2013. It was written by Sheedy and Moloney (2013) and it argues that the existing postal infrastructure can help organisations authenticate potential customers and suppliers in the digital world by combining the postal service's physical

infrastructure and the Internet to provide a stronger, multifactor form of authentication, i.e. physical authentication at the post office and online authentication using a pin number sent to the physical address of the user (token based authentication) which is then typed into the system to gain access online. We argue that this multifactor authentication can reduce security exposure and informational privacy concerns of both individuals and organisations ready to interact online. This paper has also been accepted for publication as a book chapter by the conference organisers. A select number of papers from the conference get published in a book from the conference every year.

Other publications from this work include a journal paper published in 2012 and two book chapters that are forthcoming. The journal paper was written by Moloney and Church (2012) and it argues that the Postal Universal Services Obligation (USO) has endured for, and evolved over centuries, and therefore instead of reducing the USO in our digital world, it should be strengthened and redefined to ensure all members of society enjoy the full benefits of the emerging digital world.

The first book chapter from this dissertation is entitled "*Design Principles for Public Sector Information and Communication Technologies*" and was written by Church and Moloney (2013). It is a more developed version of the Church and Moloney (2012) conference paper described above. It is forthcoming in a book entitled "*Technology Development and Platform Enhancements for Successful Global E-Government Design*" due to be published by IGI Global in November/December 2013.

The second book chapter is also forthcoming and is entitled "*Next-Gen E-Government: How do we reconcile Data Protection and Government 2.0?*" and was written by Moloney and Coyle (2014). In this chapter, we address the challenge faced by modern governments to engage with its citizens to encourage transparency and open discussion, on the one hand, and to provide digitally offered public services which require the protection of citizens' private information on the other. We propose a framework for reconciling and meeting both agendas.

This document was created with Win2PDF available at http://www.win2pdf.com.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.
This page will not be added after purchasing Win2PDF.