

**UNIVERSITY OF SOUTHAMPTON**

FACULTY OF ENGINEERING AND THE ENVIRONMENT

Civil Engineering

**Will Privacy Barriers Limit the Uptake of Intelligent Transport Systems?**

by

Scott McKenzie Cruickshanks

Thesis for the degree of Doctor of Philosophy

November 2013



UNIVERSITY OF SOUTHAMPTON

**Abstract**

FACULTY OF ENGINEERING AND THE ENVIRONMENT

Civil Engineering

Thesis for the degree of Doctor of Philosophy

**WILL PRIVACY BARRIERS LIMIT THE UPTAKE OF INTELLIGENT  
TRANSPORT SYSTEMS?**

Scott McKenzie Cruickshanks

Intelligent Transport Systems (ITS) have the potential to increase road-network capacities, reduce congestion and pollution, create shorter and more predictable journey times and significantly improve road-user safety. However, these technologies will also have the ability to track a citizen's every move, extracting information about their daily lives. This data could range from information about the user's driving style, to exactly where their vehicle was at any given time in its lifetime, right down to the radio station the driver listens to. It has been argued that privacy invasions caused by ITS will have a damaging effect on society, creating a 'Big Brother' or panopticon state.

For these fears to be fulfilled, it needs to be the case that future users are not only concerned about the privacy impacts of ITS, but that the ITS will actually cause users to change their travel behaviour. This research examines the results of both a survey of 993 people across four culturally diverse European countries (the UK, Greece, Austria and the Netherlands). The survey primarily seeks to interrogate the factors influencing a future ITS user's privacy concerns, their stated behavioural intention and their actual privacy behaviour.

The results of this research show that privacy concerns could play a significant role in limiting the voluntary uptake rate of the technology. While this may not be critical to the success of all future ITS, future ITS which require high penetration rates to be successful will definitely need to consider the privacy aspects of their system. This research also indicates that when a future ITS user is required to decide whether to disclose their personal information, they will be influenced significantly more by their demographics and the potential risks associated with disclosing the information than the rewards that are on offer. This means that ITS developers should attempt to use less sensitive data where possible, consider using a more trusted organisation to collect and store the required information and also consider the user's perception on how secure a transfer method is.



**Table of Contents**

<b>Abstract .....</b>	<b>1</b>
<b>Table of Contents.....</b>	<b>3</b>
<b>List of Tables.....</b>	<b>7</b>
<b>List of Figures.....</b>	<b>9</b>
<b>Declaration of Authorship.....</b>	<b>11</b>
<b>Acknowledgements .....</b>	<b>15</b>
<b>1. Introduction .....</b>	<b>17</b>
1.1. Background.....	17
1.1.1. Intelligent Transport Systems.....	17
1.1.2. Privacy Fears.....	19
1.1.3. Current Privacy Research Within the Transport Field.....	20
1.2. Aims and Objectives.....	20
1.2.1. Aim.....	20
1.2.2. Objectives.....	21
1.3. Key Contributions to Knowledge .....	21
1.4. Structure of Thesis .....	21
<b>2. Privacy and Intelligent Transport Systems.....</b>	<b>25</b>
2.1. Introduction.....	25
2.2. What is ‘Privacy’ .....	25
2.2.1. History.....	26
2.2.2. Different Levels of Legislation.....	28
2.3. What are ‘ITS’ .....	30
2.3.1. Data acquisition.....	31
2.3.2. Communication.....	33
2.3.3. Data Processing.....	34
2.3.4. Information Distribution and Utilisation.....	35
2.4. The Fears .....	40
2.5. The Current Situation.....	42
2.5.1. Current ITS Examples.....	43
2.5.2. Differences in Current Regulations .....	44
2.6. Future ITS.....	47
2.7. Summary.....	48
<b>3. Privacy Concern, Intention and Actual Behaviour .....</b>	<b>51</b>
3.1. Introduction.....	51
3.2. Research Areas .....	51
3.3. Privacy Concerns .....	52

3.3.1.	<i>Fundamentalists, Pragmatics and the Unconcerned</i> .....	54
3.3.2.	<i>Influence of Demographics</i> .....	56
3.4.	Behavioural Intention .....	59
3.4.1.	<i>Rational Privacy Decision-Making</i> .....	60
3.4.2.	<i>The Privacy Variables</i> .....	61
3.4.3.	<i>Irrationality</i> .....	62
3.5.	Actual Behaviour .....	64
3.6.	Unknowns .....	65
3.7.	Research Model .....	66
3.7.1.	<i>Level of Concern</i> .....	68
3.7.2.	<i>Perception of the Privacy Variables</i> .....	68
3.7.3.	<i>Behavioural Intention</i> .....	69
3.7.4.	<i>Actual Behaviour</i> .....	71
3.8.	Summary .....	72
<b>4.</b>	<b>Methodology</b> .....	<b>75</b>
4.1.	Introduction.....	75
4.2.	Methods .....	77
4.2.1.	<i>Quantitative Data</i> .....	77
4.2.2.	<i>Experimental Data</i> .....	78
4.2.3.	<i>Self-Administered Questionnaires</i> .....	78
4.3.	Phase 1 - Pilot Survey .....	80
4.4.	Questionnaire Design.....	81
4.4.1.	<i>Section A - Rewards, Consequences and Risks</i> .....	82
4.4.2.	<i>Section B – Scenarios</i> .....	82
4.4.3.	<i>Section C – Improvements</i> .....	84
4.4.4.	<i>Section D - About You and Your Choices</i> .....	84
4.5.	Phase 2 -European Union Survey .....	86
4.5.1.	<i>European Sample – Hofstede’s Cultural Dimensions</i> .....	86
4.5.2.	<i>UK Survey</i> .....	88
4.5.3.	<i>Greek Survey</i> .....	91
4.5.4.	<i>Dutch Survey</i> .....	92
4.5.5.	<i>Austrian Survey</i> .....	93
4.5.6.	<i>Sample Summary</i> .....	93
4.6.	Summary .....	95
<b>5.</b>	<b>Concerns</b> .....	<b>97</b>
5.1.	Introduction.....	97
5.2.	Levels of Concerns .....	97

---

5.3.	Perceptions of Privacy Variables.....	104
5.3.1.	<i>The Reward</i> .....	104
5.3.2.	<i>Data Sensitivity</i> .....	106
5.3.3.	<i>Trust in Data Holder</i> .....	112
5.3.4.	<i>Trust in Transfer Method</i> .....	116
5.4.	Summary.....	119
<b>6.</b>	<b>Behavioural Intention .....</b>	<b>123</b>
6.1.	Introduction.....	123
6.2.	Participant Segmentation .....	125
6.3.	Influence of Demographics on Behavioural Intention.....	127
6.4.	Influence of Concern on Behavioural Intention.....	130
6.5.	Influence of Privacy Variables on Behavioural Intention.....	133
6.5.1.	<i>Rewards</i> .....	133
6.5.2.	<i>Data Sensitivity</i> .....	134
6.5.3.	<i>Data Holder</i> .....	135
6.5.4.	<i>Transfer Method</i> .....	136
6.6.	Predicting Behavioural Intention .....	137
6.7.	Summary.....	140
<b>7.</b>	<b>Actual Behaviour .....</b>	<b>143</b>
7.1.	Introduction.....	143
7.2.	Influence of Demographics on Actual Behaviour .....	146
7.3.	Influence of Concern on Actual Behaviour .....	147
7.4.	Influence of Privacy Variables on Actual Behaviour .....	148
7.4.1.	<i>Rewards</i> .....	148
7.4.2.	<i>Data Sensitivity</i> .....	148
7.4.3.	<i>Data Holder</i> .....	149
7.4.4.	<i>Transfer Method</i> .....	151
7.5.	Influence of Behavioural Intention on Actual Behaviour.....	152
7.6.	Predicting Actual Behaviour.....	153
7.7.	Summary.....	156
<b>8.</b>	<b>Will Privacy be a Barrier to Future ITS? .....</b>	<b>159</b>
8.1.	Introduction.....	159
8.2.	Research Model Outcome.....	159
8.3.	The Links between Concern, Behavioural Intention and Actual Behaviour .....	162
8.4.	What Will Impact the Acceptability of a Future ITS in Privacy Terms .....	163
8.4.1.	<i>Demographics of users</i> .....	163
8.4.2.	<i>Cultural background of users</i> .....	163

---

8.4.3.	<i>Sensitivity of the data required</i> .....	165
8.4.4.	<i>Level of trust in the new data holder</i> .....	165
8.4.5.	<i>Level of trust in transfer method</i> .....	166
8.5.	Reducing privacy impact .....	166
8.6.	New Knowledge .....	168
8.7.	Limitations .....	169
8.8.	Recommendations for further work.....	171
8.9.	Will privacy be a barrier? .....	172
<b>9.</b>	<b>Conclusions</b> .....	<b>173</b>
9.1.	Introduction.....	173
9.2.	Aim .....	173
9.3.	Objectives .....	173
	<b>References</b> .....	<b>175</b>
	<b>Appendix A –Pilot Questionnaire</b> .....	<b>197</b>
	<b>Appendix B – English Version of European Survey</b> .....	<b>201</b>
	<b>Appendix C – Greek Version of European Survey</b> .....	<b>205</b>
	<b>Appendix D – Dutch Version of European Survey</b> .....	<b>209</b>
	<b>Appendix E – Austrian Version of European Survey</b> .....	<b>213</b>
	<b>Appendix F – Level of Concern Split by Country and Other Demographics</b> .....	<b>219</b>
	<b>Appendix G – Perception of Individual Rewards</b> .....	<b>223</b>
	<b>Appendix H – Sensitivity of Individual Data Types</b> .....	<b>225</b>
	<b>Appendix I – Trust in Individual Data Holders</b> .....	<b>227</b>
	<b>Appendix J – Trust in Individual Transfer Methods</b> .....	<b>229</b>
	<b>Appendix K – Dendogram of Number of Acceptable ITS Scenarios</b> .....	<b>231</b>



## List of Tables

Table 2-1 Benefits and Information Requirement for a Range of Current ITS .....	45
Table 3-1 Breakdown of the Areas of People’s Privacy Concerns .....	54
Table 3-2 Details of Westin’s Surveys Considered in this Report.....	54
Table 4-1 Summary of Questionnaire Scenarios and the Variables they are Testing .....	85
Table 4-2 European Country Selection – Hofstede’s Cultural Dimensions.....	87
Table 4-3 Hofstede’s Cultural Dimensions for Selected Countries .....	88
Table 4-4 Demographics of Sefton Compared to England and Wales .....	89
Table 4-5 Demographic Make-Up of the UK Mail Survey .....	90
Table 4-6 Demographic Make-Up of the European Survey .....	94
Table 5-1 Demographic Breakdown of the Level of Privacy Concern Quartiles .....	100
Table 5-2 Chi Squared Test for Independence for the Influence of Demographics on Privacy Concern Levels.....	100
Table 5-3 Variables in Binary Logistic Model of High Privacy Concern .....	103
Table 5-4 Demographic and Privacy Concern Breakdown of the Reward Perception Quartiles .....	107
Table 5-5 Chi Squared Test for Independence for the Influence of Demographics and Privacy Concern on the Reward Perception .....	107
Table 5-6 Demographic and Privacy Concern Breakdown of the Data Sensitivity Perception Quartiles .....	110
Table 5-7 Chi Squared Test for Independence for the Influence of Demographics and Privacy Concern on the Perception of Data Sensitivity.....	110
Table 5-8 Demographic and Privacy Concern Breakdown of the Data Holder Trust Quartiles.....	115
Table 5-9 Chi Squared Test for Independence for the Influence of Demographics and Privacy Concern on the level of Data Holder Trust.....	115
Table 5-10 Demographic and Privacy Concern Breakdown of the Transfer Method Trust Quartiles	120
Table 5-11 Chi Squared Test for Independence for the Influence of Demographics and Privacy Concern on the level of Transfer Method Trust.....	120
Table 6-1 Summary of Questionnaire Scenarios and the Variables they are Testing .....	124
Table 6-2 Breakdown of Acceptable Scenarios for Each Cluster .....	126
Table 6-3 Demographic and Breakdown of the Behavioural Intention Clusters .....	128
Table 6-4 Chi Squared Test for Independence for the Influence of Demographics on the Number of Acceptable ITS Scenarios .....	130
Table 6-5 Concern Level and Privacy Variable Perception Breakdown of the Behavioural Intention .....	131
Table 6-6 Chi Squared Test for Independence for the Influence of Level of Concern and Perception of Privacy Variables on the Number of Acceptable ITS Scenarios .....	132

Table 6-7 Variables in Multiple Linear Regression Model of Acceptable Number of ITS Scenarios . 138

Table 6-8 Variables in Binary Logistic Model of Acceptable ITS Scenarios..... 140

Table 7-1 Actual and Test Scenarios ..... 144

Table 7-2 Demographic Breakdown of the Actual Behaviour Clusters..... 145

Table 7-3 Chi Squared Test for Independence for the Influence of Demographics on the Number of Actual Acceptable Scenarios ..... 145

Table 7-4 Chi Squared Test for Independence for the Influence of Demographics on the Number of Actual Acceptable Scenarios ..... 148

Table 7-5 Actual and Test Scenarios ..... 153

Table 7-6 Variables in Multiple Linear Regression Model of Acceptable Number of Actual Scenarios ..... 154

Table 7-7 Variables in Binary Logistic Model of Actual Privacy Scenarios..... 156

Table 8-1 Table Showing Whether the Results of the European Survey Support the Research Model Hypotheses..... 160

## List of Figures

Figure 2-1 Assessment of surveillance across Europe (Privacy International 2011).....	29
Figure 2-2 Example of Inductive Loop Configuration (Neudorff et al. 2003) .....	31
Figure 2-3 Photograph of CCTV Camera Used to Monitor Traffic Flow (Guardian 2011).....	32
Figure 2-4 Photograph of Several Dynamic Message Signs (DMS) in the UK (Techspan 2013).....	36
Figure 2-5 Screenshot of Meteo France Travel Website (Meteo France 2013).....	37
Figure 2-6 Controversial Google Street View Image (Telegraph 2013).....	39
Figure 2-7 Diagram Showing How Cooperative Transport Systems Could Improve Road Safety (SAFESPOT 2013) .....	47
Figure 3-1 The Link Between Concerns, Intention and Behaviour .....	52
Figure 3-2 Privacy Index Results for Westin’s Surveys .....	56
Figure 3-3 Hypothesised Relationships of the Research Model .....	67
Figure 3-4 Hypothesised Relationships of between Privacy Variable and Behavioural Intention .....	70
Figure 3-5 Hypothesised Relationships of between Privacy Variable and Behavioural Intention .....	72
Figure 4-1 Flow Chart of Data Collection and Analysis.....	76
Figure 5-1 Histogram Showing the European Samples Privacy Index Scores out of 40.....	98
Figure 5-2 Percentage of Observed Participants Minus Percentage of Expected Participants in each Privacy Concern Quartile Split by Country .....	99
Figure 5-3 Percentage of Observed Participants Minus Percentage of Expected Participants in each Privacy Concern Quartile Split by Age Category .....	101
Figure 5-4 Reward Histogram.....	104
Figure 5-5 Value of Different Types of Reward.....	105
Figure 5-6 Information Sensitivity Histogram.....	108
Figure 5-7 Sensitivity of Information Types.....	109
Figure 5-8 Percentage of Observed Participants Minus Percentage of Expected Participants in each Sensitivity Quartile Split by Their Privacy Concern Quartile .....	111
Figure 5-9 Trust in Data Holder Histogram.....	113
Figure 5-10 Trust in Individual Data Holders.....	113
Figure 5-11 Percentage of Observed Participants Minus Percentage of Expected Participants in each Data Holder Quartile Split by Their Privacy Concern Quartile .....	116
Figure 5-12 Trust in Transfer Method Histogram.....	117
Figure 5-13 Trust in Individual Transfer Methods .....	117
Figure 5-14 Percentage of Observed Participants Minus Percentage of Expected Participants in each Transfer Method Quartile Split by Their Privacy Concern Quartile.....	121
Figure 6-1 Histogram of Number of Acceptable Scenarios.....	123
Figure 6-2 Histogram of Number of Acceptable ITS Scenarios.....	125

Figure 6-3 Histogram of Number of Acceptable ITS Scenarios..... 126

Figure 6-4 Comparison of the Two Extreme Clusters: Cluster 2 and Cluster 3 ..... 127

Figure 6-5 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Stated Acceptable ITS Scenarios by Their Country ..... 131

Figure 6-6 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Stated Acceptable ITS Scenarios by Their Level of Concern..... 132

Figure 6-7 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Stated Acceptable ITS Scenarios by Reward Cluster ..... 133

Figure 6-8 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Stated Acceptable ITS Scenarios by Data Sensitivity Cluster ..... 135

Figure 6-9 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Stated Acceptable ITS Scenarios by Level of Trust in Data Holder..... 136

Figure 6-10 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Stated Acceptable ITS Scenarios by Level of Trust in Transfer Method ..... 137

Figure 6-11 Correlations between Privacy Variables and Behavioural Intention..... 138

Figure 7-1 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Actual Acceptable Scenarios by Their Country..... 144

Figure 7-2 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Actual Acceptable Scenarios by Their Level of Privacy Concern..... 147

Figure 7-3 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Actual Acceptable Scenarios by Their Reward Cluster ..... 149

Figure 7-4 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Actual Acceptable Scenarios by Their Data Sensitivity Cluster..... 150

Figure 7-5 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Actual Acceptable Scenarios by Their Data Holder Trust Cluster ..... 150

Figure 7-6 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Actual Acceptable Scenarios by Their Transfer Method Trust Cluster ..... 151

Figure 7-7 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Actual Acceptable Scenarios by Their Stated Number of Acceptable Scenarios ..... 152

Figure 7-8 Correlation between Privacy Variables and Actual Behaviour ..... 154

Figure 8-1 Supported Research Model Relationships..... 161

## **Declaration of Authorship**

I, SCOTT MCKENZIE CRUICKSHANKS

declare that this thesis and the work presented in it are my own and has been generated by me as the result of my own original research.

Thesis Title: WILL PRIVACY BARRIERS LIMIT THE UPTAKE OF INTELLIGENT TRANSPORT SYSTEMS?

I confirm that:

1. This work was done wholly or mainly while in candidature for a research degree at this University;
2. Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated;
3. Where I have consulted the published work of others, this is always clearly attributed;
4. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work;
5. I have acknowledged all main sources of help;
6. Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself;
7. Parts of this work have been published as:
  - i. Cruickshanks S, Cherret T, Waterson B, Norgate S, Davies N, Speed C and J Dickinson (2013) “Will Privacy Concerns Limit the Ability of Smart Phone Technologies to Help Foster Collaborative School Travel?”, 92<sup>nd</sup> Annual Meeting of the Transportation Research Board 2013, Washington DC.
  - ii. Cruickshanks S (2013) “Will Privacy Barriers Limit the Uptake of Future Intelligent Transport Systems”, 45<sup>th</sup> Annual UTSG Conference 2013, Oxford.
  - iii. Cruickshanks and B Waterson (2012) “Privacy Decision Making in the Travel Panopticon”, Amsterdam Privacy Conference 2012, Netherlands.



- iv. Cruickshanks and B Waterson (2012) “Will Privacy Concerns Associated with Future Transport Systems Restrict the Publics Freedom of Movement?”, *Procedia-Social and Behavioral Sciences* 48 pp 941-950.
  
- v. Cruickshanks S and B Waterson (2011) “Are Privacy Fears Associated with Intelligent Transport Systems Justified?”, 43rd Annual UTSG Conference, Milton Keynes.

Signed: .....

Date:.....





## **Acknowledgements**

The contributions of many different people have made this possible. I would like to extend my appreciation especially to the following.

Dr Ben Waterson, for his guidance and advice throughout the research project, as well as his painstaking effort in proof reading the drafts, are greatly appreciated.

The students and staff of the transportation groups at the University of Southampton, the Technical University of Crete, the Technical University of Delft and the Technical University of Graz for making me feel very welcome during my stays and helping me to translate and distribute my questionnaires.

Of course, this project would not have been possible without the participation of the random members of the public who so kindly took the time to give me their views.

Last but not least, I would like to thank my wife Lucy who deserves a medal for being abandoned while I gallivanted around Europe and my son Miles without whom this thesis would have been submitted a lot sooner.



## 1. Introduction

### 1.1. Background

The creation of a wide-area, real-time monitoring system for road networks has the potential to improve user safety, dramatically reduce costs for users, governments and businesses (The World Road Association 2004) and benefit the environment (CVIS 2012). Whilst these improvements will be received positively by some, others (Buhrman 2007, Daly 2010 and Reiman 1995) may feel that the potential privacy invasions of increased monitoring could create a 'Big Brother' state (Orwell 1949).

This research seeks to establish whether the privacy concerns associated with future intelligent transport systems (ITS) will, in reality, limit the extent to which these technologies can be implemented across the whole European Union. It will then attempt to derive some general methodologies which will help ensure that, where possible, the future ITS uptake rate can be maximised. Considering the wide range of technologies that fall under the umbrella of ITS, this research seeks to achieve this by investigating which factors impact privacy decision-making in a range of real-world and ITS scenarios. This will identify the factors that consistently influence privacy decision-making in a wide array of different scenarios. In turn this will allow this research to recommend some general methodologies which can be used to reduce the privacy impact of the many different ITS that will be created in the future, in an attempt to ensure that privacy concerns will not limit their uptake.

#### *1.1.1. Intelligent Transport Systems*

ITS is a generic term for the integrated application of communications, control and information processing technologies to the transportation system. ITS covers all modes of transport, with the overall purpose of ITS being to improve decision-making, often in real time, which in turn saves lives, time, money, energy and the environment (The World Road Association 2004).

ITS systems currently in use across the globe include but are not limited to:

- Active traffic management: Both loop detectors and CCTV cameras are used to gain data on traffic flows, which can then be processed and used to control speed limits and information signs to optimise the traffic flow (Highways Agency 2012).

- Traffic signal pre-emption: A vehicle with priority (normally an emergency vehicle but sometimes public transport) sends a transmission which is received and processed by the traffic signal. The traffic signal then in turn processes this information and alters its normal cycle to ensure that the priority vehicle gains clear passage (U.S. DOT 2003).
- Electronic toll collection: Automatic number plate recognition and radio transponders are used to identify each individual vehicle that passes a toll entry and exit point. This information is then processed and the owner of the identified vehicle is automatically charged for each journey through the toll area (The World Road Association 2004).

Information is at the core of virtually all ITS, as they are based around the collection, processing, integration and supply of data, hence there is the potential for privacy concerns to arise around the level of personal information some ITS require to operate. The information obtained by these systems and the way in which it is processed will vary to a great extent with each application.

In the future, it is expected that ITS systems will be able to acquire, communicate, process and utilise more data at a higher frequency. This will enable more advanced ITS, such as cooperative transport systems, to come in to operation. Cooperative systems will work by Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications (CVIS 2012). This new flow of information could open up a 'Pandora's Box' of new ITS applications. Systems could, for the first time, have the ability to communicate with individual vehicles, and to use the knowledge of every vehicle's position and trajectory (potentially even their destination, number of people travelling, propensity to pay and the trip purpose) to optimise the network. This will open the way for personalised routing guidance, safety alerts being sent to vehicles in a certain area and speed recommendations to groups of vehicles, and many more location-specific and network-wide applications.

Drivers will also benefit from more complete and up-to-date information about traffic hazards and congestion, presented directly inside the vehicle. Through new interfaces, drivers will be able to exchange requests and recommendations. The communications channel also has the potential to allow access to information and entertainment content available on the internet, and for the vehicle users to interact with home and office (CVIS 2012). However, it is also feasible that the perception of such cooperative systems will be that the level of personal data being monitored/transferred is too large, to such a degree that the benefits of the cooperative system will not outweigh the public's privacy concerns.

### 1.1.2. Privacy Fears

In recent times, there has been a growing argument from privacy advocates, academics and the media that the growing privacy invasions associated with ITS will have a negative impact on society as a whole. Eamon Daly states in his paper, *Personal Autonomy in the Travel Panopticon* (Daly 2010):

*“The development and convergence of information and communication technologies (ICT) is creating a global network of surveillance capabilities which affect the traveller. These surveillance capabilities are reminiscent of 18<sup>th</sup> century philosopher Jeremy Bentham’s panopticon, and as such the emerging global surveillance network has been referred to as the travel panopticon. I argue that the travel panopticon is corrosive of personal autonomy...”*

The panopticon is a type of prison building, designed by English philosopher and social theorist, Jeremy Bentham in 1785. The concept of the design allows a person to observe all prisoners, without the prisoners being able to tell whether they are being watched (Bentham 1995). The major effect of the panopticon is to induce in the prisoner a state of conscious and permanent visibility that assures the automatic function of power (Foucault 1979).

Rieman describes in his paper, *Driving to the Panopticon* (Rieman 1995) that the problem with some ITS is that they not only ensure that people are seen, but it also makes them feel visible. He feels that the consequence of this is that users will alter their behaviour, and this will impact society as a whole. Others (Guardian 2009 and Buhrman 2007) have related the use of ITS to the creation of an Orwellian surveillance society. Glancy (2004) suggests that not only does ITS allow for a ‘Big Brother’, in the form of an omnipresent totalitarian government, but also a whole host of ‘Little Brothers’, in the form of private-sector information collectors, some of whom may have little respect for individual privacy.

For these fears to be fulfilled, it needs to be the case that the compulsory use of ITS will cause the public to change their travel behaviour. Additionally, these fears could cause low uptake rates of non-compulsory ITS which could prove detrimental to an ITS’s ability to operate effectively if it requires a high penetration rate.

### *1.1.3. Current Privacy Research Within the Transport Field*

As part of their 6<sup>th</sup> Framework Program, the European Commission launched three projects, CVIS, SAFESPOT and COOPERS (CVIS 2012, SAFESPOT 2013 and COOPERS 2013) to explore different cooperative systems that would share extensive amounts of information about a future road user's whereabouts with numerous different stakeholders, in return for safety and efficiency benefits. At the time of launching these projects, 'privacy' was flagged as a potential issue. As a consequence, the European Commission funded several projects with the aim to investigate different methods for making the proposed communications within a cooperative system as secure as possible from a technological/encryption standpoint (PRECOISA 2013, Sevecom 2013, EVITA 2013, Oversee 2013 and PRESERVE 2013), with the view that if the communications are made secure then the 'privacy' issue with the proposed cooperative systems would have been solved.

What the European privacy projects neglect to investigate, however, is whether even if the communications within a cooperative system are made completely secure and anonymous, these systems would still cause future transport users to travel with less freedom. Therefore, it is entirely feasible that a large amount of research effort has gone into an area that doesn't have a major impact on a future ITS user's privacy decision-making. As a consequence, the main focus of this research will be to examine what the main influencing factors of privacy decision-making across a wide range of ITS and real world scenarios are, with the expectation that the findings will provide future ITS developers with a high-level overview of the key privacy factors that could limit the uptake of their wide and varied future ITS technologies.

## 1.2. Aims and Objectives

In order to fully investigate the issues highlighted above, the following aims and objectives have been set.

### *1.2.1. Aim*

To identify the factors that influence privacy decision-making and understand the impact they will have on the successful uptake of future ITS.

### 1.2.2. Objectives

- Objective 1: Understand ‘privacy’ and how it will be relevant to current and future ITS.
- Objective 2: Compare existing, proposed and hypothetical ITS, paying particular attention to their benefits and the level of personal information they require.
- Objective 3: Identify the factors that will cause the level of personal information required by a future transport technology to become unacceptable.
- Objective 4: Understand whether views on the acceptable level of intrusion vary from person to person and discover what the influencing factors are.
- Objective 5: Draw conclusions about whether different ITS in their current, proposed and hypothetical forms will be deemed acceptable in ‘privacy’ terms.
- Objective 6: For technologies that are deemed unacceptable, improvements will be suggested.

### 1.3. Key Contributions to Knowledge

The main information that this research intends to add to existing knowledge is to clearly identify the factors that will influence a future ITS user’s privacy decision-making when confronted with a new ITS. To do this, the research will first investigate whether the findings of previous research (primarily from the field of ecommerce) is transferable to the field of transportation. Once this has been established, this research will then seek to present clear recommendations of ways in which future ITS developers can reduce the privacy impact of their future technologies.

### 1.4. Structure of Thesis

This thesis sets out to present the aims and objectives of the research. It will discuss the background to the research problem before describing the results and implications. Chapter 2 starts by reviewing the term ‘privacy’ before moving on to explore how it is relevant to both current and future ITS, in particular paying attention to the type of personal information required for these ITS to operate, and what benefits they offer in return. Chapter 2 concludes by highlighting how privacy could limit the uptake of ITS and how this is likely to vary in different countries.

Chapter 3 moves on to focus on privacy decision-making. It will do this by conducting a detailed review of the factors that will impact future ITS users' privacy concerns, their stated behavioural intention and finally their actual behaviour when they are confronted with a privacy scenario. It does this primarily by looking at research conducted within the field of ecommerce, of which the key findings are expected to be transferable to the field of transportation. The chapter concludes by drawing out a research model from the existing literature, which will be interrogated in later chapters.

Chapter 4 starts by justifying the use of a quantitative multi-country survey (UK, Greece, Austria and the Netherlands) to interrogate the aims and objectives set out in this chapter, along with the research model presented in Chapter 3. It then describes the rationale behind the questionnaire design and the choice of survey sample. The final section of this chapter outlines the different distribution methods used in each country and discusses the resultant samples, and the possible impact of using slightly different distribution methods in each country.

Chapter 5 looks in detail at the results of the Europe-wide survey in relation to likely levels of privacy concerns that will be associated with future ITS. In particular, it segments users by their level of privacy concern and explores the link between their level of concern and their stated behavioural intention and actual behaviour.

Chapter 6 focuses on future ITS users' stated behavioural intention. It does this by using the results of the European survey to first segment future users by their behavioural intention, and then to look at the perceptions of the privacy variables highlighted in Chapter 3. Chapter 6 finishes by using binary logistic regression models to investigate a user's privacy decision-making.

Chapter 7 further examines the results of the European survey, this time in relation to the participants' actual behaviour. The main concentration of this chapter is the use binary logistic regression models to both predict actual behaviour and to explore the link between actual behaviour and behavioural intention.

Chapter 8 discusses the findings of the previous chapters and ties them back to the original aims and objectives of this research. In particular, it addresses the question 'Will Privacy Barriers Limit the Uptake of Future ITS?'. It does this by highlighting what factors will impact the acceptability of a future ITS in privacy terms, and looking at methods future ITS developers could use to minimise the privacy impact of their future technologies. The final few sections of this chapter look at the limitations of this research and highlight potential areas for future research.



Chapter 9 presents the conclusions that can be made from this research. The main conclusion highlighted is that privacy has the potential to be a barrier to the uptake of some future ITS. However, by appropriately managing the factors influencing privacy decision-making a future ITS developer should be able to ensure that enough users are willing to disclose their personal information that their system should be viable.



## 2. Privacy and Intelligent Transport Systems

### 2.1. Introduction

To fulfil part of Objectives 1 and 2, this chapter will define what is meant by the term ‘privacy’ and then look in detail at how the term is relevant to future ITS. In particular, this chapter will focus on showing how personal information is central to not only the term ‘privacy’ but also to the operation of virtually all ITS, both existing and future, and as a consequence how ‘privacy’ is likely to impact future ITS.

This chapter begins by outlining a brief history of how privacy concerns have had an impact on emerging technologies. It then moves on to look at how the different stages of the information chain involved in an ITS can generate different types privacy fears. This chapter will then look at how existing ITS have been impacted by privacy concerns. The final section of this chapter looks at how future ITS are likely to vary from the existing ones, in terms of the personal information they will require and the high level of privacy concerns that are likely to be linked to them.

### 2.2. What is ‘Privacy’

In order to judge the impact privacy will have on future ITS, it is essential to have a clear understanding of what is meant by the term ‘privacy’. The most widely accepted definition of ‘privacy’ is that offered by privacy guru Alan Westin in his book, *Privacy and Freedom*, (Westin 1967), in which he characterises privacy as “*The claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.*”

However, the term ‘privacy’ is perhaps better summed up by philosopher Judith Jarvis Thompson (1977) who stated “*Perhaps the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is.*” Jarvis Thompson is not alone in taking this stance (Beaney 1966, BeVier 1995, Post 2001 and Solove 2002). Solove (2006) suggests that the main reason behind the lack of clarity is that “*Privacy seems to be about everything, and therefore it appears to be nothing.*” This fact is supported by J. Thomas McCarthy (1987); “*It is apparent that the word ‘privacy’ has proven to be a powerful rhetorical battle cry in a plethora of unrelated contexts... Like the emotive word ‘freedom,’ ‘privacy’ means so many different things to so many different people that it has lost any precise legal connotation that it might once have had.*”

### 2.2.1. History

One thing that is clear about privacy, however, is that the concept has been around since at least the ancient times and across numerous cultures (Privacy International 2011). Many religious texts discuss the need for privacy, including the Bible (Hixson 1987 and Moore 1984) and the Qur'an (An-Noor and Al-Hujraat). There is also evidence of people protecting their personal privacy in classical Greece and ancient China (Warren and Brandeis 1890).

In more modern times, the concept of privacy and its perceived importance has changed with social and political views and the advent of new technologies (Westin 2003). The seminal moment for privacy literature was in 1890 when – largely in response to the increase in newspapers and photographs (made possible by new printing technologies) – future US Supreme Court Justice, Louis Brandeis, and lawyer, Samuel Warren, expressed a concept of privacy as an individual having “*the right to be left alone.*” (Warren and Brandeis 1890)

In 1948, the ‘right to privacy’ was established within Article 12 of the Universal Declaration of Human Rights (UN 1948), although the term ‘right to privacy’ was not defined:

*“No-one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”*

In Europe, this was further elaborated upon in Article 8 of The Convention for the Protection of Human Rights and Fundamental Freedoms, first drafted in 1950 (Europe 1950).

*“(1) Everyone has the right for his private and family life, his home and his correspondence.*

*(2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”*

The next era of significant change in how people viewed privacy and their right to it was between 1961 and 1979 (Westin 2003). This period saw the creation of powerful information technology systems, which had the ability to be used for surveillance of the masses. These technologies were initially widely embraced by governments and private companies alike (Westin 1967). However, it was not long before these technologies were causing concerns for an individual's right to privacy both in academia (Brenton 1964 and Packard 1964) and the mass media (Westin 2003). Worldwide, these fears prompted many governments to start regulating the collection and handling of personal information (Banisar and Davis 1999). The first data protection law was created in the Land of Hesse in Germany in 1970. This was shortly followed by similar national laws in Sweden, the US, Germany and France in 1973, 1974, 1977 and 1978 respectively (Flaherty 1989).

The next major step-change in technology that brought privacy issues further to the fore came in the 1990s, with the creation and rapid uptake of the World Wide Web, wireless communications and data mining software. While these technological developments have had many positive effects, they have also generated many concerns about an individual's privacy. An example of this is that while the newly discovered use of customer-focused marketing allowed businesses to better target the population, direct marketing (and especially telemarketing) rapidly grew with these new technologies, and consumer annoyance grew throughout the decade, leading to a significant amount of negative coverage of what was portrayed as privacy-intrusive business-marketing in the media (Westin 2003).

In response to the growing privacy issues caused by the significant advance in technologies in the 1990s, the European Union enacted the Data Protection Directive (EU 1995). The Directive focused on establishing the following:

- The right to know where the data originated
- The right to have inaccurate data rectified
- The right of recourse in the event of unlawful processing
- The right to withhold permission to use data in some circumstances

Another key aspect of the European data protection model was that it was enforceable through the legal system. In 1997, the European Union responded directly to the privacy concerns caused by the technological advances in the telecommunications industry by supplementing the 1995 directive with the Telecommunications Privacy Directive (EU 1997). This directive aimed to protect users of digital television, landline telephones, mobile networks and other telecommunications systems (Privacy International 2011).

What history has shown is that after significant advancements are made to information technologies, it is highly likely that before long, peoples' views on personal privacy will evolve and people will begin to express a higher level of concern. In the past, these concerns have led to significant changes to legislation and the way in which these technologies are operated. It is likely that the same will be true of future cutting-edge technologies. ITS and, in particular, the location-based services (LBS) they offer have the potential to cause the next evolution in the way privacy is perceived.

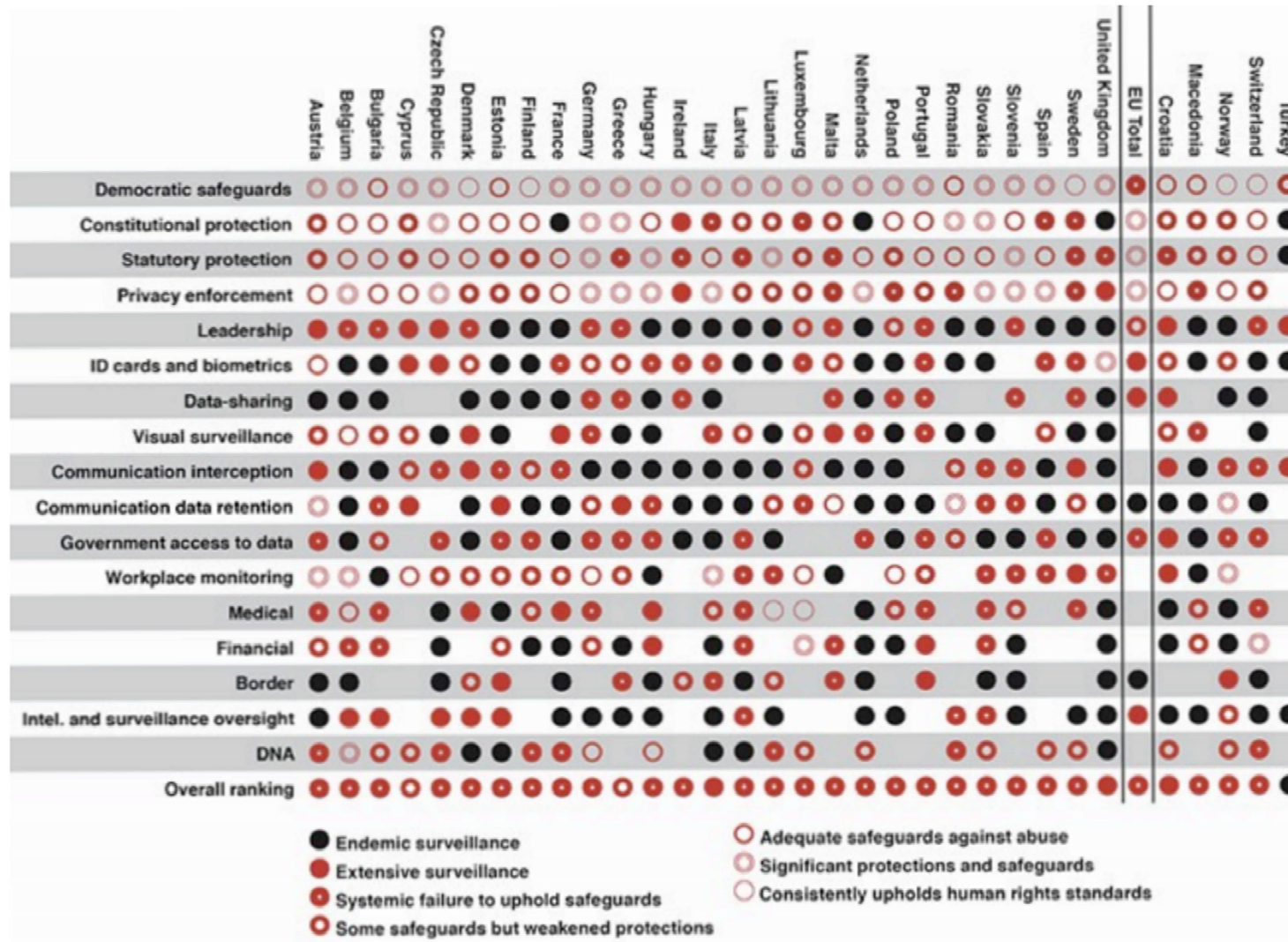
### *2.2.2. Different Levels of Legislation*

Although a look into the past shows a clear link between new technologies and a rise in the level of privacy concerns and subsequent legislation to help curb these concerns, what this does not highlight is the extent to which government policies and legislation varies from country to country. Figure 2-1 shows the results of an assessment of surveillance across Europe conducted by a UK based charity, Privacy International, who defend and promote the right of privacy across the world. The assessment demonstrates that even across the 27 EU member states in 2011, all of which are democracies, the acceptable level of privacy intrusion by country varies significantly.

Overall the results show that the UK and Italy accept the highest level of state intrusion. On the other hand the Greek and Cypriot states are shown to be the least intrusive. This assessment also shows that there does not appear to be that much consistency over the acceptable level of intrusion across different aspects. In the UK for example, the assessment shows that some significant protections and safeguards are in place with regards to ID cards and biometrics, but for virtually all of the other privacy aspects extensive surveillance was witnessed. It is interesting to note that in the UK there was significant media pressure against a proposal for national ID cards (BBC 2004, Politics.co.uk 2008 and Manchester Evening News 2010) and national polls showed a deteriorating national support for the idea which led to the proposals being cancelled in 2010 (Home Office 2011). National ID cards in the UK is a good example of how media outrage over privacy aspects and a lack of public support can prevent a project from being politically feasible in a democracy.

The differences in the level of intrusions in different countries and aspects highlights further that there appears to be no hard and fast rules for privacy. A look at the history of privacy concerns and the diversity in current level of intrusion across the EU shows that there is the very real prospect of the privacy aspects of a future ITS being deemed acceptable in one country but being deemed unacceptable in another. This research will need to focus on looking at the drivers of privacy concerns and investigate how many of these drivers could be present in future ITS and how they could alter future ITS users' behaviour in relation to using these technologies.

Figure 2-1 Assessment of surveillance across Europe (Privacy International 2011)



### 2.3. What are ‘ITS’

According to the Directive 2010/40/EU of the European Parliament on the framework for the deployment of Intelligent Transport Systems, Intelligent Transport Systems (ITS) are systems in which information and communication technologies are applied in the field of road transport, including infrastructure, vehicles and users, and in traffic management and mobility management, as well as for interfaces with other modes of transport (European Union 2010). Since the 1980s, ITS have been developed by both the private sector and academia and have attracted billions of dollars in funding for research and development (Weiland and Purser 2000 and Deakin et al. 2009).

Information is at the core of virtually all ITS, as they are based around the collection, processing, distribution and utilisation of information, hence there is the potential for privacy concerns to arise around the level of personal information some ITS require to operate. Due to their dependence on information, ITS can effectively be thought of as information chains. Although the concept of using an information chain to manage traffic networks is not new, the advance that ITS brings is the use of advance technologies at each stage of the information chain to increase efficiency. The stages of the information chain can be seen below (The World Road Association 2004):

1. Data Acquisition
2. Communication
3. Data Processing
4. Information Distribution
5. Information Utilisation

At each stage of the information chain, a wide range of ever changing technologies are used. The following sections will outline each stage and describe some of the technologies that are being used at each stage at the time of writing this thesis.

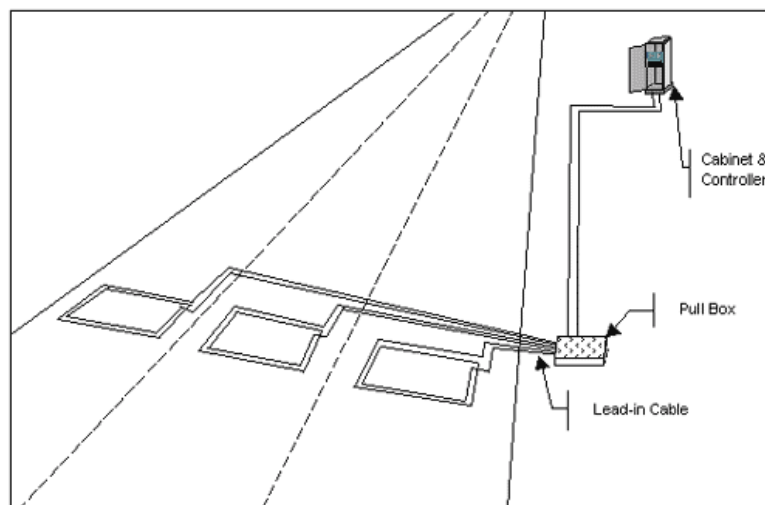


### 2.3.1. Data acquisition

The first stage in the information chain is the acquisition of the raw information the ITS will inform/act upon. The types of raw information collected are as wide and varied as the systems themselves, ranging from information about the current road conditions to an individual vehicle's current configuration. Numerous types of detectors/sensors are used by ITS to gain the required insights into the current transport situation. Some provide undetailed anonymous information that has historically attracted very low levels of privacy concerns (Ritchie et al. 2005). Others can collect highly detailed information that can identify the exact movements of individual vehicles and people which have in some cases raised privacy concerns (Michael et al. 2006).

How the amount/type of information required by an ITS might impact privacy concerns can be seen clearly by looking at three different detection methods used to gain information on traffic flows along a section of highway. Induction loop detectors have classically been used to measure the volume and speed of vehicles along a stretch of highway. An induction loop is an electromagnetic detection system which uses a moving magnet to induce an electrical current in a nearby wire when a vehicle passes over it (US DOT 2006). Figure 2-1 shows an example of an inductive loop configuration. Standard induction loops are not able measure travel times for longer distances or to survey the route-choice behaviour of drivers as each vehicle is completely anonymous and multiple induction loops cannot identify the movements of a specific vehicle (Friedrich et al. 2008). Due to the fact that virtually no identifiable information is detected by the induction loops, minimal privacy concerns have been raised about the technology's use.

**Figure 2-2 Example of Inductive Loop Configuration (Neudorff et al. 2003)**



A more complex method of gaining information about current traffic flows is by detecting Floating Car Data (FCD). FCD uses either on-board units equipped within vehicles or, in more recent times, mobile phones carried within vehicles to provide regular updates about the position of a vehicle (Turksma 2000). FCD is a valuable source of detailed up-to-date traffic information which can provide an understanding of individual travel behaviour and near real-time traffic performance data on any part of large networks (Fabritiis et al. 2008). However, unlike induction loops it is possible that FCD could be used as a surveillance method, although companies deploying FCD systems give assurances that all the data is made anonymous in their systems, or kept sufficiently secure to prevent abuses.

The consequence of this is that while most drivers value up-to-date traffic information, some are wary of the use of FCD, because of the potential for misuse (Rass et al. 2008). Security issues that have not been an issue in the past for FCD because most projects collected their data from fleet management systems but now a new source of data is becoming widely available from GPS units in private vehicles. Subsequently data security is proving crucial to gain acceptance from the vehicle owners. In particular, drivers have highlighted the fear that law enforcement will gain access to their speeds via calculations derived from FCD and be prosecuted for speeding (Rass et al. 2008).

**Figure 2-3 Photograph of CCTV Camera Used to Monitor Traffic Flow (Guardian 2011)**



Another method which after processing allows a more detailed breakdown of traffic flow is the use of close circuit television (CCTV). CCTV cameras collect images of the traffic travelling along the highway, which are transferred to a monitor/recording device, where they are available to be watched, processed and/or stored (Gill and Spriggs 2005). As every vehicle has a unique number plate, it is possible to identify an individual vehicle at various points along a highway (unlike with induction loop sensors) (Friedrich et al. 2008). As with FCD, the level of information provided by multiple CCTV cameras is significantly more detailed than that provided by induction loops, and systems that use CCTV data can easily be used for the surveillance of individuals and their vehicles. In fact, the technology is often used for that exact purpose within cities (Wood 2006). Although CCTV systems are currently in use in numerous countries around the globe, they are a lot more prevalent in some countries like the United Kingdom than others like Austria (Norris et al. 2004).

By comparing the level of privacy concerns associated with the collection of induction loop, CCTV and FCD data it is apparent that the type of information collected by an ITS will have a direct link to the level of privacy concerns associated to the technology. The less sensitive it is the less likely it will be for privacy concerns to be raised over the use of the ITS. The key point that should be taken forward about the data acquisition stage of an ITS is that the level of privacy concerns associated to future ITS are likely to be closely linked to the sensitivity of the data that is required from the user. As a result it is likely that a future ITS developer will need to strongly consider the privacy implications of requiring different types of information for their proposed ITS to operate.

### *2.3.2. Communication*

Once raw data has been collected by a sensor/device, the next stage in the ITS information chain is for this information to be communicated to another device, normally a computer for processing. This information will be communicated either through a wired/stationary method or through a wireless/mobile communication. Wired communications are more costly to install in financial terms, but generally then have low running costs. Wireless communications on the other hand tend to have lower set up costs, but greater operating costs (The World Road Association 2004). Traditionally, stationary sensors such as induction loop detectors and CCTV cameras will utilise wired communications whereas mobile sensors like the ones used to detect FCD are required to use wireless communications.

From an information security perspective, wired and wireless communications will present different challenges. In particular future ITS that will employ wireless sensory networks (Lewis 2004) will be presented with unique challenges over traditional networks. Firstly it is likely that the sensor nodes will be deployed in accessible locations and secondly the sensor nodes may have resource constraints which could limit their ability to store, process and transmit sensed data, which may introduce additional challenges for privacy preservation (Perrigg et al. 2004, Li et al. 2009).

The different privacy challenges faced by different communication methods could feasibly mean that different communication methods could generate different levels of privacy concerns amongst future ITS users. The impact different information transfer methods have on the acceptability of ITS is something that this research will need to investigate further and is something doesn't appear to have been addressed directly before in existing literature.

### *2.3.3.Data Processing*

The next stage in the information chain is to process the raw data that has been collected and communicated. This is often done remotely by a server/computer running bespoke software. The actual methodology used by each ITS will vary greatly and is only limited by the technology developers imagination and ability. Some of the techniques used for processing the raw data include data dictionaries, data fusion, data exchange and digital map matching (The World Road Association 2004).

Information from induction loop detectors is often sent via a wired communication to a traffic control system, often located close to a dynamic signalised junction. This control system is then responsible for processing information from one or more induction loops and adjusting the timings of the signals to optimise the capacity of the junction (Papageorgiou et al. 2003). Likewise, individual FCD from numerous different sources can be collected and combined by a remote server to produce a detailed breakdown of the traffic flow along a stretch of highway which can then in turn be used by other applications (Schäfer et al. 2002).

Raw CCTV data can also be processed by a computer, either in a remote location or within the camera itself to recognise all of the vehicle number plates that it views, and store/transmit this number plate information along with a location and time stamp (Lotufo et al. 1990). This automatic number plate recognition (ANPR) data can then either be stored or used for further processing. By combining ANPR data from a number of different cameras it is possible to produce information about an individual vehicle's movements and calculate the vehicle's average speed between two cameras, which can then be used for enforcement purposes. ANPR data can also be used for monitoring traffic flows and for road pricing (ANPR Tutorial 2012).

The London Congestion Charge (Litman 2006) uses ANPR data obtained from various CCTV cameras around the outskirts of central London to cross-check vehicles entering central London with a database of users who have paid to enter the area. If the identified number plate is not on this database, the number plate is then cross-referenced with a national database which contains the details of every vehicle's registered owner in the country to provide contact details for enforcement purposes (Leape 2006). By combining several different data sources, ITS such as those used for the London Congestion Charge are potentially creating highly sensitive information. It is very likely that the privacy concerns associated with combined datasets will be significantly greater than the concerns associated with the individual data sources.

This section shows that the privacy issues associated with data processing conducted by future ITS are similar to those linked to the data acquisition stage discussed earlier in the chapter. It is likely that for both stages, the level of concern generated by future ITS will be linked directly to the perceived sensitivity of the obtained data in the case of the acquisition stage and the perceived sensitivity of the data created during the processing stage. As mentioned in section 2.3.1 this is something that this research will need to focus particular attention on.

#### *2.3.4. Information Distribution and Utilisation*

Once the raw data has been processed, the ITS can then either distribute the processed information back to the appropriate stakeholders, utilise this information by causing some change to the transportation system or a combination of the two. As with the other stages in the information chain, numerous methods can be used to distribute the processed information back to travellers. The most common reason for distributing information back to road users is to either improve their safety by warning them of poor conditions ahead or to reduce congestion by either influencing the speed at which they drive or by diverting them onto less congested routes. Common distribution methods include conventional radio receivers, dynamic message signs (DMS) and the internet (The World Road Association 2004).

For years, car radios have been used to distribute up-to-date traffic information to motorists. In the UK a 24 hour, 365 day a year service called Traffic Radio is broadcast by the Highways Agency (Highways Agency 2013). This service aims to inform road users of current delays and road works by presenting information gained from a wide range of sources including the Agency's National Traffic Control Centre and Transport for London's Traffic Control Centre (Traffic Radio 2011).

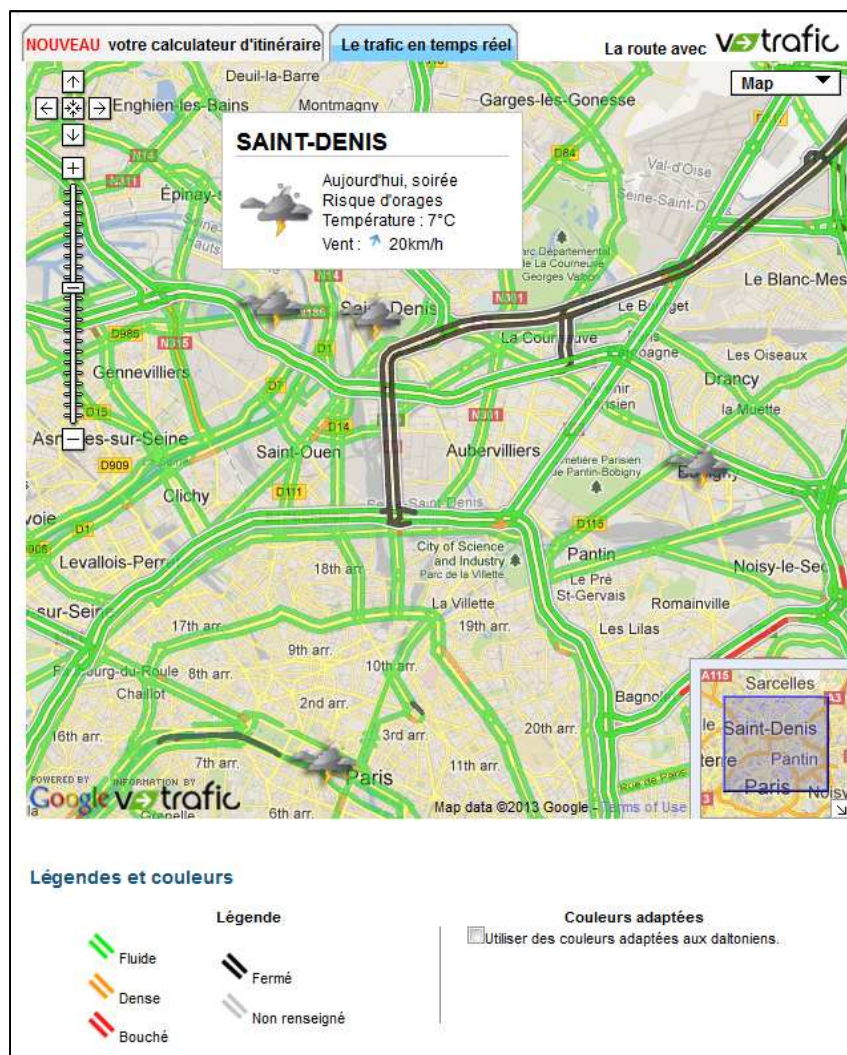
Another distribution method is the use of DMS, which are road signs with messages that can be changed in real time (Figure 2-4). Most often, messages are controlled remotely by a traffic management centre and their displays are continually monitored to ensure accuracy. The messages can be used to warn of congestion, accidents and incidents, road work information, speed limits for a specific stretch of highway and general driving advice (warnings against driving when tired or drunk) (Dudek 2004).

**Figure 2-4 Photograph of Several Dynamic Message Signs (DMS) in the UK (Techspan 2013)**



The Internet is another common method for distributing processed travel information. Many regions and cities have made real-time traffic flow maps, camera pictures, weather and road conditions, as well as static information such as traffic legislation and other relevant news, available on their websites (The World Road Association 2004). An example of such a website is the Meteo France Travel Website (Meteo France 2013). This site displays information about the current traffic flows on the highway network in France. Meteo France sources up-to-date traffic information which has been processed from FCD by a private company called Mediamobile, who in turn have obtained this information from Orange Network in France (Mediamobile 2012 and GPS Business News 2012). Meteo France then combine this up-to-date travel information with information about current weather conditions across the country and display this information on a digital map. Figure 2-5, shows a screenshot of the service. The website also allows users to get travel-time predictions under the current road conditions (Meteo France 2013).

Figure 2-5 Screenshot of Meteo France Travel Website (Meteo France 2013)



From a privacy perspective, virtually all of the information distributed back to travellers by current ITS is completely anonymous and usually the result of a series of anonymous data sources being combined together. However, if the personal data involved is perceived as being more sensitive, who the information is being distributed to could play a significant role in the level of privacy concerns generated. Earlier in this chapter, it was mentioned that one of the primary fears users have of FCD is that it will be distributed to law enforcement agencies (Rass et al 2008). It is probably also the case that future ITS user's will want to withhold different types of information from different groups of data holders. For example, a user may not mind their local garage having information about their driving behaviour but they not want their insurance company gaining access to the same information.

Although different in nature from most existing and future ITS in the sense that the most users may not have individually contributed their own personal information, Google Street View has caused controversy over the fact that it has made potentially sensitive personal information publically available. Google Street View is a technology featured on Google Maps that provides panoramic views of many streets around the world (Google Maps 2013). It should be noted that whilst the majority of users of the application have not contributed information to the data that is distributed publically, they have informed Google (a private company) of places of interest to themselves which they in turn can use for commercial gain.

Privacy advocates have objected to this feature, pointing to views of people engaging in activities visible from public property in which they do not wish to be seen publicly (USA Today 2007). Figure 2-6 is an example of a controversial image that has been uploaded onto the site for the world to see. It has even been reported that images displayed on Google Street View have led to married couples getting divorced (The Sun 2009). The concerns have led to several temporary bans of Street View in countries around the world including Austria (PHYS ORG 2010), Greece (BBC 2009) and Czech Republic (NBC News 2010) within the European Union.

This controversy highlights the potential issues a future ITS developer could face if their technology makes a user's personal information to the general public. It is likely that future ITS user's will trust different types of personal information with different groups of future data holders. This research will have to investigate further the impact different future data holders will have on the acceptability in privacy terms of future ITS.

Not all ITS distribute processed information back to stakeholders. Instead, they carry out actions that impact the way in which the transport network operates. This data utilisation can range from the automation of toll booths and the altering of traffic signal cycle times to the automatic enforcement of traffic offences. Section 2.1.3. has already touched upon two existing ITS that utilise processed information. The first, dynamic traffic signals, utilise the processed information from one or more induction loops to make alterations to the signal cycle times (Papageorgiou et al. 2003). This final act in the ITS information chain is automatic and provides a road user with the benefits associated with reducing congestion (time, cost and CO<sup>2</sup> savings). The example that was described in some detail was the London Congestion Charge's use of an ITS to automatically issue penalty notices to users who had not paid to enter central London. This automatic enforcement provides Transport for London (a government agency) with a large cost saving over manual enforcement, enabling them to spend the saved money on other services that would provide benefits to travellers within London.



**Figure 2-6 Controversial Google Street View Image (Telegraph 2013)**



Historically, the utilisation stage of the ITS information chain has not attracted large amounts of privacy concerns when compared to the earlier stages of the information chain. The likely rationale behind this is that by this stage in the information chain, the ITS has already collected, processed and communicated the future ITS user's personal information and it is now using the processed information to give a reward back to the ITS user. Therefore, by this stage in the information chain it is likely that most of the privacy concerns would already have been created and it is even possible that the reward offered by the information utilisation may offset some of the concerns generated earlier in the information chain.

In summary, this section has shown that the impact the distribution and utilisation stage of the ITS information chain has on the level of privacy concern is likely to depend entirely on which future data holders are going to gain access to a user's personal information. The perceived level of trust a future ITS user has in a future data holder is likely to vary from user to user and depend greatly on the characteristic of the future data holder. This is another factor that this research will have to investigate further. Unlike the other stages in the ITS information chain, the distribution and utilisation stages of an ITS potentially has the ability to offset the privacy impact of the earlier stages by offering a reward in return for the personal information provided by the future ITS user. Again, this is something that will need to be investigated further.

## 2.4. The Fears

You only have to look at historical proposals for road price charging to see the potential impact that privacy fears could have on future ITS systems (Ison and Rye 2005, Chartered Institute of Transport 1990,1992 and Jones and Hervik 1992). For example, in the 1980s, a proposal for electronic road pricing in Hong Kong was rejected by the public for amongst other reasons being an invasion of road users' privacy (Borins 1988, Pretty 1988 and Hau 1990). Advocates of road pricing systems will point to systems similar to the one proposed in Hong Kong that have been successfully implemented such as the Singapore Electronic Road Pricing (ERP) in 1998 (Tuan Seik 2000) and the London Congestion Charge in 2003 (Leape 2006) to suggest that the privacy concerns associated with the proposed Hong Kong System were unfounded.

The counter argument to this – and something this research will explore in more detail – is that the countries in which road pricing have been successfully implemented already had a history of using what some could consider privacy-invading technologies such as CCTV cameras on a mass scale. This indicates that either the citizens of these countries have grown used to being monitored and now find it acceptable, or that something in their citizens' cultural makeup makes them find monitoring more acceptable (Ison and Rye 2005 and PROGRESS Project 2004). Therefore, just because a scheme is acceptable in privacy terms in one country does not mean that it will be acceptable in privacy terms in another; the difference in the reactions to very similar road pricing schemes in London and Hong Kong can be cited as an example of this.

As some ITS technologies provide a mechanism for the real-time surveillance of an individual's movements and are also capable of combining and processing this information with other personal data about an individual throughout their lifetime (Glancy 1995), it is a very easy to conjure up scenarios in which supposedly innocent ITS systems can be used to physically track individuals. This in turn could lead to; the harassment of people found driving on the wrong side of town, the creation of advertising targeting people who use a competitor's car park, and the totalitarian monitoring of drivers of commercial vehicles (Gillmor 1993). For instance, after a relatively short period of tracking a vehicle, it may be possible to predict "*when someone is or is not at home; where they work, spend leisure time, go to church, and shop; what schools their children attend; where friends and associates live; whether they have been to see a doctor; and whether they attend political rallies*" (The Privacy Bulletin 1990).

Such scenarios become even more acute if it is probable that the use of a ITS will someday be mandatory for all, whether as a matter of law or of practicality (Agre 1994). The thought of the mandatory use of ITS systems is linked very closely with fears stated in Chapter 1 surrounding the possible panopticon effect that could be created by the use of ITS (Daly 2010). Rieman (1995) went as far as stating that the consequence of mandatory ITS use will be that individuals will alter their behaviour and travel with less freedom, and this will impact society as a whole. He links to a future world as portrayed in the science-fiction film, *Demolition Man*, where constant enforcement of totalitarian laws leads to individuals becoming more childlike and exempt of freedom of expression.

For these fears to be fulfilled, it needs to be the case that the use of ITS will cause citizens to change their travel behaviour. Conversely, for these fears to be unjust it needs to be proven that future ITS will not cause citizens to stop using their vehicles, or stop travelling with the same freedom that they currently enjoy. An example of this is that citizens should still feel that they are able to travel to potentially taboo (but legal) locations, such as political meetings, casinos or abortion clinics, without these actions having repercussions at a later date. At present, it is possible that a person's whereabouts can be compromised by innocent means, for example, somebody walking past a place of worship at the time of another person entering or exiting the building. In most cases however, it is felt that the risk of their whereabouts being compromised and having a detrimental effect on them, is outweighed by the reward for travelling to these locations. This principle will need to remain the same after the future ITS are implemented.

An important point to note is that ITS cannot be blamed for creating a Big Brother/panopticon society, if it is used to uphold the laws of a country, and therefore causes citizens behaviour to change to obedience of the law. The most obvious example of this would be a technology that communicates to a central control centre and issues speeding tickets every time vehicles were detected breaking the speed limit. It is likely that such a system would cause public and media outrage (at least initially), but this is arguably because of perceptions of the underlying laws, not that the technology is intruding on individual privacy.

Even if the use of future ITS systems is not mandatory (either legally or practically) privacy concerns could still lead to a system failing if the required uptake rate of the technology is not met, for example, if a completely voluntary ITS such as personal satellite navigation units (which are fairly common place across the European Union (Axon et al. 2012)) required a certain uptake rate amongst road users for the technology to function efficiently. If the technology is then heavily associated with privacy concerns, it could lead to not enough people buying/using the technology to meet the required uptake rates for the system operate effectively and the technology would then fail because of privacy concerns. Although satellite navigation units do not require a certain user uptake rate to operate efficiently, potentially a lot of the future ITS systems that will be discussed later do.

In summary, the fears about future transport technologies causing a Big Brother/panopticon state could be justified if a ITS system is made mandatory and a citizen's privacy concerns prevent them from carrying out a lawful action that they would have carried out if the new technology had not have been implemented. In addition to this, privacy concerns could impact the feasibility of non-mandatory ITS that require high uptake rates to operate effectively. This is especially true if the developers of these technologies do not consider the privacy impacts of their systems. Both of these cases rely on road users acting in a privacy-preserving manner. Therefore, although it is important to consider a road user's level of concern relating to a proposed ITS it is more important to consider their likely future actions with regards to the ITS, as the expressed fears will only come to fruition if citizens act on their privacy concerns.

## 2.5. The Current Situation

Although there are privacy concerns associated to some degree with all ITS, since the 1980s they have been used with growing frequency across the globe to solve a wide range of different problems (Weiland and Purser 2000). The fact that these systems are currently used shows that, in most cases, the benefits offered by the ITS outweigh the privacy concerns associated with them. Very few ITS systems have been deemed completely unacceptable because of privacy invasions (Hong Kong Road Pricing) but several proposed systems have had to be modified to alleviated privacy concerns expressed about the proposed ITS. Due to privacy concerns, the Netherlands was forced to offer an anonymous version of their OV-chipkaart (Griffioen 2011). The OV-chipkaart is a smart card system that facilitates the payment of trips on all public transport in the Netherlands. Users now have the choice between using an anonymous 'pay as you go' card which requires topping up anonymously or a card that is linked directly to a user's bank account which allows them to be billed directly for any trips they make. Other benefits of using the card linked to their personal details is that the card can be cancelled if it is lost or stolen and some users, such as students and pensioners get discounts on their fares which they would not receive if they used the anonymous card (OV-chipkaart 2013).

Even with the introduction of the ‘anonymous’ OV-chipkaart, the privacy concerns associated with the technology have not been completely eradicated and in February 2013 there was a debate in the Dutch House of Representatives where the following points were made (Privacy First 2013):

- That the ‘anonymous’ OV-chipkaart was not actually anonymous because it contains a unique identification number in the radio frequency identification (RFID ) chip (Finkenzeller 2010) that is embedded within the card which enables travellers to be identified and tracked afterwards through the linking of transactions.
- That as long as truly anonymous cards do not exist printed travel tickets should remain available to travellers who want to remain anonymous.
- That a special anonymous discount card should be introduced for children and the elderly.
- That the current retention period for OV-chipkaart data should be reduced to an absolute minimum with travellers given the option to erase their travel history at any given moment (Privacy First 2013).

As ITS systems have become more complex and have required the collection of greater volumes of personal information, the privacy concerns associated with the systems have increased. It has also become clear that a system that is acceptable in one country is not always acceptable in the exact form in another; several examples of this are given later in this chapter. Therefore, to help predict where future difficulties may lie, it is important to examine the privacy aspects of a range of current ITS systems.

### *2.5.1. Current ITS Examples*

Table 2-1 highlights the benefits and personal information requirements of five diverse ITS that have been implemented across the European Union. Of the five system types in Table 2-1, road-pricing systems have proven to be most controversial in privacy terms. Not only was the road pricing scheme in Hong Kong deemed unacceptable because of concerns over privacy, but other forms of automated travel pricing have also proved controversial, such as automated toll booths and smart travel cards.

In the United States, automated toll booths that use RFID tags have caused controversy as the data they stored has not only been used for its intended primary purpose (billing) but also as evidence in numerous legal trials including divorce hearings (MSNBC 2007). As mentioned earlier, the OV-chipkaart in the Netherlands has also caused controversy because with the data they store it is possible to identify an individual’s movements around the country/city (Prins et al. 2011).

The ‘Oyster’ card in London, UK which is similar to the OV-chipkaart has also been criticised for being an invasion of privacy (BBC 2003), especially as law enforcement regularly access Transport for London’s Oyster card database in search of personal information on travellers (Dunn 2012) with national security agencies having been reported as wanting to have access to the whole database (Guardian 2008). One prominent European politician has even stated that he refused to buy an Oyster card fearing that it could be used to spy on him (Telegraph 2013)

It is probably of no coincidence (something this research will investigate) that these automated travel pricing systems have caused more controversy than most other ITS that are currently in existence. This is because they combine at least two sensitive data sources such as a register of vehicle owners with information about the vehicles movements. By doing this, these systems create a new database of information that could potentially be perceived as highly sensitive by some.

If this information fell into the wrong hands, any number of worst case scenarios could come to fruition. Several other existing ITS systems use information that identifies individual vehicles (see ANPR and FCD both discussed earlier) but to date the privacy concerns associated with these technologies have been limited because the vehicles identifications have not been combined with the owner information. This indicates that the exact type of data a system requires to operate will be a key factor behind whether privacy will limit that system’s uptake.

### *2.5.1. Differences in Current Regulations*

Some of the previous sections have touched on the fact that some ITS systems that have been acceptable in some countries have been deemed unacceptable in others (Section 2.4.). This could be for a variety of different reasons, but the primary one for current ITS is that the legal doctrine concerning the privacy aspects of ITS varies quite significantly even across the European Union, as demonstrated by Figure 2-1. A good example of these discrepancies in regulations can be seen from how different countries regulate the use of ANPR data. Although there are numerous benefits to the end user, such as improved safety (due to the police enforcement) and reduced journey times (due to the traffic control and electronic toll collection), not every country feels that these benefits outweigh the loss of their personal information (Guardian 2003). This is demonstrated by the fact that some countries that use ANPR have legal requirements that limit the extent to which APNR data can be used, and how long the data obtained by ANPR can be kept.

**Table 2-1 Benefits and Information Requirement for a Range of Current ITS**

<b>ITS Type</b>	<b>Example</b>	<b>Information Required</b>	<b>Data Stored / Holder</b>	<b>Benefits</b>
Signal Control	Dynamic Signal Control (Dudek 2004)	Anonymous Loop Detector Information	Anonymous Loop Data Information is Stored by the Signal Operator normally a Local Authority	Reduced Congestion (Time, Cost and Environmental Savings)
Collison Warnings	Adaptive Cruise Control (Vahidi and Eskandarian 2003)	Radar sensor mounted to front of vehicle detects the proximity of the vehicle in front	No information is stored or given away	Improved Safety
Automotive Navigation System	Satellite Navigation Unit (SatNav Forensics 2013)	Regular update of a vehicles current position	No information is stored or given away	Time Saving
Real Time Traffic Information	Meteo France Travel Information (Meteo France 2013)	Anonymous FCD provided by Orange network users in France and current weather conditions	Anonymous FCD is stored by both Orange and Mediamobile (GPS Business News 2012)	Reduced Congestion (Time, Cost and Environmental Savings)
Automated Travel Pricing	London Congestion Charging (Winters 2004)	Time, location and license plate details of vehicles entering/exiting congestion charge area	Data is stored by Transport for London and checked with a database of users who have paid to enter the area. License plates that are not on this register are then cross referenced with a register of owners so that a penalty notice can be issued.	Reduced Congestion (Time, Cost and Environmental Savings)

In Germany, for example, on 11 March 2008, the Federal Constitutional Court of Germany ruled that some areas of the laws which permitted the use of ANPR violated the German citizen's right to privacy (Bundesverfassungsgericht 2008). As a consequence, it was made illegal to store any information which was not for any pre-determined use (such as the enforcement of speeding laws or the tracking of suspected criminals). The UK and the US, on the other hand, have extensive ANPR networks that allow the police and security services to track all car movements around the country. Unlike in Germany, this information can be used for any purpose including analysis for improvements or intelligence and for use as evidence in legal hearings (Guardian 2007). In the UK, this information will be stored in the National ANPR Data Centre for two years (Independent 2005), whereas in the US, there is no time limit on the length of time this information can be kept, and this information can even be shared with third parties (New York Times 2010).

The different levels of legislation with regards to ANPR is just one example that demonstrates that the data required by both existing and future ITS could lead to privacy concerns, which in the case of Germany led to the use of the ITS being limited. It is not only the use of ANPR that varies significantly by country; so does the use of electronic toll booths (Bennet et al 2002) and CCTV (Gras 2002). There is no conclusive evidence that explains the differences in not only different countries regulations but also their citizen's general perception of privacy. Some argue that previous experiences shape a nation's perception, as a consequence the UK and US are tolerant of more surveillance because of recent terrorist incidents (Haggerty and Gazso 2005). It is also often reported that one of the main reasons for Germany's more protective stance is the abuse of surveillance systems carried out by the Nazi party (Whitman 2003).

It is also argued that once individuals experience being monitored by one technology they are then more likely to accept being monitored by other methods, hence why road pricing was deemed acceptable in London but not in some other countries as the residents were already used to being monitored by a wide scale CCTV network (Ison and Rye 2005). On the other hand, others have argued that an individual's views on privacy are linked more heavily to their cultural upbringing than their experiences (Bellman et al. 2004 and Millberg et al. 2000). This is something that this research will explore in more detail.

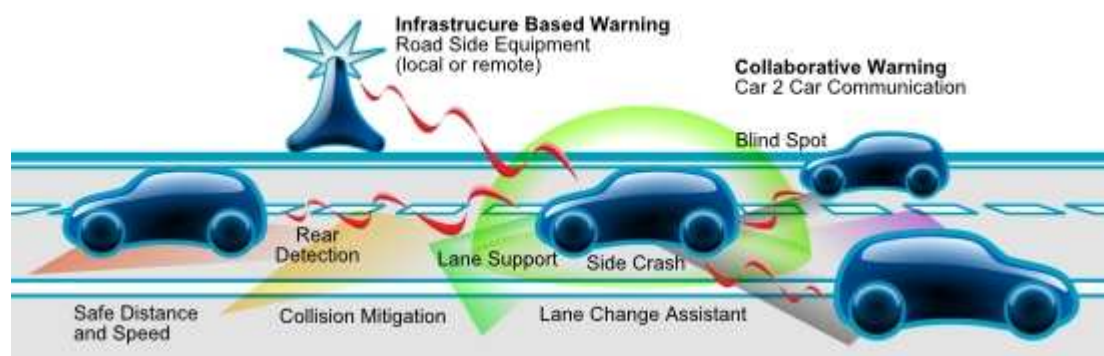


## 2.6. Future ITS

In the future, it is expected that ITS systems will be able to acquire, communicate, process and utilise more data at a higher frequency. This will enable more advanced ITS such as cooperative transport systems to come in to operation. Cooperative systems will enable rapid Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications. These new communications could range from vehicles giving other vehicles their exact position in real-time to significantly improve safety, to individual vehicles informing the infrastructure of their destination, number of people travelling, propensity to pay and the trip purpose to optimise the transport network (CVIS 2012).

In 2006, the European Commission launched three projects as part of their 6<sup>th</sup> Framework Program that looked specifically at using cooperative systems to increase road safety and traffic efficiency (Toulminet et al. 2008). The CVIS (Cooperative Vehicle Infrastructure Systems) project aimed to design and test the core technologies required for cooperative systems (CVIS 2012). As Figure 2-7 shows, the SAFESPOT project focused on using cooperative communications to significantly improve safety conditions for road users (SAFESPOT 2013). The third project, COOPERS (COOPERative Systems for Intelligent Road Safety) investigated how road operators could utilise cooperative systems (COOPERS 2013).

**Figure 2-7 Diagram Showing How Cooperative Transport Systems Could Improve Road Safety (SAFESPOT 2013)**



All three projects demonstrated that cooperative transport systems are not only achievable in technology terms, but that they would offer some genuine benefits, especially with regards to safety and efficiency improvements. Other than a couple of questions in an end-user survey conducted as part of the CVIS project, these projects spent very little time considering how potential privacy concerns associated to these technologies could potentially limit their uptake (CVIS 2007). The results of the CVIS end-user survey suggested that any privacy concerns associated with future cooperative transport would be outweighed by the benefits on offer. It must be stressed, however, that the topic was not explored in any great detail and the survey sample comprised mainly of car enthusiasts.

At the same time as funding the three cooperative transport research projects outlined above, the European Commission also funded several projects investigating methods for making the proposed communications within a cooperative system as secure as possible from a technological/encryption standpoint (PRECOISA 2013, Sevecom 2013, EVITA 2013, Oversee 2013 and PRESERVE 2013). Although these projects could potentially help alleviate some of the privacy fears associated with future ITS, none of these research projects have actually considered how willing the future ITS users would be to share their personal information, or which factors would influence their privacy concerns. They have all instead looked at what is possible technologically to make any shared data as secure and anonymous as possible.

It could be argued, however, that the public's perceptions of how secure these communications are (which could be very different to the actual level of security), how sensitive they feel the information they are giving away is, and how safe they feel their personal information is in other stakeholders hands will play a more significant role in a future ITS user's actual behaviour. Therefore, it needs to be investigated whether despite the numerous benefits offered by cooperative systems, they are outweighed by concerns caused by the new information flows they would create. This is something that this research will attempt to address.

## 2.7. Summary

This chapter has shown that although the term 'privacy' is hard to precisely define. A look back at recent history has shown that after significant IT advances, it is likely that peoples' views on personal privacy will evolve and people will begin to express a higher level of concern. In the past, these concerns have led to significant changes to legislation and the way in which these technologies are operated, so it is definitely feasible that the same will happen with future ITS systems.

This chapter has also highlighted how all ITS (both existing and future) rely heavily on information to operate efficiently. It is the ever-growing demand for more information about the transport network which has led to a rise in privacy concerns associated to ITS. It has been shown that the different stages of the ITS information chain have the potential to create privacy concerns for different reasons. The variables that have been highlighted as being likely to impact a user's willingness to use a future ITS include the type of information the ITS intends to collect, whether it will be combined with other information types which could increase the sensitivity of the information, how the information will be communicated between the various stages of the information chain and who can gain access to both the raw and processed information used by the ITS.

In order for future ITS to be deemed unacceptable in 'privacy' terms, it is not a case that the public will have to be concerned about the technology, but that they will act in a manner that protects their personal information. This means that a user will either travel with less freedom if the use of an ITS is mandatory or opt not use an ITS if it is not made mandatory. It is therefore necessary that this research considers future users' likely privacy behaviour, not just their level of concern. This is something that has not been heavily investigated within the transportation field.

The majority of the 'privacy' research within the transport field to date has focused on finding technological methods for making data more secure and anonymous. Although it is likely that secure and anonymous communications will alleviate some of the privacy concerns associated with future ITS, it is currently unknown whether a future ITS user's perceptions of the privacy risks and their likely privacy behaviour will be altered sufficiently by these technological advances. The dearth of knowledge about which factors will influence a future ITS user's actual privacy decision-making is something that this research will attempt to address. It is feasible that current attempts at making ITS communications secure and anonymous either fall short or potentially even overshoot the mark, as it is possible that a future ITS user's privacy concerns are not linked to their data being anonymous. This research aims to start building up a more detailed picture of what drives users' actual privacy behaviour in relation to future ITS, so that ITS developers can focus on the privacy aspects which have the greatest impact.



### **3. Privacy Concern, Intention and Actual Behaviour**

#### **3.1. Introduction**

The previous two chapters have demonstrated how privacy concerns and ITS are closely interwoven. This chapter aims to take the discussion a step further and examine individuals' privacy decision-making, in an attempt to investigate the factors which will determine whether a variety of different future ITS will cause potential users to act in a privacy protecting manner. The 'Fears' section of Chapter 1 has shown that the privacy fears associated with future ITS will only come to fruition if people actually travel with less freedom than they do at present. To investigate the point at which future ITS users will travel with less freedom, this chapter will look at three different areas; their level of concern, their stated behavioural intention and their actual behaviour when confronted with a privacy scenario.

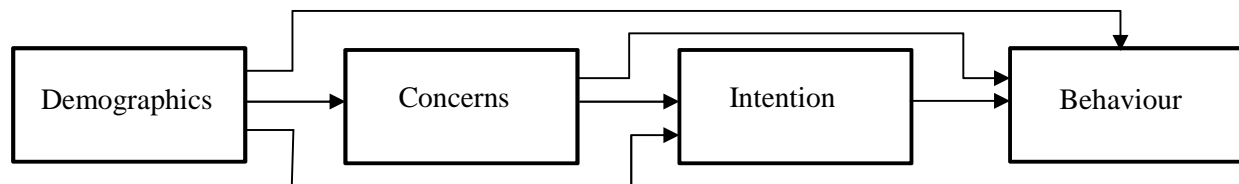
#### **3.2. Research Areas**

As the term 'privacy' is so broad, it impacts many different academic fields, including but not limited to law, social science, philosophy and economics. The most relevant research for future ITS has been conducted in the field of e-commerce where social and economic theories have been used to investigate the privacy aspects of existing and future web usage. The majority of the research in this area has focused on measuring the level of privacy concern associated with the use of websites and investigating what influences these concerns (Fox et al. 2000, Phelps et al. 2000 and Wallis 2007). A significantly smaller amount of research has investigated peoples' actual privacy behaviour when using e-commerce services (Hui et al. 2007 and Spiekermann et al. 2001). This research into actual behaviour has shown that there is potentially a significant disconnect between people being concerned about a technology and them actually acting upon this concern (Berendt et al. 2005). It is therefore of the utmost importance that this research not only considers the factors influencing concern levels, but also the factors that will influence a person's actual privacy behaviour.

As this research is seeking to see whether privacy will limit the uptake of technologies that have not been created yet, it will also be important to explore the link between a person's stated behavioural intention and their actual behaviour. This will enable conclusions to be made about future ITS user's likely actual behaviour by investigating their stated behavioural intention.

This research will therefore look in detail at three distinct aspects of privacy – concern, behavioural intention and actual behaviour – and the links between the three aspects. The likely connections between the three aspects are shown in Figure 3-1, where the arrows indicate the predictions of how each of the aspects will impact one another. This research will seek to explore these areas and connections in significant detail.

**Figure 3-1 The Link Between Concerns, Intention and Behaviour**



### 3.3. Privacy Concerns

The previous chapter identified that there is a clear trend of new information technologies raising the levels of privacy concerns amongst the public. Since the mid 1990s, several pieces of research have looked into the root causes of privacy concerns that new technologies appear to exacerbate. Work conducted by Smith, Millberg and Burke (1996) developed the ‘Concerns for Information Privacy’ (CFIP) framework. It identified and measured the primary dimensions of individuals’ concerns about information privacy practices. The result was a 15-item instrument which is split into four distinct dimensions. The instrument was developed by a process that included examinations of privacy literature, experience surveys, focus groups, and the use of expert judges.

The four distinct areas that the CFIP instrument measures are: Collection, Errors, Unauthorised Secondary Use and Improper Access. The Collection dimension revolves around the idea that individuals often perceive that great quantities of their personal data are being accumulated (whether it is true or not) and they resent this. The Error dimension considers individuals’ fears that protections against deliberate and accidental errors in their stored personal data are inadequate.

The Unauthorised Secondary Access dimension stems from fears that information collected from individuals for one purpose is being used for another, without authorisation from the data owner (either by the same organisation or an independent third party). The final dimension, Improper Access, involves concerns that peoples’ personal data is readily available to others not properly authorised to view or work with this data.

Initial findings provided by Smith, Millberg and Burke (1996) suggest that there may be a hierarchy of concern regarding the various dimensions. Their research identified Improper Access and Unauthorised Secondary Use as the areas of high concern, although there were differences within these areas, as samples ranked them at varying levels of importance. Collection and Errors were identified as areas of less concern.

Another piece of research (Bellman et al. 2004) used the CFIP instrument to see whether privacy concerns were different in different countries. The results of this survey indicated a clearer hierarchy, with Secondary Use being the biggest concern globally, and Improper Access being ranked just behind. There is then a big jump until either Collection or Errors is ranked last (depending on the country sampled).

The Internet Users' Information Privacy Concerns (IUIPC) framework (Malhotra et al. 2004) took a different approach to addressing peoples' privacy concerns. As a result, they found it possible to characterise IUIPC in terms of three factors: Collection, Control and Awareness. The Collection factor looks at individuals' concerns about the amount of information being collected by an organisation (same as CFIP). The Control factor sees whether it is important that people have control over their personal data and what organisations do with it. This takes a slightly different view to CFIP. The final factor, Awareness, looks at how important it is that people know what their personal information is used for.

Malhotra, Kim and Agarwal (2004) surveyed a sample of people using their IUIPC framework, in combination with the CPIF framework. They discovered that users rated Awareness as the most important privacy factor, marginally higher than Secondary Use. The Control factor was shown to have a similar importance to the Collection factor, which is in the lower tier of concerns. A combination of the CFIP and IUIPC and their associated surveys have shown that privacy concerns associated with any scenario can be split into two tiers, with three areas of concern in each. These concerns should be equally relevant to ITS. The breakdown of the areas of concern can be seen in Table 3-1.

In terms of future ITS, this indicates that the major causes of concern will be a user's fear that their personal information will either be used in an unauthorised way by the original data holder, or that a third party will acquire their data. It is also fair to say that the user will be more scared of the unknown (and will assume the worst), so if security devices are put into place to stop Secondary Use and Improper Access, the user of the ITS needs to be told about them.

**Table 3-1 Breakdown of the Areas of People’s Privacy Concerns**

<b>Rank</b>	<b>Tier</b>	<b>Concern</b>	<b>Details</b>
1	1	Awareness	The fact the user does not know what the authorised use of their personal data is
2	1	Secondary Use	The fact the user is not confident that their personal data will only be used for what they authorised it for
3	1	Improper Access	The fact that the data may be stolen/viewed by someone who is not authorised
4	2	Control	The fact that users want to be in control over who/what their personal data is used for
5	2	Collection	Fears over the fact that too much of their personal data is being collected
6	2	Errors	Fears that their personal data might contain accidental or deliberate errors

### *3.3.1. Fundamentalists, Pragmatics and the Unconcerned*

Most of the early work studying general privacy concerns was conducted by Alan Westin, between 1978 and 2004, in which he carried out over 30 privacy-related surveys (Westin 2003). These surveys covered general privacy, consumer privacy, medical privacy, and other privacy-related areas. This literature review has only considered the surveys he conducted into general privacy (as the results of these surveys are the most transferable to the transport) and in particular, the findings of five surveys identified in Table 3-2. A detailed analysis of these surveys has been carried out by Kumarguru (2005).

**Table 3-2 Details of Westin’s Surveys Considered in this Report**

<b>Year</b>	<b>Name of Study</b>
1990	Equifax Executive Summary
1996	Equifax-Harris Consumer Privacy Survey
2000	Privacy On & Off the Internet: What Consumers Want
2001	Privacy On & Off the Internet: What Consumers Want
2003	Most People Are ‘Privacy Pragmatists’ Who, While Concerned about Privacy, Will Sometimes Trade it Off for Benefits



The common interest that these five surveys have is that they all use what Westin calls his ‘General Privacy Concern Index’. This index categorises a person’s views on privacy into one of three groups: The Fundamentalists, The Pragmatics and The Unconcerned.

Fundamentalists are generally distrustful of organisations that ask for their personal information and are in favour of new laws and regulatory action to spell out privacy rights and provide enforceable remedies. Fundamentalists generally choose privacy controls over consumer-service benefits, when these compete with each other.

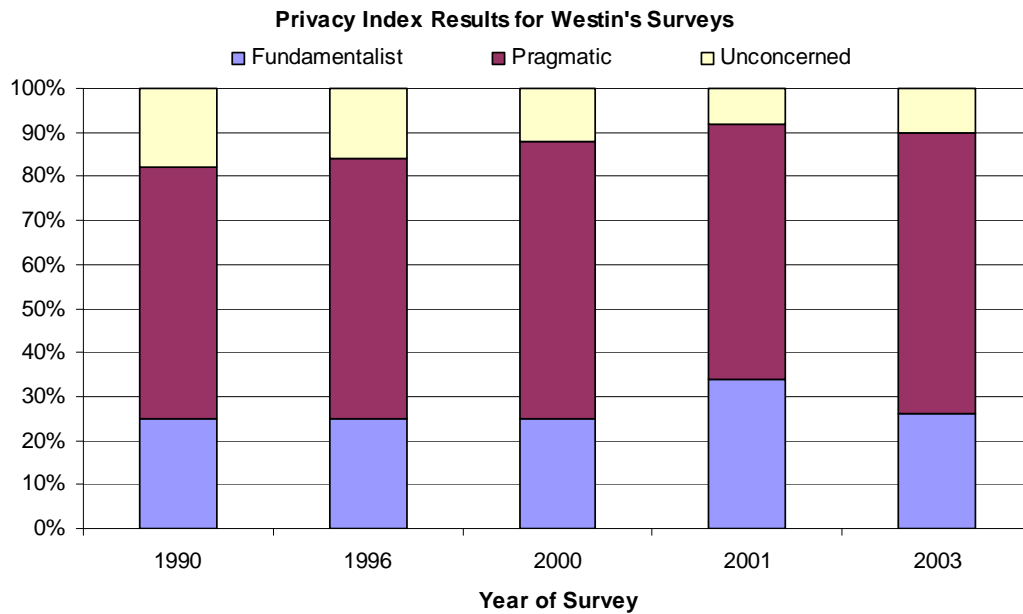
Pragmatics weigh the benefits of various consumer opportunities and services against their privacy concerns. They believe that organisations or governments should ‘earn’ the public’s trust, rather than assume automatically that they have it. Most importantly, they want the right to opt-out of giving away their personal information.

The Unconcerned are generally trustful of organisations collecting their personal information and are ready to forego privacy claims to secure benefits. They are not in favour of the enactment of new privacy laws and regulations (Kumaraguru 2005).

To determine which group a person falls into, Westin uses a standard framework. The surveys each split the sample into Fundamentalists, Pragmatics and Unconcerned. Figure 3-2 shows how the sample of each survey was distributed.

Several trends can be drawn from the results shown in Figure 3-2. Firstly, the more recent surveys indicate that roughly 63% of populations are privacy Pragmatics, 27% are privacy Fundamentalists and 10% are Unconcerned. These surveys also indicate that the general public are becoming more concerned about privacy, as there has been a shift, with the privacy Unconcerned turning into privacy Pragmatics. The number of privacy Fundamentalist has remained constant, except for a slight inconsistency immediately after the September 11 terrorist attacks in 2001.

It needs to be taken into consideration that all these results are for surveys that were conducted in the US and it is quite likely that they have a more liberal view on privacy than some other countries (Bellman et al. 2004). Also, the most recent survey is ten years old, so it is possible that there have been further attitude shifts in the period since.

**Figure 3-2 Privacy Index Results for Westin's Surveys**

### 3.3.2. Influence of Demographics

Other relevant surveys that have examined privacy concerns include the 2007 Community Attitudes Towards Privacy Study, which was conducted by Wallis Consulting Group and commissioned by the Office of the Privacy Commissioner, Australia (Wallis 2007). This survey shows that peoples' privacy concerns increase with age and education level. Another study (Phelps et al. 2000), disagreed with the fact that peoples' overall privacy concerns increase with education level; they suggest the opposite is true. Additionally in the Wallis Consulting Group survey (Wallis 2007), it is shown that certain privacy concerns have their own specific demographic influences, for example, people living in urban areas have more trust in retailers and young people are more concerned about giving away their home phone numbers and address (which is against the previous evidence that young people are less concerned about privacy issues).

A survey conducted by The Pew Internet and American Life Project into trust and privacy online (Fox et al. 2000) looked at how peoples' privacy perceptions varied according to demographics and internet experience. This study confirms the age bias indicated in the Wallis Consulting Group Survey. It also goes on to show that in the US, ethnic minorities are likely to have increased privacy concerns, as are females over males, although it also identifies that privacy fears associated with internet use decrease significantly with user experience.

Studies have also been conducted into whether privacy concerns vary between nations. Milberg, Smith and Burke (2000) found during their research that cultural values were associated with differences in privacy concerns. The term ‘cultural value’ was taken from work conducted by Hofstede (1980) which explored the differences in beliefs held by citizens of different nations even when other differences such as economics, politics, technology and other external pressures had been eroded. He found that a nation’s cultural value could be defined by four distinct dimensions; Power Distance, Individualism, Masculinity and Uncertainty Avoidance (Hofstede 2000)

The Power Distance Index (PDI) measures the extent to which the less powerful members of organisations and institutions (such as a family) accept and expect that power is distributed unequally. This represents inequality, but defined from below, not from above. It suggests that a society’s level of inequality is accepted by the followers as much as by the leaders. For example, a nation with a high PDI is likely to have a much larger gap between the wealthy and poor than a country with a low PDI score.

Individualism (IND) measures the degree to which individuals in nations are integrated into groups. Countries with a high IND score are likely to comprise populations in which the ties between individuals are loose; everyone is expected to look after him/herself and his/her immediate family. Conversely, countries with low IND scores are likely to be nations in which people integrated into strong, cohesive groups, often extended families (with uncles, aunts and grandparents) which continue protecting them in exchange for unquestioning loyalty.

Masculinity (MAS) refers to whether a particular national culture has more ‘masculine’ or ‘feminine’ traits. A high MAS score will typically belong to a country in which the population are assertive, materialistic, and competitive. In a country with a low MAS, score the opposite is likely to be true.

The Uncertainty Avoidance Index (UAI) deals with a society’s tolerance for uncertainty and ambiguity. It indicates to what extent a culture programs its members to feel either uncomfortable or comfortable with change. Countries with a high UAI score try to minimise the possibility of uncertainty and change by applying strict laws and rules. Again, the opposite can be said of a country with a low UAI score (Hofstede 2005).

Bellman, Johnson, Korbin and Lohse (2004) also found during their research that cultural values were associated with differences in privacy concerns. However, unlike Milberg et al. (2000) who found that concerns about information privacy were positively associated with Power Distance, Individualism, Masculinity and negatively associated with Uncertainty Avoidance they found that three of the Hofstede indices (Power Distance, Individualism, Masculinity) had an influence on privacy concerns in the opposite direction to that reported by Milberg et al. (2000). The influence of the fourth index (Uncertainty Avoidance) was not significant

The negative association between individualism and privacy concern found in the study by Bellman et al. (2004) is also supported by other cross-cultural research, which has found that people from cultures with high individualism are comfortable with disclosing higher levels of private information (Lewin 1936 and Ting- Toomey 1991). Two other examples of research that have shown this phenomenon are; Maynard and Taylor (1996) who found that students from Japan (IND = 46) had higher levels of privacy concern than students from the United States (IND = 91), and a privacy survey conducted by IBM (1999), which found that citizens from the United States were twice as likely to be classified as “low” in privacy concern compared to citizens from Germany (IND = 67).

The variance in these results show that whilst someone’s cultural values might influence their level of privacy concern, other cross-country differences could also have an impact on someone’s level of privacy concern. For example, it has been shown that citizens from countries with a history of having high government regulation of information privacy have high levels of privacy concerns and express a desire for even stronger regulation (Millberg et al. 2000 and Bellman et al. 2004).

From these surveys conducted on general privacy, it is clear that someone who has the following characteristics; from a country with strong privacy regulation and low individualism, elderly, female, live in a rural area, is in an ethnic minority; and has little experience of using existing ITS systems are more likely to be a privacy fundamentalist than someone who is; from a country with low privacy regulation and high individualism, young, male, in an ethnic majority, live in urban areas and have significant of experience of using existing ITS (as long as they have not had any bad privacy experiences). Previous surveys have shown a mixed response to the influence of education levels on privacy concerns.

### 3.4. Behavioural Intention

The previous sections of this chapter have highlighted the causes and variance of peoples' privacy concerns. It has also been clarified earlier that in order for the privacy fears associated with future ITS to come to fruition, peoples' actual behaviour will have to be influenced. It is therefore important to examine the influences behind a person's stated behavioural intention and their actual behaviour. It is not always the case that being concerned about something will actually result in someone altering their actions (Berendt et al. 2004).

This is an important aspect when considering whether the privacy fears associated with future ITS are justified, because although the users may have privacy concerns about future ITS, they could be ignored by the user in order to reap the benefits on offer. In choosing whether to disclose personal information when confronted with a privacy scenario, the future ITS user will have to make a complex and often ambiguous and subconscious trade-off. The user will want to protect the security of their data and avoid the misuse of their information. However, the user will also want to benefit from sharing their personal data with peers and third parties. The outcome of the scenario will come down to whether the user feels that the benefit of the reward on offer outweighs potential misuse of their information. This trade-off can be seen as a form of cost-benefit analysis, which naturally would fall into the realm of economics (Aquisiti 2010).

As this research is seeking to make judgements on the privacy aspects of technologies that are yet to be invented, it is necessary for it to consider users stated behavioural intention with regards to future ITS as well as their actual behaviour when faced with an existing privacy scenario. The rationale behind this is that the future ITS user can state whether they would be willing to disclose their personal information to a future ITS long before it is actually developed. It will also be possible for this research to explore the link between stated behavioural intention and actual behaviour for privacy scenarios that already exist. This will help conclusions to be made about a future ITS user's likely actual behaviour with regards to various undeveloped ITS.

Very little research has explored the factors that influence peoples' stated privacy intention. Virtually all previous research, especially within the field of transportation, has explored a user's level of privacy concern and the factors that impact it. Some research within the field of e-commerce has explored peoples' actual behaviour and the influencing factors (discussed later in this chapter) but this is not directly relevant to what this research is trying to achieve because it explores peoples' actual behaviour in relation to technologies that already exist.

As a consequence, this research will attempt to fill some of the void that exists in the existing literature by finding information about the influencing factors of peoples' stated privacy intention and how it could subsequently be used as a predictor of actual behaviour.

#### *3.4.1. Rational Privacy Decision-Making*

Since the late 1970s, economists have been interested in privacy (Posner 1978, Posner 1981 and Stigler 1980). From this point, some have used the dichotomy between privacy attitudes and actual privacy behaviour (Berendt et al. 2004, Hann et al. 2002) to claim that individuals are acting rationally when it comes to privacy. Under this view, individuals may accept small rewards for giving away information, because they expect future damages to be even smaller (Aquisiti and Grossklags 2005).

As a rational economic agent, an individual will be expected to act according to expectancy theory, which holds that individuals will behave in ways that maximise positive outcomes and minimise negative outcomes (Van Eerde and Thierry 1996, Vroom 1964). Laufer and Wolfe (1977) were the first people to use this trade-off to derive a privacy calculus that would act as a predictor of whether individuals would find privacy scenarios acceptable or not. This calculus perspective is evident in several studies of privacy concerns (Hann et al 2008, Hui et al 2007, Milne and Gordon 1993). According to these studies, consumers perform a cost-benefit analysis of all the variables related to a particular scenario, in order to make their decisions.

Culnan and Bies (2003) have also argued 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. They went on to create a privacy calculus model that was based around a cost-benefit analysis. In recent years, various pieces of research have continued to create and validate privacy calculus models (Zhou 2011, Liu et al 2004, Dinev and Hart 2006, Culnan and Armstrong 1999, Xu et al. 2009, Xu et al. 2010, Pee 2011). Unfortunately, none of these are particularly relevant to future ITS systems, as most were focused on web-based marketing, although Xu, Parks, Chu and Zheng (2010) did explore the privacy calculus involved with location-based services in mobile phones.

One key factor that needs to be considered when looking at the privacy trade-off is that all of the judgements an individual makes depends heavily on their personal perception of the risks and rewards. In particular, the risk associated with a privacy scenario will be heavily dependent on the individual's perception of just how sensitive the required information is, just how much they trust the future data holder, and how much they trust the information transfer method.

### *3.4.2. The Privacy Variables*

When exploring the privacy trade-off discussed in the previous section in the context of the way a future ITS could generate privacy concerns, it is important to consider the cost and reward variables present in every scenario. In Chapter 2 it was shown that historically, a user's willingness to use a ITS will likely be impacted by their perception of; the type of information the ITS intends to collect, whether it will be combined with other information types which could increase the sensitivity of the information, how the information will be communicated between the various stages of the information chain and who can gain access to both the raw and processed information used by the ITS.

These variables can be classified into three distinct cost variables that are present in every privacy scenario; the type of information that is being disclosed (data sensitivity), who the personal information is going to (data holder) and how the personal information is getting to the new data holder (transfer method). In addition to the cost variables, if a future ITS user is going to perform a cost benefit trade-off, the reward on offer for disclosing the personal information will also be a key variable (reward).

A couple of pieces of previous research have explored how the perceptions of these variables vary (Rose et. al 2012, Bughin 2011 and Wallis 2007). It has been shown that there is quite a distinct tiering of how sensitive different types of information are. Of low sensitivity is information such as an individual's gender, age, name, email address and interests. The medium sensitivity category includes information about an individual's past purchases, media usage and location. In the high sensitivity category are financial data, social media posts and health information. (Rose et al. 2012 and Wallis 2007).

The perception of how secure personal information is with different data holders is also very varied with Wallis (2007) finding that 91% of survey participants trusted their personal information with the Health Sector but only 17% of the participants trusted the same information with the e-commerce industry. Rose J, Rehse O and B Röber (2012) found that 48% of participants stated that they had privacy concerns relating to social networking sites compared to only 4% of participants have privacy concerns relating to car manufacturers.

None of the aforementioned pieces of research asked participants for their perception of how secure different transfer methods were, however in Chapter 2, it was highlighted that peoples' perceptions of how secure wired and wireless communications were varied and it is expected that this trend will hold true to a wider range of communication methods. No previous research has been found that looks at the impact the perception of different types of rewards has on a user's willingness to disclose their personal information, although several pieces of research have looked at the impact of offering different levels of financial reward had on the amount and type of information an individual would be willing to disclose (Hui et al. 2007, Bughin 2011 and Rose et al. 2012). This is discussed further in Section 3.5(Actual Behaviour).

Work by Dwyer, Hiltz and Passerini (2007) discovered that a user's level of trust in a social networking site and its different members directly impacted a user's willingness to disclose their personal information on two different social networks. The greater the level of trust the more information they were likely to share. Other research has found that trust is strongly related to information disclosure in addition to successful online interactions (Metzger 2004 and Jarvenpaa and Leidner 1998).

Trust is defined by Mayer, Davis and Schoorman (1995) as "*the willingness of a party to be vulnerable to the actions of another party*" and it also forms a central component of social exchange theory (Roloff 1981). Social exchange theory presents a cost-benefit analysis with respect to social interactions. Trust is believed to be used in the calculation as a perceived cost (Metzger 2004). This ties in closely to the theory being developed in this thesis — that if the benefits of a future ITS outweigh the perceived costs, which will be centred around the data type required, the level of trust a user has in the future data holders and the level of trust in the transfer method — then the technology will be acceptable. This research will not attempt to explore the influencing factors of a future ITS user's perceived level of trust in the privacy variables but will instead focus on investigating how a user's perceived level of trust is likely to influence their privacy decision-making.

#### *3.4.3.Irrationality*

Although research and progress has been made into the use of rational privacy calculus models to predict peoples' actual behaviour, other researchers (Murphy 1996, Hirshleifer 1980, Aquisti 2004) have criticised the assumptions of rational behaviour underlying these privacy models as they fail to capture the complexity of human privacy decision-making.



Aquisti (2004) critiques the assumption of rationality in privacy decisions by suggesting that the field of Behavioural Economics offers proof that in numerous decision-making scenarios, humans do not act with complete rationality; they instead act in an irrational, but potentially predictable manner. Acquisti highlights three main reasons behind why human beings are not able to act as completely rational agents when they are faced with a privacy scenario. Firstly, the individual will likely be basing their calculations on incomplete information. Secondly, human beings have a ‘bounded rationality’ and finally humans are easily impacted by psychological distortions.

Incomplete information will affect the estimation of costs and benefits. For instance, is it possible for an individual to be aware of actual probability of a privacy invasions occurring and the actual cost of the consequences if a privacy invasion takes place? It can be argued that these probabilities could be calculated by looking at historic records which report the frequency of such events taking place. However, this sort of statistic is not known by the average individual. To make matters more complex, the majority of privacy invasions can be invisible. Many of the costs associated with exchanging personal information may only be discovered several years after the exchange has taken place (Acquisti 2004).

This leads into the bounded rationality theory, which questions whether human beings actually have the capacity to accurately calculate all the parameters relevant to the privacy scenario, even if they had complete information. In traditional economic theory, the agent is assumed to have both rationality and unbounded computational-power to process information. However, human individuals do not possess unbounded computational-power (Simon 1982). For most individuals, the cognitive costs involved in trying to find complete information and then to calculate the best strategy when faced with a privacy decision are too high, so it has been suggested they will just resort to simple heuristics (Acquisti 2007).

In addition to having incomplete information and being bounded by rationality, research within the field of Behavioural Economics has confirmed the impact of several forms of psychological distortions on individual decision-making. Some of these distortions are likely to be transferable to privacy decision-making. For example, individuals have a tendency to discount ‘hyperbolically’ future costs or benefits (Rabin and O’Donoghue 2000, O’Donoghue and Rabin 2001). Hyperbolic discounting has been proven to have an effect on privacy decisions (Acquisti 2004); it was shown that individuals are willing to give away their personal information at a cost in return for immediate gratification. Related to immediate gratification is the tendency to underinsure oneself against certain risks (Kunreuther 1984).

Other biases that have been linked to privacy decision-making (Aquisti 2007) include optimism bias (Weinstein 1989), where the misperception that one's risks are lower than those of other individuals under similar conditions, and cumulative risk bias (Slovic 2000), where, for instance, individuals do not fully realise the cumulative relation between the low risks of each additional data exposure building up to be a serious danger, especially as once released, personal information can remain available over long periods of time. Aquisti (2009) also demonstrated that the endowment effect (Kahneman and Tversky 1979, Thaler 1980) impacts privacy decision-making, by showing that individuals are willing to pay far less money to protect their personal information than they would be willing to receive for selling their personal information. This possibly highlights why numerous commercial privacy protection services have proved unsuccessful.

In summary, it is therefore fair to expect individuals when faced with a privacy scenario to attempt to rationally trade-off the reward on offer against the potential cost of disclosing their personal information (which will depend on how sensitive the data type is, how secure the information will be in the hands of the new data holder and how secure the transfer method is). However, the field of Behavioural Economics suggests that it is not possible for humans to act completely rationally, so their privacy decision-making process will be impacted by a lack of complete information, bounded rationality and psychological distortions.

### 3.5. Actual Behaviour

It has already been touched upon that some previous research has been conducted into peoples' actual privacy behaviour, although the vast majority of it is focused within the field of e-commerce. This research primarily focuses on observing a group of participants' behaviour when faced with a variety of privacy scenarios (Speikermann et al. 2000, Hui et al. 2007 and Bughin 2007). These pieces of research have shown there is a significant disconnect between a user's level of privacy concern and their actual behaviour, with it being shown that virtually all individuals are more likely to disclose their personal information than their level of concern dictates (Berendt et al. 2004 and Bughin 2011).

Others have used the observed results to create privacy calculus models (see Section 3.4) and while some of these resulted in models that predicted with reasonable accuracy the privacy behaviour of their participants, none of these pieces of research focuses on either a technology that does not already exist or a technology that is remotely close to most future ITS, so they are not very transferable to this research.

No research has been found that explores the link between an individual's stated privacy intention and their actual privacy behaviour. However, numerous other pieces of research from within the transport field have looked at the link between someone's stated behavioural intention and their actual behaviour (Chatterjee et al. 1983, Couture and Dooley 1981 and Hensher 2001). Evidence from these pieces of research suggests that a user's stated intention will provide a reasonable account of their actual choices (Wardmann 1988).

In addition the theory of planned behaviour explores the link between beliefs and behaviour. Ajzen (1991) found that intentions to perform behaviours of different kinds can be predicted with high accuracy from attitudes toward the behaviour and subjective norms. It is also found that these intentions, together with perceptions of behavioural control, account for considerable variance in actual behaviour. It is anticipated that the more positive a person's attitude towards a particular behaviour and the subjective norm, and the greater the perceived behavioural control, the more likely it is that a person will state their intention to perform the behaviour. Provided the person has sufficient control over the behaviour, they would then be expected to actually carry out this intention when the opportunity arises (Ajzen 2002).

### 3.6. Unknowns

From the review of literature, it is apparent that not enough is known about several aspects of both human privacy decision-making and how well previous research – mainly from the field of ecommerce – transfers to the transportation field for any accurate conclusions to be made about how future ITS will be impacted by privacy issues. This section of the thesis will highlight the main areas in existing knowledge that this research will need to add to in order for the aims and objectives of this research to be met.

The first thing that needs to be known is whether research conducted in other fields, predominantly the field of ecommerce, is directly transferable to the ITS sphere. In particular it needs to be confirmed that the impact demographics has on privacy concerns which is fairly established in other fields remains true for transportation. In addition to this, the impact of an individual's cultural background needs to be explored further as the research conducted to date has produced results that are both inconclusive and contradictory. Considering that most future ITS developers are looking to launch their systems in more than one country a better understanding of the impact different cultural backgrounds has on privacy behaviour is essential.

This research will also need to explore future ITS users' perceptions of the four privacy variables (data sensitivity, trust in data holder, trust in transfer method and the reward on offer) which are expected to be present in a range of different existing and future ITS. Research to date in other fields primarily focused on the perceptions of data sensitivity and the level of trust in different data holders.

Following on from exploring the perception of the privacy variables, this research will need to form a better understanding of how a future ITS user's demographic and perceptions of the four privacy variables impact not only the level of concern associated with a new ITS but also the user's stated behavioural intention and their actual behaviour. This is something that has only been lightly explored in other fields and never touched upon in the field of transportation.

The final major area that this research will have to investigate is the extent to which a future ITS user's privacy behaviour will be rational and based on a cost-benefit trade of instead of irrational and based on heuristics. Even if it is shown that future users will act irrationally it is likely that they would act in a predictably irrational manner which could help conclusions to be made about the feasibility of future ITS in privacy terms.

### 3.7. Research Model

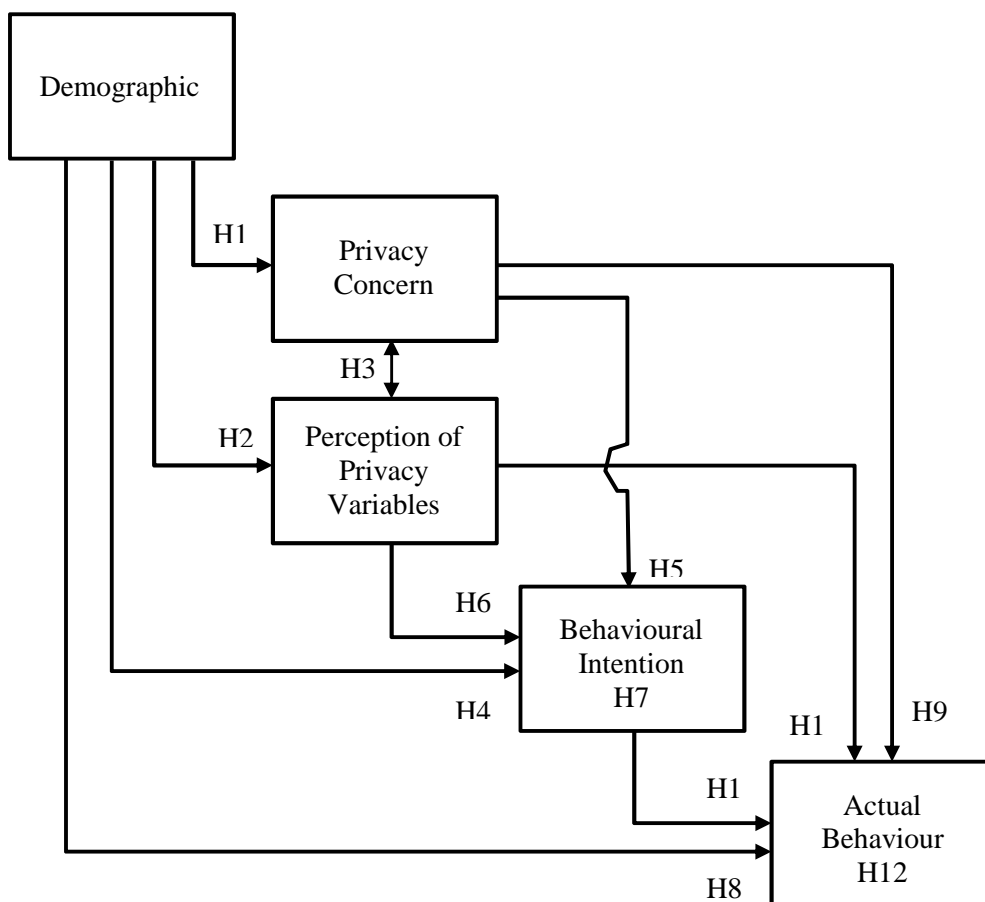
To ensure that all of the known unknowns highlighted in the previous section are explored, this section presents a model which has been drawn out from the existing literature. This model will need to be interrogated for further conclusions about the impact privacy will have on future ITS to be made. The research model aims to help identify the factors that will influence a future ITS user's privacy decision-making. This research will not attempt to develop a detailed understanding of 'why' these factors influence privacy decision-making. Instead the focus of this research will be to identify the key drivers of a future ITS user's privacy decision-making, as this will inform future ITS developers the factors that they need to address in order for their ITS to be deemed successful in privacy terms.

As this research is trying to draw conclusions about future ITS that are yet to be implemented, it is not possible to witness actual privacy decision-making relating to these technologies. It is, however, possible to investigate a user's level of privacy concern and their behavioural intention with regard to future ITS. It is also possible to investigate the link between a user's demographics, level of privacy concern, stated behavioural intention and actual behaviour for privacy scenarios that already exist. This will then make it possible to draw conclusions about their likely actual behaviour in relation to a specific future ITS.

Earlier in this chapter Figure 3-1 indicated that it is likely that future ITS user's level of privacy concern is likely to influence both their, stated behaviour and actual behaviour. The theory of planned behaviour as discussed in Section 3.5 suggests that intentions to perform behaviours of different kinds can be predicted with high accuracy from attitudes toward the behaviour and subjective norms (Ajzen 1991). The social contract theory touched upon in Section 3.4.2 also suggests when deciding whether a social interaction is acceptable or not an individual will carry out a cost-benefit analysis where trust is believed to be used in the calculation as a perceived cost (Roloff 1981 and Metzger 2004).

Figure 3-3 shows the model that attempts to combine elements of both the theory of planned behaviour and social contract theory. Some elements of the theory of planned behaviour such as the influence of social norms have been excluded for simplicity, as this research is only attempting to identify which variables influence privacy decision-making in the current snapshot of time. Whilst, other elements such as the influence of behavioural attitude (privacy concern) and stated intention on actual concern have been considered, along with the cost-benefit analysis of the privacy variables proposed in social contract theory. Figure 3-3 shows how the 12 hypotheses about how the future ITS user's demographics, level of privacy concern, stated behavioural intention and actual behaviour will be interlinked. This research will seek to explore each in detail.

**Figure 3-3 Hypothesised Relationships of the Research Model**



### *3.7.1. Level of Concern*

Previous research has shown that a future ITS user's level of concern is likely to be linked to their demographics (Kumaraguru et al. 2005, Phelps et al. 2000 and Wallis 2007). In particular, research within the field of e-commerce has shown that levels of concern are likely to vary with cultural background, increase with age, be higher in females, be higher in ethnic minorities, vary with level of education, increase with household income and decrease with experience of using a technology (See Section 3.3.2)

*H1: A user's level of privacy concern will be impacted by their demographics such as their age, gender and cultural background.*

### *3.7.2. Perception of the Privacy Variables*

Previous research suggests that a future ITS user's perception of the privacy variables – reward, data sensitivity, level of trust in data holder and level of trust in transfer method – will all vary with the demographics of the future user (See Section 3.4.2). It is also likely that the level of a user's privacy concern will be correlated with the three privacy cost variables. For example, logic would dictate that if somebody is concerned about privacy in general then they are more likely to find their personal information more sensitive and have less trust in some data holders and transfer methods. The relationship between general privacy concern and the perception of the privacy variables has not been explored previous to this research, so this research will have to attempt to fill this void in literature.

*H2: A user's perception of the four privacy variables will be impacted by their demographics such as their age, gender and cultural background.*

*H3: A user's perception of the three privacy cost variables will be linked to the user's general level of privacy concern.*

### 3.7.3. Behavioural Intention

Existing literature also advises that it is likely that a future ITS user's stated behavioural intention will be impacted by their demographic background. The key demographics that influence the level of a person's privacy concerns and hence may impact their actual privacy decision-making are age, gender and cultural background (Bellman et al. 2004, Cruickshanks and Waterson 2012, Fox et al. 2000 and Wallis 2007). In addition to this, it is expected that users with a high level of privacy concern are less likely to state that they would find any given privacy scenario acceptable (although they will still disclose more than their level of concern would suggest) (Berendt et al. 2005 and Bughin 2011).

*H4: A user's stated behavioural intention with regard to the action they would take when faced with a privacy scenario will be impacted by their demographics such as their age, gender and cultural background.*

*H5: A user's stated behavioural intention with regard to the action they would take when faced with a privacy scenario will be impacted by their general level of privacy concern.*

It has been argued that when faced with a privacy scenario, a user will act in a rational manner and weigh the reward on offer against the potential cost of disclosing their personal information (see Section 3.4). As a consequence, it is expected that as a user's perception of the reward on offer increases, so will the likelihood of them stating that they will find a privacy scenario acceptable (Berendt et al. 2004 and Hann et al. 2002).

*H6a: The perceived value of the reward on offer will have a positive impact on a user's behavioural intention.*

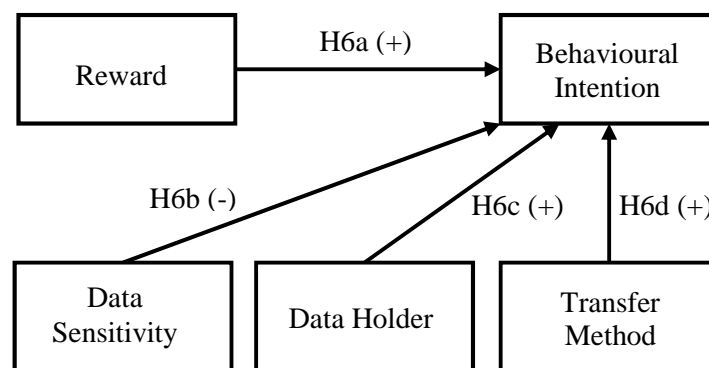
On the contrary, a user will be expected to act to minimise making decisions that will have a negative impact (Van Eerde and Thierry 1996 and Vroom 1964). Therefore, if a user perceives a scenario to be high risk, they are less likely to disclose their personal information. The risk associated with any scenario will be a combination of the risks associated to; the sensitivity of the information required; the level of trust the user has in the person/organisation the data is going to; and the level of trust the user has in the transfer method (Metzger 2004). Previous surveys of privacy concerns have shown that each of these values vary with individual perception (Phelps et al. 2000 and Wallis 2007). Figure 3-4 shows how this research expects the perceptions of the four privacy variable to impact a user's stated behavioural intention.

*H6b: The level of sensitivity associated with a data type will negatively impact a user’s behavioural intention.*

*H6c: The level of trust a user has in the new data holder will have a positive impact on the user’s behavioural intention.*

*H6d: The level of trust a user has in the data transfer method will have a positive impact on the user’s behavioural intention.*

**Figure 3-4 Hypothesised Relationships of between Privacy Variable and Behavioural Intention**



Unlike the historic privacy calculus models that assume complete rationality (see section 3.4), this hypothesised research model assumes that a user uses the perceived values for risk and reward to calculate the outcome of a privacy scenario. By doing this, this model will reduce at least one of the flaws to using a rational model highlighted earlier; incomplete information (Aquisti 2004). This model should therefore limit the impact irrationality has on predicting the outcome of a user’s privacy decision-making process.

*H7: A user’s stated behavioural intention will primarily be derived from their demographics, general level of primary concern and a trade-off between their perceptions of the reward on offer against the risk associated with a scenario.*



### 3.7.4. Actual Behaviour

Similar to stated behaviour intention, it is anticipated that a future ITS user's actual behaviour will be influenced by their demographics, level of privacy concern and their perception of the privacy variables (Chatterjee et al 1983, Wardmann 1988 and Ajzen 1991). Figure 3-5 shows the expected relationships between the perceptions of the privacy variables and a user's actual behaviour.

Although it is predicted that most of the variables that influence stated behavioural intention will also influence actual behaviour, it is possible that the degree to which each variable influences the privacy decision-making process in a real and hypothetical scenario could vary. For example, the perception of the reward on offer could have a greater influence on the privacy decision-making process for an actual scenario than a hypothetical one (Berendt et al. 2004 and Bughin 2011).

*H8: A user's actual behaviour will be impacted by their demographics such as their age, gender and cultural background.*

*H9: A user's actual behaviour will be impacted by their general level of privacy concern.*

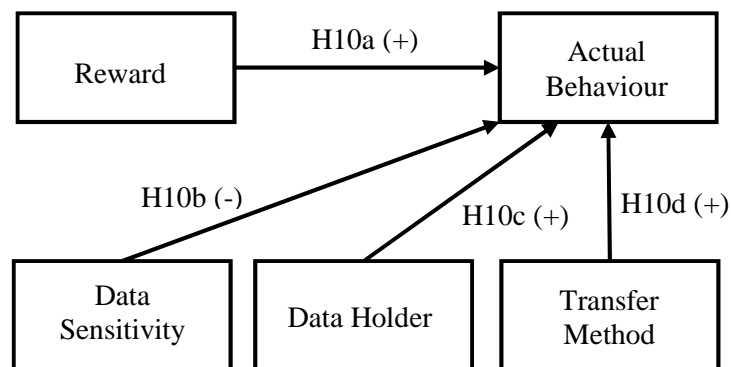
*H10a: The perceived value of the reward on offer will have a positive impact on a user's behavioural intention.*

*H10b: The level of sensitivity associated with a data type will negatively impact a user's behavioural intention.*

*H10c: The level of trust a user has in the new data holder will have a positive impact on the user's behavioural intention.*

*H10d: The level of trust a user has in the data transfer method will have a positive impact on the user's behavioural intention.*

The strongest predictor of actual behaviour, however, is likely to be a user's stated behavioural intention for a given privacy scenario. It is anticipated that users who state that they would be willing to disclose their personal information in a privacy scenario are significantly more likely to do so than those who stated they would not. However, previous research has shown that in reality all users are likely to disclose more personal information than they state they would (Berendt et al. 2004 and Hann et al. 2002).

**Figure 3-5 Hypothesised Relationships of between Privacy Variable and Behavioural Intention**

*H11: A user's actual behaviour will be significantly impacted by their stated behavioural intention.*

As with stated behavioural intention, it is anticipated that by using a user's perceptions of the privacy variables (instead of actual values based on historical evidence) and a user's stated behavioural intention it could limit amount of irrationality that to accounted as some of the factors that cause bounded rationality (Simon 1982 and Aquisti 2004) have been accounted for. This should result in a future ITS user's demographics, level of privacy concern, perception of the privacy variables and their stated behavioural intention being the primary factors which impact a future ITS user's actual behaviour.

*H12: A user's actual behaviour will primarily be derived from their stated behavioural intention, demographics, general level of primary concern and a trade-off between their perceptions of the reward on offer against the risk associated with a scenario.*

### 3.8. Summary

This chapter has shown that four main factors are likely to impact a future ITS users actual behaviour when they have to decide whether to disclose their personal information to a future ITS or not. Firstly, a user's demographics are likely to influence not only their actual behaviour, but also the other main influencing factors. Previous evidence suggests that the elderly, females, people with a high income and ethnic minorities are expected to act in a more privacy-preserving manner.

The second factor that is expected to influence a future ITS user's actual behaviour is their general level of privacy concern. The literature review has shown that whilst not everyone will act upon their concerns, a concerned future ITS user will be more likely to act in a privacy-preserving manner than a user with a low level of privacy concern.

The third and probably most critical factor that is expected to influence not only on stated behavioural intention but also a future ITS user's actual behaviour is the user's perceptions of the privacy. It has been suggested that a future ITS user will act in a rational manner and attempt to weigh the reward gained by disclosing their personal information against the potential cost of disclosing the information. A user is likely to calculate the risk associated with disclosing their personal information by using their perceptions of how sensitive the data being disclosed is, how safe their information is with the new data holder and how safe their data is while being transferred.

The final key factor that is projected to be a key predictor of a future ITS user's actual behaviour is their stated behavioural intention. It is anticipated that there will be a strong link between users who state they will disclose their personal information and those that actually will. The literature review also suggests that most users will disclose more personal information when actually faced with a privacy scenario than they state they will do. Whilst numerous researches have explored the factors that impact a person's level of general privacy concern, the same cannot be said for the factors that will influence a person's stated behavioural intention and actual behaviour when being confronted with a privacy scenario. This is especially true for the field of transportation where it is believed that this research is the first to consider the factors that will influence a future ITS user's actual behaviour instead of just measuring their level of concern about the future technologies.



## 4. Methodology

### 4.1. Introduction

This chapter outlines and justifies the methodology used to achieve the aim of this research, which is to better understand the factors influencing privacy decision-making and the impact they will have on the success of future ITS. To achieve this target, the methodology, set out to meet all of the objectives set out in Chapter 1. Figure 4-1, shows a flow chart of the data collection and analysis that was required to meet all of the objectives.

*Objective 1: Understand ‘privacy’ and how it will be relevant to current and future ITS*

An understanding of ‘privacy’ has been developed through a thorough literature review. The research model developed in response to the literature review (see Chapter 3) suggests that before a user carries out any action, be it driving their car, using an internet search engine or making a phone call, he/she will carry out a privacy risk-reward calculation. The research model also suggests that this process could be impacted by inaccurate calculation of the risks and rewards, the user’s bounded rationality or even the fact that the user is impacted by innate biases.

*Objective 2: Compare existing, proposed and hypothetical ITS, paying particular attention to their benefits and the level of personal information they require.*

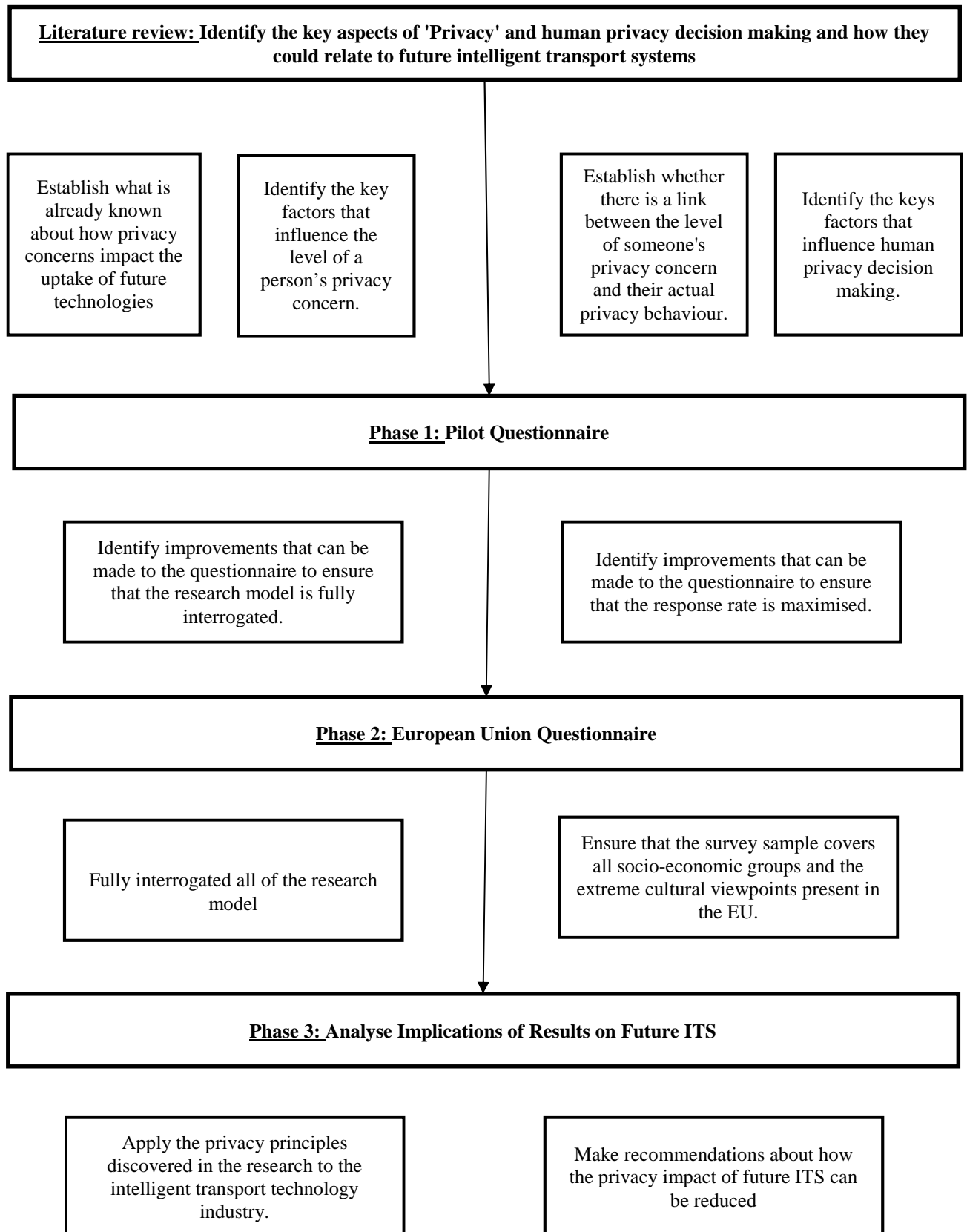
Chapter 2 has shown that the benefits and informational requirements of existing and proposed ITS are wide and varied. It is therefore important to identify the factors that will influence future ITS user’s actual privacy behaviour.

*Objective 3: Identify the factors that will cause the level of personal information required by a future transport technology to become unacceptable.*

The research model, created after a thorough literature review, will be tested with quantitative data. After validation, the model should make it possible to draw conclusions about the point at which a privacy scenario becomes unacceptable.

*Objective 4: Understand whether views on the acceptable level of intrusion vary from person to person throughout the European Union member states and discover what the influencing factors are.*

Figure 4-1 Flow Chart of Data Collection and Analysis



This objective will be achieved by ensuring that the data that will be used to interrogate the research model truly represents the people who live and travel throughout the European Union. As long as this is the case, statistical analysis of the data set will show how people's views vary from person to person and nation to nation.

*Objective 5: Draw conclusions about whether different ITS in their current and hypothetical forms will be deemed acceptable in 'privacy' terms.*

After the research model has been tested, it will be possible to apply the validated research model to the ITS included in Chapter 2. This will enable conclusions to be made about whether these technologies are acceptable in 'privacy' terms.

*Objective 6: For technologies that are deemed unacceptable, improvements will be suggested.*

Once all three phases of the research methodology have been concluded, it will be possible to evaluate how the technologies/legislation could be improved to meet the public's demands. It will then be at this stage that it is possible to conclude whether 'privacy' could prevent future ITS from being implemented.

## 4.2. Methods

### *4.2.1. Quantitative Data*

To meet objectives 3-6 it is essential to test the research model created after the literature review, with a large unbiased data set so that the privacy factors can be analysed using statistical processes.

Quantitative methods are best used when the expected outcome is clearly known; this is the case with this research, as essentially this research is applying theories proven in one field to another (Creswell 2009). Quantitative methods can also be used to determine which factors and variables influence or determine an outcome, whereas qualitative methods are used in a more exploratory method when limited theories already exist (Creswell 2009). Again, this highlights that quantitative methods will be the most suitable for testing the research model.

Qualitative research could also have been used to explore why future ITS user's act in the way they do when faced with a privacy scenario. However, as the focus of this research is primarily on identifying the factors that influence privacy decision-making instead of why they influence privacy decision-making, the benefits of doing this could have been limited. This fact combined with the solid research model meant it felt appropriate to focus the research effort on a purely quantitative methodology instead of also seeking qualitative data.

#### *4.2.2. Experimental Data*

The most useful quantitative data for testing the research model presented in the previous chapter would be experimental data. This data would be derived by witnessing participants' actual behaviour when faced with a privacy scenario. Details of the participant's demographics, their level of privacy concern and stated influencing factors would also be measured. This method has been used with some notable success in some previously mentioned research conducted within the field of ecommerce (Berendt et al. 2004).

Unfortunately, as this research is seeking to explore the likely privacy behaviour associated with ITS that are not yet fully developed, it is not possible to observe user's privacy behaviour while using these technologies. Although some ITS are already fully operational and some observations about how they are treated in privacy terms could be made, Chapter 2 has already highlighted that existing ITS could potentially not create the same high levels of privacy concerns as some in the future could, therefore drawing conclusions from these technologies will not enable all of the aims and objectives of this research to be achieved, although as mentioned earlier in the discussion on the theory of planned behaviour (Section 3.5), it is feasible that social norms with regards to privacy and disclosing personal information could also change which in turn could impact privacy decision-making

#### *4.2.3. Self-Administered Questionnaires*

With regards to this research and excluding experimental data, the best instrument for collecting large amounts of quantitative data about future ITS users' likely privacy behaviour is by using self-administered questionnaires. This is because the questionnaires can be designed to probe for information about a future ITS user's current level of privacy concern, their current actual privacy behaviour and also their stated behaviour intention with regard to various future ITS. In addition, self-administered questionnaires are an efficient method to sample large numbers of individuals, across all socio-economic groups with a standardised method at relatively low costs (Oppenheim 2005).



It is important that the sample population is selected carefully, so that it covers as many socio-economic groups as possible, to allow the results to be extrapolated to represent a wider population. It is also important to consider whether the people who refused to respond to the questionnaire have a different viewpoint from those people who were willing to complete the questionnaire (Malhotra and Birks 2003). The main way of limiting the potential for this bias to occur is to ensure a relatively high response rate (>10%), this can be achieved by ensuring that the survey is short in length, gives the participant an incentive for completing the questionnaire (even if it is just the feeling of helping someone else) and making sure the subject-matter is interesting (Dillman 2007).

Another important aspect of a self-administered questionnaire is that it is designed in such a way that every participant's understanding of the questions is the same. If this is achieved, an advantage that self-administered questionnaires have over interview based surveys is that they are often more reliable than an interview-based questionnaire. In an interview-based questionnaire, the interviewer is more likely to influence the respondent through the tone of their voice, assisting the participant with guiding information and influencing the participant into giving the interviewee the answer they believe they want to hear. This is especially true when asking for opinions (Von Sanden 2004).

There are several possible methods for distributing self-administered questionnaires and, with the appropriate planning, it is possible to combine the different methods to reach a larger sample. The possible methods include web-based questionnaires, postal questionnaires and hand-distributed questionnaires (Dillman 2007). Web-based questionnaires have the benefit that they are relatively low cost to set up, and are then free to distribute to a wide sample. It is even possible for the participants to forward on the questionnaire to further recipients creating a large data set.

However, there are several negative points associated with using a web-based questionnaire. Firstly, not everyone has access to the internet so certain socio-economic groups are eliminated completely, and even if everyone had access to the internet, the actual response rate is historically fairly low (Dillman 2007). Secondly, samples that contain only web-based results are potentially biased by the fact that only the views of people who are willing to transfer their personal information across the internet will be sampled. This is a point that is of particular pertinence to this research as it is attempting to see whether people are willing to share personal information over various forms of technology, so limiting the sample to only people who are willing to exchange their information over the internet is flawed.

Another more targeted and unbiased method for distributing the questionnaire is by using the postal system. This method allows the use of census data combined with mailing lists (such as the electoral register) to target specific areas that include all the relevant socio-economic groups. The main downside of postal surveys is that they are relatively costly (when compared to web-based questionnaires) and they historically have low response rates, which leaves the sample open to bias. The other main method for distributing self-administered questionnaires is by hand. The major benefit to this method is that it will ensure responses from targeted socio-economic groups. The main downside to this method is that they are slow to complete and depending on labour costs, can be expensive especially if a large sample is required. Dillman (2007) recommends that the best method for distributing a self-administered questionnaire is to use a combination of the different distribution methods. This will ensure that the survey will sufficiently cover all of the required socio-economic groups, but also take advantage of the cost-efficiency of some of the less targeted methods.

In summary, the major benefits of using a self-administered questionnaire to collect quantitative data are that they are good for collecting a large amount of information from individuals, and the anonymous nature of the questionnaires means that individuals may reveal more sensitive information than in a face-to-face interview (Nardi 2006). The most substantial problem with self-administered questionnaires, however, is that it is very easy for the sample selection process to become biased due to a combination of the relatively low response rates some of the distribution methods have, and the fact that the views of the people who refuse to complete the questionnaire could be different to that of those who do complete the questionnaire.

### 4.3. Phase 1 - Pilot Survey

Before the quantitative questionnaire was used across a wide sample to interrogate the research model, it was important to trial the questionnaire first. The crucial things to test were; that the data set it creates can be used to interrogate the research model appropriately; that participants were able to understand it and answer all of the questions in a correct and useful manner; and that everything possible has been done to the questionnaire design to maximise the response rate.

To ensure that the pilot survey targeted a wide range of people, a website and paper version of the questionnaire was created (see Appendix A). This web-based survey was identical to the paper version of the questionnaire, except for the fact that it also asked the participant for their location, nationality and the type of area in which they reside before they can move on to the privacy based questions.

The web-based survey was sent out to friends and family of the author and they were asked to forward on the link to the research website ([www.internationalprivacysurvey.com](http://www.internationalprivacysurvey.com)) to their own friends and family in turn. In addition, twenty paper versions of the questionnaire were handed to colleagues to test that the paper version of the questionnaire was also acceptable. The pilot survey sampled 134 participants in total and although the sample was relatively small and had a significant amount of selection bias, it was still possible to use the results/feedback from the survey to test the questionnaire before it was used on a wider European sample.

The results of the pilot survey showed that the majority of the questionnaire worked well, although there was room for a couple of improvements. The main improvement centred on making sure that every question had a purpose and that it helped to validate the research model in some way; this was not true for every question in the pilot questionnaire. Another problem area that the results of the pilot survey identified was that people were struggling to understand and answer Section A in an appropriate manner. This was also supported by feedback received from people who had filled in the questionnaire. Once the questionnaire had been redesigned it was sent to a further small pilot (22 fellow students and friend) to ensure that the changes made to the survey had had the desired effect – which they appeared to.

#### 4.4. Questionnaire Design

This section of the report looks into the general design of the final quantitative questionnaire that formed the major part of this research (see Appendix B). The main aim of the questionnaire was to explore the known unknowns and to interrogate the research model found in the previous chapter. This was achieved by examining how an individual perceives the privacy variables that are taken into account when making privacy decisions, and seeing how this compared to the decisions that the participants took in numerous privacy scenarios. The questionnaire also sought to gain information about the participants existing privacy habits and preferences.

In addition to the questions, the questionnaire included a covering letter/home page which acted as the primary tool for improving the questionnaire response rates. Several tried-and-tested methods were used on the covering letter/home page including; stating that by completing the questionnaire that they will be helping the author, giving them an honest assessment of the length of time it will take to complete the survey; and explaining briefly what the research is trying to achieve in an attempt to gain the participants interest (Dillman 2007).

#### *4.4.1. Section A - Rewards, Consequences and Risks*

The aim of this segment of the questionnaire was to explore how an individual values the privacy variables identified in the literature review. These variables are the reward on offer, the type of information that is being exchanged, who the information is being exchanged with and how the information is going to be exchanged.

There are several methods for scaling the values someone attributes to a variable. These include: maximum difference scaling, ranking, and rating methods (Cohen 2003). In the pilot survey, a form of maximum difference scaling (Cohen 2003) was used as it appeared to be the best all-round method. Unfortunately, the maximum difference scaling questions in the pilot survey (see Appendix A) proved confusing for some of the participants and as a consequence, some surveys were either left incomplete or filled in incorrectly. Due to these errors, it was decided that using a rating system to determine the participant's perception of the privacy variables would be the best method to use. Due to the number of variables present, a ranking system would have been too difficult/time consuming for participants (Rankin and Grube 1980).

In addition to the new question structure, Section A of the final questionnaire (see Appendix B) also asked questions that not only tied in directly with the scenarios in Section B, but also with the voluntary demographic questions found in Section D, which was not the case in the pilot questionnaire. Also, included in Section A are four questions that were first used by Professor Alan Westin (Kumaraguru 2005) for determining whether a person was a privacy Fundamentalist, Pragmatist or Unconcerned. This information was extremely useful when it came to analysis of the results.

#### *4.4.2. Section B – Scenarios*

Section B of both the pilot and the final questionnaires (Appendences A and B respectively) asked the participant whether they would say 'Yes' or 'No' to a range of privacy scenarios. The main aim of this section was to test whether from knowing how the participant values the privacy variables (they were measured in Section A of the questionnaire) it is possible to predict their stated preference in a range of hypothetical privacy scenarios. The privacy scenarios give the participant information about the reward on offer, the type of personal information they have to give away, who the information is going to and how it is getting there.

In the final questionnaire, three different types of scenario were used, each using variables that had been directly measured in the previous section of the questionnaire. This was not the case for all of the scenarios in the pilot questionnaire, and was one of the key differences between the two questionnaires. The three types of scenario were either related to potential future ITS, general life, or tests of real-life privacy scenarios. Table 4-1 shows the ten scenarios that were included in the European survey.

Whilst this research seeks to investigate how privacy decision-making will impact future ITS, only 4 of the 10 scenarios were based around ITS. The rationale behind this was that whilst it is important to explore how the participants act when faced with a privacy scenario in the transport world it is also important to explore whether the participants would act in a similar or different way when faced with a privacy scenario in general life. As a consequence, three general scenarios were included in the questionnaire so that comparisons between the general and ITS scenarios could be made. It was also felt that to explore a future ITS user's likely actual behaviour that three test scenarios should be included in the questionnaire so that the link between stated behaviour and actual behaviour could be investigated.

A conscious decision was also made to frame the scenarios in the same way they would be framed in real life, even though this could introduce differences in interpretation and some ambiguity. The reasoning behind this was that as this research was looking at how future ITS users are likely to act when faced with the privacy scenario in the real world it is important that the scenarios are framed in the same way. Most of the rewards offered in real life privacy scenarios are open to ambiguity and do not have a definitive value. For example, having passenger airbags will improve the safety of your family but it is very difficult to put a figure on the percentage increase in safety and it will not make the vehicle completely safe. Also when a car owner is pitched optional safety features (potentially such as future ITS) the selling point will be to 'improve safety' but it is unlikely that the safety feature will be promoted by stating it will improve your family's safety by 'X' amount.

Likewise it can be argued that a lot of the risks involved in the privacy scenarios will be equally affected by how they are framed in the real world, so it is appropriate that this research attempts to frame the risks in the same way they will be presented in real life. For example, when choosing to use a car park that uses ANPR for ticketing purposes or not, a driver is likely to know very little about; the operator of the car park (other than they are a private company/local authority), what personal information is actually being taken from them (it is unlikely that all users of the car park will realise that their car number plate is being monitored and recorded), what is being done with this information and (in particular whether it is being given to third parties) and also the method their data is being transferred.

In addition to the privacy scenarios, Section B of the questionnaire also contained two further questions. The first tested whether making the information exchange anonymous improves the participant's willingness to accept a privacy scenario. This was done by asking a duplicate scenario, but this time making it so that the data exchange is anonymous. The other question asked in Section B relates to the privacy fears highlighted in the literature review and simply asked the participant whether they would change their travel behaviour if their location at all times was made public.

#### *4.4.3. Section C – Improvements*

Section C of the questionnaire was designed to test whether the conclusions made in the literature review about the causes of privacy concerns are indeed correct. In addition, Section C has been designed to highlight the most desirable privacy improvements that could be implemented to a future transport system.

It was chosen to ask the participants about which improvements they want (each improvement links directly to one of the six main causes identified in the literature review). It was decided against asking about the causes directly, because this has already been done in several other pieces of research (Bellman et al. 2004, Malhotra et al. 2004 and Smith et al. 1996).

#### *4.4.4. Section D - About You and Your Choices*

Section D was primarily designed to find out as much about the participant as possible; not only their demographics, but also whether their stated preferences and scenario answers actually match up to their actions in reality. This is measured by asking the participant whether they currently use loyalty cards, shop online and whether they have or would be willing to go through airport security. These actions match exactly with the three test scenarios (see Table 4-1), so a direct comparison can be made between the participants stated preference and their actual behaviour.

Several further tests of the participant's actual privacy behaviour were also created. Firstly, answering the demographic information questions was made voluntary. Although this will limit my knowledge of the participant, it will validate how protective someone is of certain types of information. In addition, the participant was asked for further contact details in return for the chance to earn £20/20€ worth of gift vouchers for filling out a follow up survey. Although there was no intention to conduct any follow-up survey, this was a test to see whether the participant is willing to give away some personal information in return for the chance to earn a reward.

**Table 4-1 Summary of Questionnaire Scenarios and the Variables they are Testing**

Type of Scenario	Question	Reward on Offer	Information Type	Data Holder	Transfer Method
ITS	During a car journey would you tell a company the road and weather conditions in your location via a wireless network if it would help to reduce your impact on the environment?	Environment	Weather Conditions	Company	Wireless Internet
ITS	Would you tell the government by text message exactly where you plan to travel if it reduced your travel time?	Time	Location	Government	Text
ITS	During a car journey would you tell a stranger your location over a wireless network if it improved the safety of you and your family during the journey?	Safety	Location	Stranger	Wireless Internet
ITS	Would you let a private company know about your driving behaviour (speed at which you travel, how you travel etc) if it reduced your insurance premiums?	Cost	Driving behaviour	Company	N/A
Gen	Would you tell a journalist in a private meeting your musical preferences in return for a rise in your social standing?	Image	Musical Preferences	Journalist	Private F2F Meeting
Gen	Would you tell a close friend your embarrassing secrets in a letter sent by postal mail if you thought it would bring you a lot of enjoyment?	Enjoyment	Secrets	Friend	Post
Gen	Would you tell your medical conditions to a random doctor via a mobile phone if you thought it would improve your health?	Safety	Medical Record	Medical Professional	Mobile
Test	Would you give the details of everything that you purchase to a private company by email in return for a financial gain?	Cost	Purchase History	Company	Wired Internet
Test	Would you send your credit card details over an internet connection to a private company to book a room at a hotel in order to receive a discount online?	Cost	Bank Details	Company	Wired Internet
Test	Would you allow a security guard to search you and your luggage if it might improve your safety?	Safety	Secrets	Stranger	Public F2F Meeting

#### 4.5. Phase 2 -European Union Survey

The main method of data collection during this research was a wide sampled quantitative survey in order to validate the research model. As highlighted earlier in this chapter, the most common quantitative method for gaining a large sample is via self-administered questionnaires as they provide reliable results while remaining fairly cost/time efficient. The main area of concern with using self-administered questionnaires is ensuring that the sample remains unbiased by covering most socio-economic groups. This is a particularly valid concern for this research as the literature review highlighted that it was likely that a future ITS user's demographic and cultural background was likely to impact their privacy behaviour. It was therefore of the utmost importance that the questionnaire was distributed to a full range of the cultural and social groups present within the European Union. Ideally a worldwide sample would have been used as it would have been more diverse than just a European one. However, this research was funded by the NEARCTIS project (NEARCTIS 2012) which in turn received funding under the seventh Research Framework Programme of the European Commission (European Commission 2012) which meant the sample was limited to the European Union only. This section of the report describes how the European sample was derived and then goes into more detail about the exact methodologies and sample demographics achieved in the four regional surveys.

##### *4.5.1. European Sample – Hofstede's Cultural Dimensions*

To ensure that the privacy views of the full range of cultures present in the European Union are measured, four separate countries were surveyed. These countries represent the four extreme national cultural corners of Europe. National cultures can be described according to the analysis of Geert Hofstede, who breaks them into four independent and measureable dimensions. As discussed in section 3.4.2, these dimensions consist of Power Distance, Individualism, Masculinity and Uncertainty Avoidance (Hofstede 2001).

For each country in the European Union, Hofstede has measured the cultural dimensions. To identify the four cultural corners in Europe that will form the countries in which the European questionnaire will be distributed, the four countries whose cultural dimension score covered the biggest range were found. Table 4-2 shows the calculations that were carried out to find the four most cultural diverse countries within Europe. For practicalities sake, only countries which had either a full or associated partner of the NEARCTIS research group (NEARCTIS 2012) were considered as the funding for this research was contingent on being conducted in conjunction with more than one of the NEARCTIS partner institutes.



Table 4-2 European Country Selection – Hofstede’s Cultural Dimensions

Countries				PDI C1	PDI C2	PDI C3	PDI C4	IND C1	IND C2	IND C3	IND C4	MAS C1	MAS C2	MAS C3	MAS C4	UAI C1	UAI C2	UAI C3	UAI C4	min PDI	max PDI	min IDV	max IDV	min MAS	max MAS	min UAI	max UAI	Diversity*
Austria	Greece	Sweden	UK	11	60	31	35	55	35	71	89	79	57	5	66	70	112	29	35	11	60	35	89	5	79	29	112	16251732
Austria	Greece	Norway	UK	11	60	31	35	55	35	69	89	79	57	8	66	70	112	50	35	11	60	35	89	8	79	35	112	14465682
Austria	Greece	Netherlands	UK	11	60	38	35	55	35	80	89	79	57	14	66	70	112	53	35	11	60	35	89	14	79	35	112	13243230
Denmark	Greece	Portugal	UK	18	60	63	35	74	35	27	89	16	57	31	66	23	112	104	35	18	63	27	89	16	66	23	112	12415500
Denmark	Greece	Sweden	UK	18	60	31	35	74	35	71	89	16	57	5	66	23	112	29	35	18	60	35	89	5	66	23	112	12312972
Austria	Greece	Portugal	UK	11	60	63	35	55	35	27	89	79	57	31	66	70	112	104	35	11	63	27	89	31	79	35	112	11915904
Denmark	Greece	Norway	UK	18	60	31	35	74	35	69	89	16	57	8	66	23	112	50	35	18	60	35	89	8	66	23	112	11707416
Denmark	Greece	Turkey	UK	18	60	66	35	74	35	37	89	16	57	45	66	23	112	85	35	18	66	35	89	16	66	23	112	11534400
Denmark	Greece	Italy	UK	18	60	50	35	74	35	76	89	16	57	70	66	23	112	75	35	18	60	35	89	16	70	23	112	10900008
Denmark	Greece	Switzerland	UK	18	60	34	35	74	35	68	89	16	57	70	66	23	112	58	35	18	60	35	89	16	70	23	112	10900008
Denmark	Greece	Ireland	UK	18	60	28	35	74	35	70	89	16	57	68	66	23	112	35	35	18	60	35	89	16	68	23	112	10496304
Denmark	Greece	Netherlands	UK	18	60	38	35	74	35	80	89	16	57	14	66	23	112	53	35	18	60	35	89	14	66	23	112	10496304
France	Greece	Sweden	UK	68	60	31	35	71	35	71	89	43	57	5	66	86	112	29	35	31	68	35	89	5	66	29	112	10115874
Denmark	Greece	Spain	UK	18	60	57	35	74	35	51	89	16	57	42	66	23	112	86	35	18	60	35	89	16	66	23	112	10092600

\*The diversity score was calculated by multiplying the max country score minus the min country for each dimension by one another

Table 4-3 shows the cultural dimensions of the four countries that were chosen to represent the cultural corners of Europe; UK, Greece, Netherlands and Austria. It is evident from the table that this sample comprises of at least one country that scores both high and low in every category. This should aid the analysis of how culture impacts on people’s privacy decision-making.

**Table 4-3 Hofstede’s Cultural Dimensions for Selected Countries**

Country	Uncertainty		Masculinity	Power
	Avoidance	Individualism		Distance
UK	<b>35</b>	<b>89</b>	66	35
Greece	<b>112</b>	<b>35</b>	57	<b>60</b>
Netherlands	53	80	<b>14</b>	38
Austria	70	55	<b>79</b>	<b>11</b>

#### 4.5.2. UK Survey

The survey sample in the UK was derived by using UK 2001 census data (at the time of the sample being created, data from the most recent census conducted in 2011 was not available), to identify a region that closely resembles that typical demographic makeup of the country as a whole. A random sample of the whole of that region will closely reflect that of the wider population. The region that best matched the overall national average profile for education levels, distance travelled to work, employment status, mode of travel to work, ethnicity and social grade was found to be the Metropolitan District of Sefton. This region was identified by seeing which region was within the closest number of standard deviations to the national average for each of demographic factors mentioned above. Table 4-4 shows how this region compares to the whole of the country.

In the UK, two electoral registers are created for each district; a full register (containing the names and addresses of all eligible voters) and an edited register containing the names and addresses of all those who do not specifically ‘opt-out’ of being included. While the full register remains with the local authority, the edited register is available to purchase by companies. Half of the surveys sent out were sent to people selected randomly from the edited electoral register for Sefton, but as those people who have opted out of being on the edited register are likely to have different privacy views from those who have not opted out of the register, the remainder of the questionnaires were sent to addresses that did not appear on the electoral register (addressed simply to the ‘homeowner’ as their name was unknown).

**Table 4-4 Demographics of Sefton Compared to England and Wales**

		England and Wales	Metropolitan District of Sefton
Education Level	No Qualifications	29.1%	31.0%
	Levels 1-3	44.2%	45.4%
	Levels 4-5	19.8%	16.7%
Distance Travelled to Work	0-5km	49.0%	47.0%
	5-20km	33.5%	35.6%
	20km +	12.6%	12.8%
Employment Status	Employed	60.6%	55.7%
	Retired	13.6%	16.8%
Mode of Travel to Work	Private Vehicle	56.3%	56.7%
	Walk/Cycle	12.8%	12.4%
Ethnicity	White British	84.5%	96.7%
Social Grade	AB	22.0%	20.9%
	C1	29.7%	30.7%
	C2	15.1%	13.6%
	D	17.2%	16.3%

2,000 paper-based questionnaires (see Appendix B) were sent out to the random sample in July 2011 (1,000 to addresses not on the edited electoral register). Along with the questionnaire, a ‘free post’ return envelope was also attached. Three weeks after the questionnaires were initially sent out, a reminder/thank you postcard was sent to boost the response rate. Respondents were also given the option to fill in the questionnaire online instead of paper, if they preferred. In total 196 completed questionnaires were received back, which gave an overall response rate of 9.8%. 100 of those received back were from questionnaires addressed to people on the edited electoral register, meaning that the remaining 96 were not on the electoral register.

Table 4-5 shows how the demographic make-up of the responders to the mail survey compared to the demographic make-ups of Sefton and England. It becomes apparent from this table that responses were received from each socio-economic group, although not in the proportion that was expected. The actual sample contained proportionally more people over 55, retired and with a high education level than in either the Sefton or England. Although this is not ideal, no socio-economic group has been completely missed (and employed 20-40 year olds are notoriously bad at responding to postal questionnaires).

**Table 4-5 Demographic Make-Up of the UK Mail Survey**

		England Census Results 2001	Sefton Census Results 2001	UK Mail Survey Results Aug 2011
Gender	Male	48.7%	47.2%	50.5%
	Female	51.3%	52.8%	49.5%
Age	16-25	15.2%	13.2%	6.7%
	26-35	18.5%	15.2%	6.7%
	36-45	18.3%	18.5%	14.0%
	46-55	16.4%	16.6%	20.7%
	56-65	12.9%	14.3%	25.7%
	66-75	9.3%	11.4%	16.8%
	75+	9.4%	10.9%	8.9%
Ethnicity	White British	84.5%	96.7%	90.9%
Education Level	None	29.1%	31.0%	13.0%
	Level 1-3	44.2%	45.4%	47.8%
	Level 4+	26.7%	23.7%	39.1%
Employment Status	Employed	74.3%	69.8%	47.3%
	Student	4.8%	4.5%	4.8%
	Retired	8.9%	11.4%	30.3%
	Unemployed	2.2%	2.7%	5.3%
	Other	9.8%	11.7%	12.2%
Marital Status	Single	49.1%	47.1%	25.0%
	Married	36.9%	37.3%	60.6%
	Divorced	7.0%	7.0%	13.3%
	Widowed	7.0%	8.6%	1.1%

To address this imbalance in the survey sample, a web-based survey was used to sample an extra 69 employed 18-50 year olds. These participants were targeted by getting a private company with a wide range of socio-economic levels represented within their staff to ask their employees to fill in the web-based version of the European survey. Whilst it was highlighted earlier that using technology to survey participants about whether privacy concerns would prevent them from using a future technology was not ideal. It was decided that it was better to further collect the views of the demographic groups that were lightly covered by the paper version of the questionnaire and accept that some of the extreme views could potentially have been missed, in order to prevent some demographic groups from being under represented, which would make analysis of the demographic influencing factors less accurate. A demographic breakdown of the complete UK sample of 265 participants can be seen in Table 4-5.

#### *4.5.3. Greek Survey*

A different strategy was used for distributing the self-administered questionnaire in Greece. The main reason behind this was that postal distribution proved to be impractical, due to difficulties over obtaining an up-to-date, unbiased mailing list. On top of this, the response rate of a small pilot of hand-posted questionnaires was very poor at 2.5%. Therefore, it was decided that the best approach was to conduct a random web-based questionnaire, followed up by manually distributing a paper version of the questionnaire to targeted socio-economic groups that were not appropriately covered by the web-based questionnaire.

In October 2011, the survey was first translated into Greek (see Appendix C), with particular care being taken to ensure that the meaning of the questions was exactly the same in both English and Greek before it was distributed via email to several different email lists. (Only one difference was noticed was that the term ‘ethnicity’ does not exist in Greek, so when participants answered questions about their ethnicity, they answered with their nationality which is slightly different). These distribution lists included the staff and students of the Technical University of Crete, The Hellenic Institute of Transport and ITS-Hellas. Participants were also asked to forward the questionnaire to their friends and family.

The web-based questionnaire received 118 responses, mainly from students and employed males. To improve this sample, a paper version was manually distributed to random members of the public in various locations around Chania, Crete. In order to ensure that all social-economic groups were covered, no location was visited more than once, and on each occasion, slightly different groups of people were targeted. To ensure that the questionnaire remained self-administered, the participants were not given any help or assistance with filling out the questionnaire, to ensure that this was consistent with all of the other surveys that have been conducted to date. The distribution lists that the first emails were sent to (before they were forwarded on) would ideally have been more detached from the ITS field so that any potential for the samples involvement in the field of ITS impacting the results could be eliminated. Unfortunately, it proved very difficult to source a more neutral list and whilst there is some potential for the initial distribution list to influence the results of the survey the majority of the Greek sample (all of the paper responses) were likely to have no direct link to the field of ITS. This ensured that fair comparisons of each countries results could be made.

In total, 130 paper versions of the Greek questionnaire were completed, meaning that the total Greek response was 248. The demographic make-up of the Greek responses can be seen in Table 4-6. It is clear from this table that virtually all of the socio-economic groups are well covered. However, some of the groups are underrepresented; people aged over 66, people who earn over €60,000 and the unemployed. This is not ideal, but fortunately the UK sample covered all of these areas well so through analysis about the impact these factors have on people's privacy decision-making can still be conducted.

#### *4.5.4. Dutch Survey*

In February 2012, the Greek survey strategy was also used to distribute the survey in the Netherlands. Again, the main reason behind this was that postal distribution proved to be impractical, because of difficulties in obtaining an up-to-date, unbiased mailing list. The survey was first translated into Dutch (see Appendix D) and both a paper and web-based version of the questionnaire was produced. The web-based questionnaire was then distributed through contacts at the University of Delft and a variety of Netherlands-based private companies. The distribution list comprised of a mix of people who had direct links with the transportation field and some that did not. This approach received 147 responses, mainly from students and employed males.

To improve this sample, a paper version of the questionnaire was manually distributed to random members of the public in various locations around Delft, The Hague and Rotterdam. In order to ensure that all social-economic groups were covered, no location was visited more than once, and on each occasion, slightly different groups of people were targeted. To ensure that the questionnaire remained self-administered, the participants were not given any help or assistance with filling out the questionnaire, to ensure that this was consistent with all of the other surveys that have been conducted to date.

Unfortunately, due to extreme cold weather at the time of the survey, it proved fairly difficult to find people willing to participate in the survey. Only a total of 76 completed the survey by this method, meaning that the total Dutch response was 223. Of the four different countries sampled, the Dutch sample relied most heavily on the web-based version of the survey which meant that is the most susceptible sample to missing the views of people who were too worried about privacy concerns associated to disclose information over the internet. The demographic make-up of the Dutch responses can be seen in Table 4-6. It is clear from this table that virtually all of the socio-economic groups are covered. However, due to the difficulties faced with the targeted paper survey, the web-based sample which was a predominately male sample had a larger than ideal impact on the total Dutch sample and as a consequence, the total sample had a slight male dominance.

#### *4.5.5. Austrian Survey*

The Austrian survey was conducted in May 2012 using a similar strategy to that used in Greece and the Netherlands. The questionnaire was first translated into German, but unlike the Greek and Dutch questionnaires, no paper version of the questionnaire was created. Instead, only a web-based version was created, screenshots of which can be seen in Appendix E. Like the Dutch and Greek surveys, the first step was to distribute the web-based survey via email to several contacts through Technical University of Graz and several Austrian companies. This resulted in 122 responses, mainly from students and employed males.

To collect more responses and to balance the sample, several tablet devices were used to target random members of the public in various locations around Graz (in a similar way that paper versions of the questionnaire was used in the other countries). A tablet device was used instead of a paper version of the questionnaire as it was not only more efficient, but had been proven in the past to create better response rates, as for many of the participants it is the first time they had experienced tablet technologies (Rechter and Fellendorf 2012). To ensure that the questionnaire still remained self-administered, the participants were given a small amount of tuition on how to use the touchscreen devices before being left alone to complete the questionnaires unaided. One potential issue with using the tablet device was that technology was being used to survey views on technology but it was felt that the benefits of using the tablet devices outweighed the slight potential for bias. In total, 135 participants completed the survey via the tablet device, resulting in a total Austrian sample size of 257. The demographic make-up of the Austrian responses can be seen in Table 4-6. Like the surveys completed in the other countries, virtually all of the socio-economic groups are well covered.

#### *4.5.6. Sample Summary*

In total, 993 useful responses were received from the European survey. The Greek, Dutch and Austrian surveys effectively all used the same distribution strategies (web-based survey followed by targeted in-person questionnaires). This resulted in the samples in all three of these countries having a slight male bias as the initial web-based was distributed mainly through contacts in technical industries/universities where males significantly outnumber females. Additionally, because a significant proportion of the participants were either university students or staff, these samples include more students and highly educated people than an average cross-section of the country as a whole but in every country a views were received from the full cross-section of the public.

**Table 4-6 Demographic Make-Up of the European Survey**

		UK Survey (N=265)	Greek Survey (N=248)	Dutch Survey (N=223)	Austrian Survey (N=257)	Sample Total (N=993)
Gender	Male	49.4%	53.2%	57.4%	51.4%	<b>52.7%</b>
	Female	49.4%	43.5%	39.9%	45.1%	<b>44.7%</b>
	Declined to Answer	1.1%	3.2%	2.7%	3.5%	<b>2.6%</b>
Age	16-25	10.2%	22.6%	15.7%	23.7%	<b>18.0%</b>
	26-35	12.8%	33.1%	23.3%	28.0%	<b>24.2%</b>
	36-45	18.1%	16.1%	13.9%	14.8%	<b>15.8%</b>
	46-55	15.5%	14.1%	15.7%	13.2%	<b>14.6%</b>
	56-65	18.1%	5.6%	12.1%	5.4%	<b>10.4%</b>
	66-75	13.6%	1.2%	10.8%	3.5%	<b>7.3%</b>
	75 Plus	6.0%	0.0%	2.7%	0.8%	<b>2.4%</b>
	Declined to Answer	5.7%	7.3%	5.8%	10.5%	<b>7.4%</b>
Employment	Student	6.4%	28.2%	17.5%	26.5%	<b>19.5%</b>
	Employed	49.4%	46.4%	46.6%	48.6%	<b>47.8%</b>
	Retired	23.0%	7.3%	17.9%	7.8%	<b>14.0%</b>
	Unemployed	5.7%	2.4%	3.1%	1.9%	<b>3.3%</b>
	Other	13.6%	12.1%	12.1%	12.1%	<b>12.5%</b>
	Declined to Answer	1.9%	3.6%	2.7%	3.1%	<b>2.8%</b>
Household Income	Less than €20,000	29.4%	47.6%	37.2%	38.1%	<b>38.0%</b>
	€20,000-€39,999	32.5%	23.8%	26.9%	24.5%	<b>27.0%</b>
	€40,000-€59,999	12.8%	8.9%	14.3%	10.9%	<b>11.7%</b>
	€60,000-€79,999	8.3%	2.0%	4.0%	3.9%	<b>4.6%</b>
	More than €80,000	4.5%	1.6%	3.1%	2.7%	<b>3.0%</b>
	Declined to Answer	12.5%	16.1%	14.3%	19.8%	<b>15.7%</b>
	Ethnicity	Majority	86.4%	86.3%	84.3%	82.1%
Minority		7.5%	4.4%	10.3%	7.0%	<b>7.3%</b>
Declined to Answer		6.0%	9.3%	5.4%	10.9%	<b>8.0%</b>
Education Level	None	12.1%	8.9%	12.1%	7.8%	<b>10.2%</b>
	Compulsory School	27.2%	3.2%	15.2%	7.4%	<b>13.4%</b>
	Non-Compulsory School	15.1%	23.8%	18.4%	31.5%	<b>22.3%</b>
	Undergraduate	17.7%	34.7%	24.7%	26.1%	<b>25.7%</b>
	Postgraduate	24.5%	24.6%	25.1%	21.8%	<b>24.0%</b>
	Declined to Answer	3.4%	4.8%	4.5%	5.4%	<b>4.5%</b>



This is clear to see when compared to the UK sample which used a different sampling technique. The majority of the participants in the UK survey were contacted by post, which allowed it to have a more even male/female split and was less dominated by students and highly educated people. The UK sample did, however, under-represent 20-40 year employed people and over-represent retired and unemployed people. However, the total European sample provides a representative sample of the four different countries, which will enable fair conclusions to be made about the impact of culture on privacy decision-making within the transport field.

#### 4.6. Summary

The method of data collection used to collect the quantitative data required to test the research model and to achieve the aims and objective of this research was a self-administered questionnaire that was distributed in four culturally diverse European countries via a multi-modal method. This questionnaire sought to investigate the participants' perceptions of the privacy variables before testing how the participants would act in a variety of privacy scenarios that were created out of the privacy variables the participant was questioned about earlier in the questionnaire. A total of 993 useful responses were received and the total European sample sufficiently covered all of the socio-economic groups so that the impact on future ITS users' privacy decision-making could be accurately measured using the appropriate statistical methods.



## 5. Concerns

### 5.1. Introduction

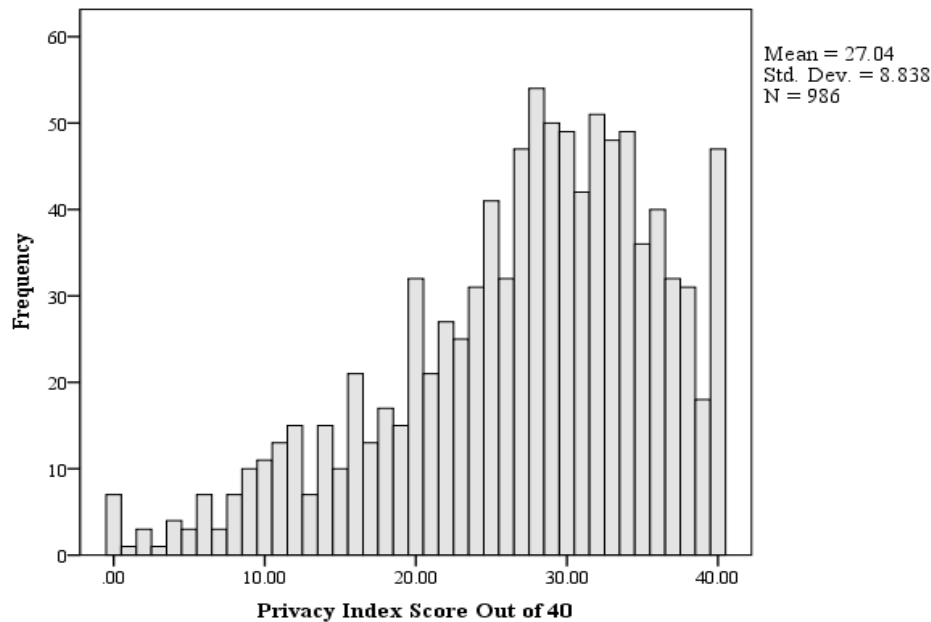
This Chapter will start to examine the research model developed in Chapter 3 and, in particular, it will explore the participants' level of privacy concern and their perceptions of the four privacy variables; the reward on offer, the sensitivity of the data required, the level of trust in the data holder and the level of trust in the transfer method. Chapters 2 and 3 highlighted that it is likely that a future ITS user's level of concern will play a role in whether they act in a privacy preserving manner or not. Previous research also suggests that a person's demographics would be heavily linked to their level of concern (Phelps et al. 2000 and Wallis 2007). This chapter will explore the extent to which the level of concern varies across the European survey sample and whether their demographic background influences these levels in the way that is expected; increase with age, be higher in females, be higher in ethnic minorities, vary from country to country, increase with education and income levels. This chapter will then move on to explore how the perceptions of the four ITS privacy variables (highlighted in Chapters 2 and 3) vary not only with the survey participant's demographics, but also with their expressed level of privacy concern.

### 5.2. Levels of Concerns

Section A of the European survey included four questions that Westin had previously used to classify a participant's level of privacy concern (Kumarguru 2005). The participants were asked to give a score between 0 (do not agree at all) and 10 (fully agree) for the following four statements:

1. You are concerned about threats to your privacy today
2. Organisations seek excessive amounts of information from consumers
3. Federal governments invade citizens' privacy
4. You have lost control over the circulation of your personal information

Figure 5-1 shows a histogram of the total privacy index score out of 40 for the complete European sample. Except for a small proportion of the sample scoring either 10 or 0 for every statement, the histogram shows the privacy concern totals have a negatively skewed normal distribution with a mean score of 27 out of 40. This result is slightly surprising as it was expected that three distinct groups would be clearer; the Fundamentalists, the Unconcerned and the Pragmatics. Instead, approximately 95% of the European survey sample has given non-extreme answers, which would suggest that they would fall within the pragmatic category.

**Figure 5-1 Histogram Showing the European Samples Privacy Index Scores out of 40**

If the survey participants are broken into four segments according to their total privacy index percentile, several demographic trends become apparent. Table 5-1 shows the demographic make-up of each of the four percentile segments. According to the demographic breakdowns, the participant's country had a large influence on their level of privacy concern. This can be seen clearly from Figure 5-2, which shows the observed minus expected number of participants in each segment from each of the different countries. Participants in the United Kingdom and the Netherlands appear to be more concerned about privacy as they have a greater than expected number of participants; the opposite is true for Austria and Greece. This supports previous research that suggests a person's cultural background will have a large influence on their attitude towards personal privacy. It is unlikely that these differences in concern level could have been caused by differences in the distribution methods used in each country. The reason behind this is that the Dutch and UK surveys had the highest and lowest use of a web-based distribution method yet they exhibit fairly similar concern levels which would not be expected in the distribution method had a direct link to the concern levels expressed.

A point to note is that the United Kingdom and the Netherlands have the highest scores for the individualism dimension; 89 and 80 respectively. These results therefore go against the predicted outcome (that countries with high individualism will be less concerned about privacy (Maynard and Taylor 1996 and IBM 1999)) but supports the findings of work conducted Millberg, Smith and Burke (2000) which showed that privacy concern increased with the individualism dimension.

**Figure 5-2 Percentage of Observed Participants Minus Percentage of Expected Participants in each Privacy Concern Quartile Split by Country**

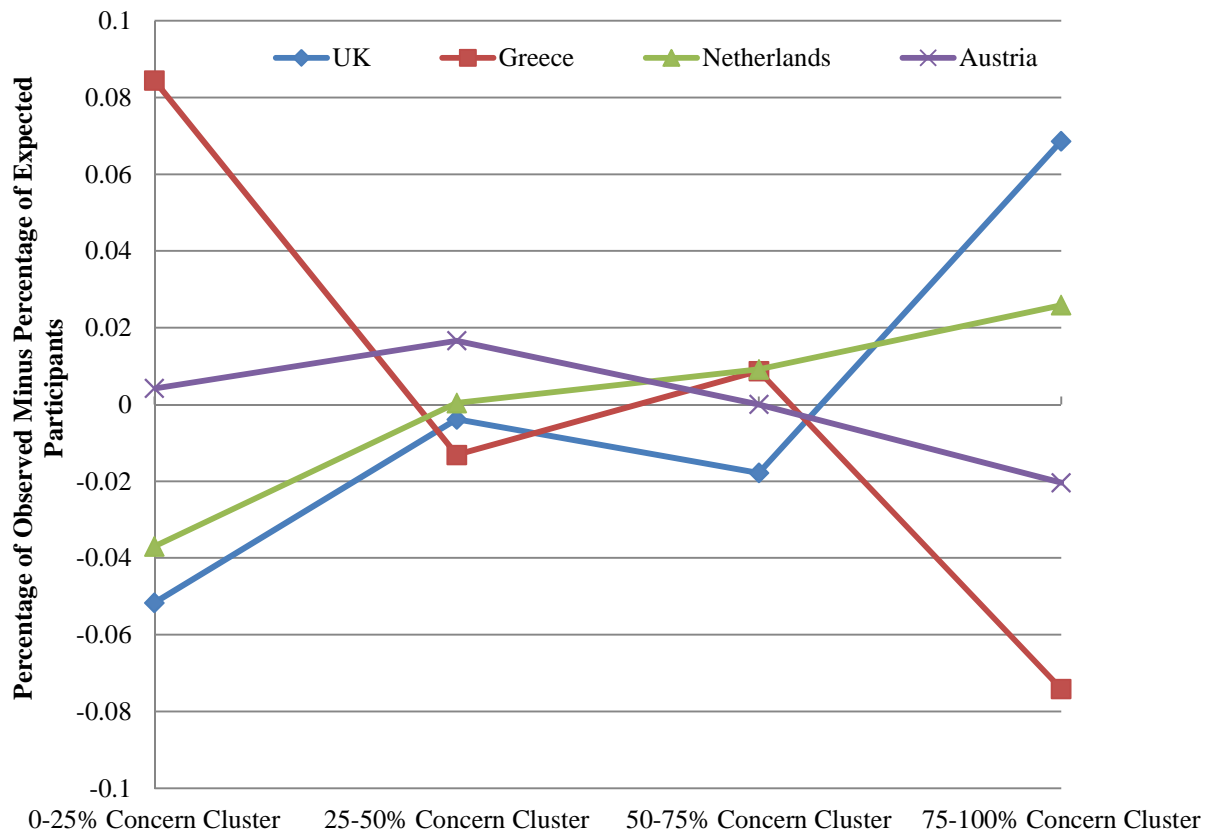


Table 5-1 also shows that in addition to their cultural background, a participant's gender and income level seemed to be directly linked to the level of privacy concerns. The percentage of females in each segment steadily increased as the level of concern increased. The number of high-income participants present in each segment increased as the mean concern level of the segment also increased. From the analysis of the concern segments, no clear trends can be seen for the influence of age, education level, whether the participant was in the ethnic minority or whether they have previously experienced an invasion of their privacy have on the participant's level of concern.

**Table 5-1 Demographic Breakdown of the Level of Privacy Concern Quartiles**

Percentile	Age (Over 54)	Gender (Female)	Education		Wage (Under £/€20000)	Wage (Over £/€60000)	UK (Yes)	ND (Yes)	GR (Yes)	AT (Yes)	Minority (Yes)	Privacy Invasion (Yes)
			(University Level)									
0-25% (N = 238)	25.1	44.1	50.0		50.7	6.5	21.0	18.9	33.6	26.5	5.9	33.5
25-50% (N = 256)	32.2	44.3	58.2		44.7	9.7	25.8	22.7	23.8	27.7	8.6	32.7
50-75% (N = 238)	26.1	47.0	50.8		42.6	9.7	24.4	23.5	26.1	26.1	6.3	30.5
75-100% (N = 254)	30.4	48.0	48.6		42.9	10.5	33.1	25.2	17.7	24.0	7.2	34.8

**Table 5-2 Chi Squared Test for Independence for the Influence of Demographics on Privacy Concern Levels**

Variable	p	Significant?
Age	0.015	Yes
Gender	0.196	No
Education	0.052	Borderline
Income	0.215	No
Country	0.001	Yes
Minority	0.010	Yes
Experience	0.185	No

In order to identify and assess the trends across the sample, it is necessary to perform a statistical test which is suitable for examining categorical data, and a Chi Squared test for independence was judged the most appropriate method. The test requires a large sample size to ensure validity and with close to 1000 participants, this method is particularly appropriate (Greenwood and Nikulin 1996). Table 5-2 shows the results of a Chi Squared test for independence conducted on all of the demographic variables to determine if it identified any trends with the level of privacy concerns.

A Pearson Chi Square ( $p$ ) value less than 0.05 indicates the existence of a significant relationship; if it is larger than this there is none. One negative aspect of the Chi Squared test is that it will only identify where a trend exists but it will not give any reasons as to the type of relationship or why the relationships exist. Table 5-2 shows that significant trends exist between a participant's age, country and whether they are in the ethnic minority and their level of privacy concern. This is contrary to the earlier cluster analysis which showed that an individual's age has no bearing on their level of concern. The most likely rationale behind the disconnect between the analysis of the concern segments and the Chi Squared test results is that the Chi Squared test considered all of the various age groups whereas the analysis of the concern segments only looked only at how many participants were aged 55 or over. This suggests that age categories need to be explored in more detail.

**Figure 5-3 Percentage of Observed Participants Minus Percentage of Expected Participants in each Privacy Concern Quartile Split by Age Category**

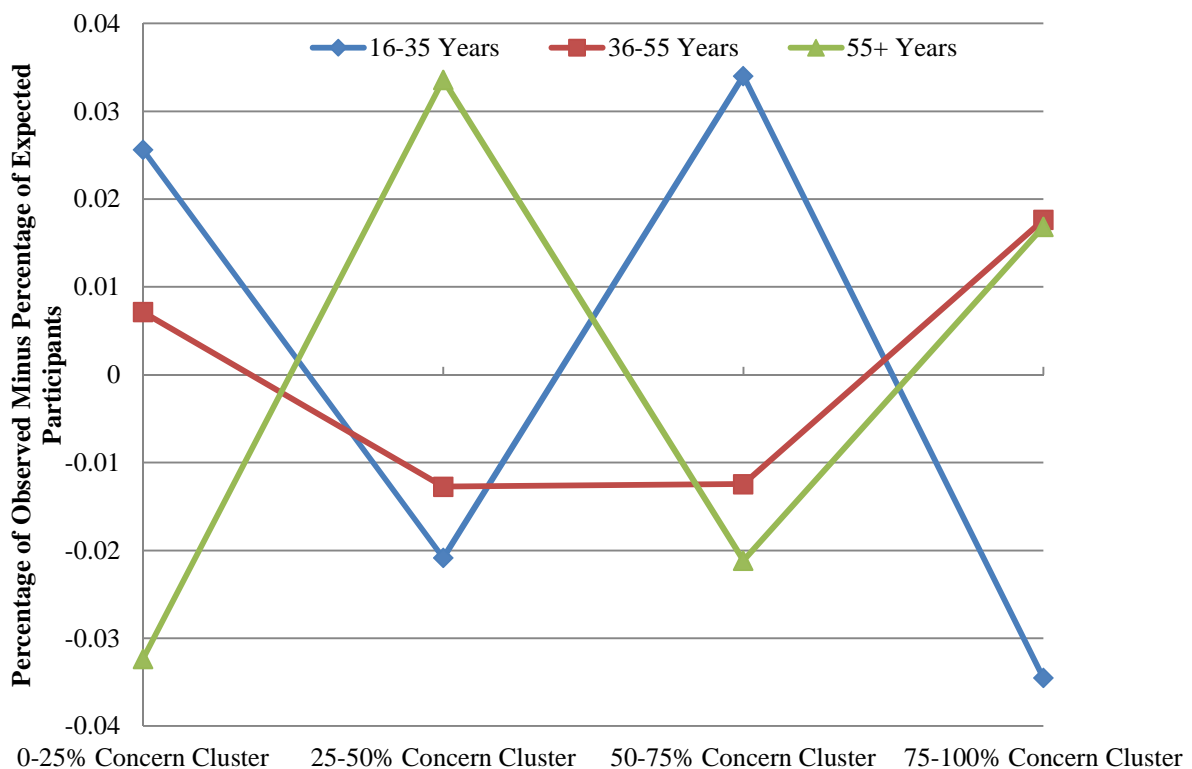


Figure 5-3 shows that whilst it is clear that some age categories are more likely to fall into specific concern segments than others, especially for the middle concern percentiles, no clear trends regarding the impact of age on the level of concern emerge. If, however, only the two extreme concern segments are taken into account, the results suggest that the level of concern significantly increases with age, which supports the findings of previous research (Fox et al. 2000, Phelps et al. 2000 and Wallis 2007).

Another factor that needs to be considered when analysing the results is the fact that it is possible that the impact of the participant's country (or another variable) is so dominant that it may disguise the individual impact of some of the other demographic influences such as gender, education etc.

The figures within Appendix F show the impact of the different variables by country and show how they appear to have a different impact in each country. For example, when split by country: gender is not important in the United Kingdom and Greece, but in the Netherlands women are more concerned than men. The opposite is true in Austria. It is also shown that minorities are less concerned in the United Kingdom, but more concerned in the Netherlands and Austria. The impact of household income is mixed in all the countries, except the United Kingdom where people with a low household income had a lower level of privacy concern. The effect of education level is interesting as it shows that highly educated people have a greater than expected number of participants in the middle two percentiles but not the two extreme clusters which could mean that they could be considered as Pragmatists. Even when split by country, no real trends emerged for the impact of age on the participants' levels of concern.

In order to model the impact of the demographic variables and their various two-way interactions, a backwards stepwise logistic regression was used to predict whether a participant was likely to be in the two highest concern clusters by using their demographic data and all of the two-way interactions between the demographics. Table 5-3 shows the output from the model. The model had a Cox and Snell  $R^2$  value of 0.298 and a Nagelkerke  $R^2$  value of 0.399 which indicates that participants' demographics and their two-way interactions account for between 30-40% of the variance in the participants' level of concern. The model improves the likelihood of identifying somebody who is in the top two privacy concern segments from 54.6% (by simply predicting that everyone is in the top two concern clusters) to 71.7% an improvement in accuracy of 17.1%.



The results of the European survey have shown that a person's demographics will significantly impact their level of privacy concerns. They also suggest that a person's age, cultural background and whether they are in the ethnic minority or not are particularly important. It has also been shown that it is important to consider the demographic two-way interactions, for example, it was shown that in the Netherlands females are more concerned about privacy than men, whereas in Austria the opposite was true. However, if only the impact of gender across the whole European sample is considered then no trend is discovered, as the effects in each country cancel each other. In general, however, the results of the European survey have supported much of the previous research that has looked into the influencing factors of a person's level of privacy concern, therefore it is fair to say that the evidence supports the first hypothesis in the research model.

*H1: A user's level of privacy concern will be impacted by their demographics such as their age, gender and cultural background. – SUPPORTED*

**Table 5-3 Variables in Binary Logistic Model of High Privacy Concern**

<b>Variable</b>	<b>Wald</b>	<b>df</b>	<b>Sig.</b>
Country	22.619	3	.000
Education	39.683	4	.000
Gender	40.018	1	.000
Wage	45.559	4	.000
Minority	19.058	1	.000
Minority * Wage	31.201	4	.000
Country * Minority	6.792	3	.079
Age * Minority	37.720	5	.000
Experience * Wage	8.765	4	.067
Gender * Experience	7.701	1	.006
Education * Experience	10.647	4	.031
Gender * Wage	53.383	4	.000
Education * Wage	73.040	16	.000
Country * Wage	23.851	12	.021
Age * Wage	62.894	20	.000
Country * Gender	9.409	3	.024
Age * Gender	10.211	5	.069
Country * Education	20.137	12	.065
Age * Education	55.071	20	.000

### 5.3. Perceptions of Privacy Variables

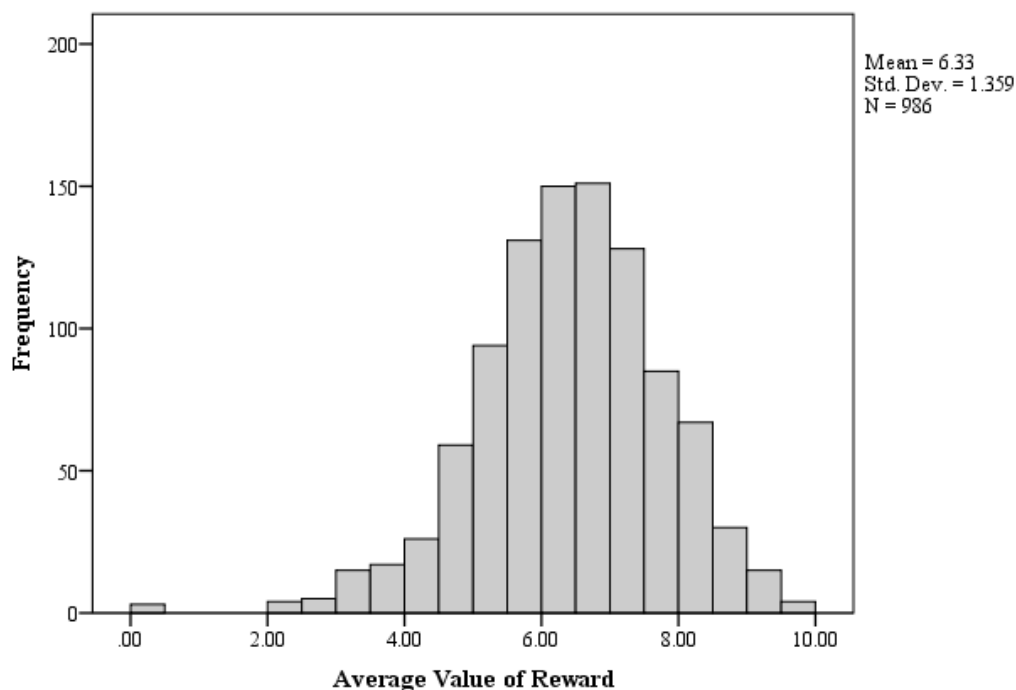
Unlike other previous research, the European survey sought to gather perceptions on the four privacy variables that could be present in a future ITS. Part B of the European survey asked the participant to grade on a scale of 0 to 10 how valuable, safe, and sensitive various different rewards, data holders, transfer methods and information types were.

#### 5.3.1. The Reward

The rewards that the participants of the survey were asked to consider were; improved safety, a cost saving, a time saving, an increase in their enjoyment, a reduction in their carbon emissions and an improvement in their social image. Figure 5-4 shows a histogram of the mean perception of the value of all the rewards. This graph shows that the participant's mean perception of the rewards on offer is distributed normally around a mean score of 6.3.

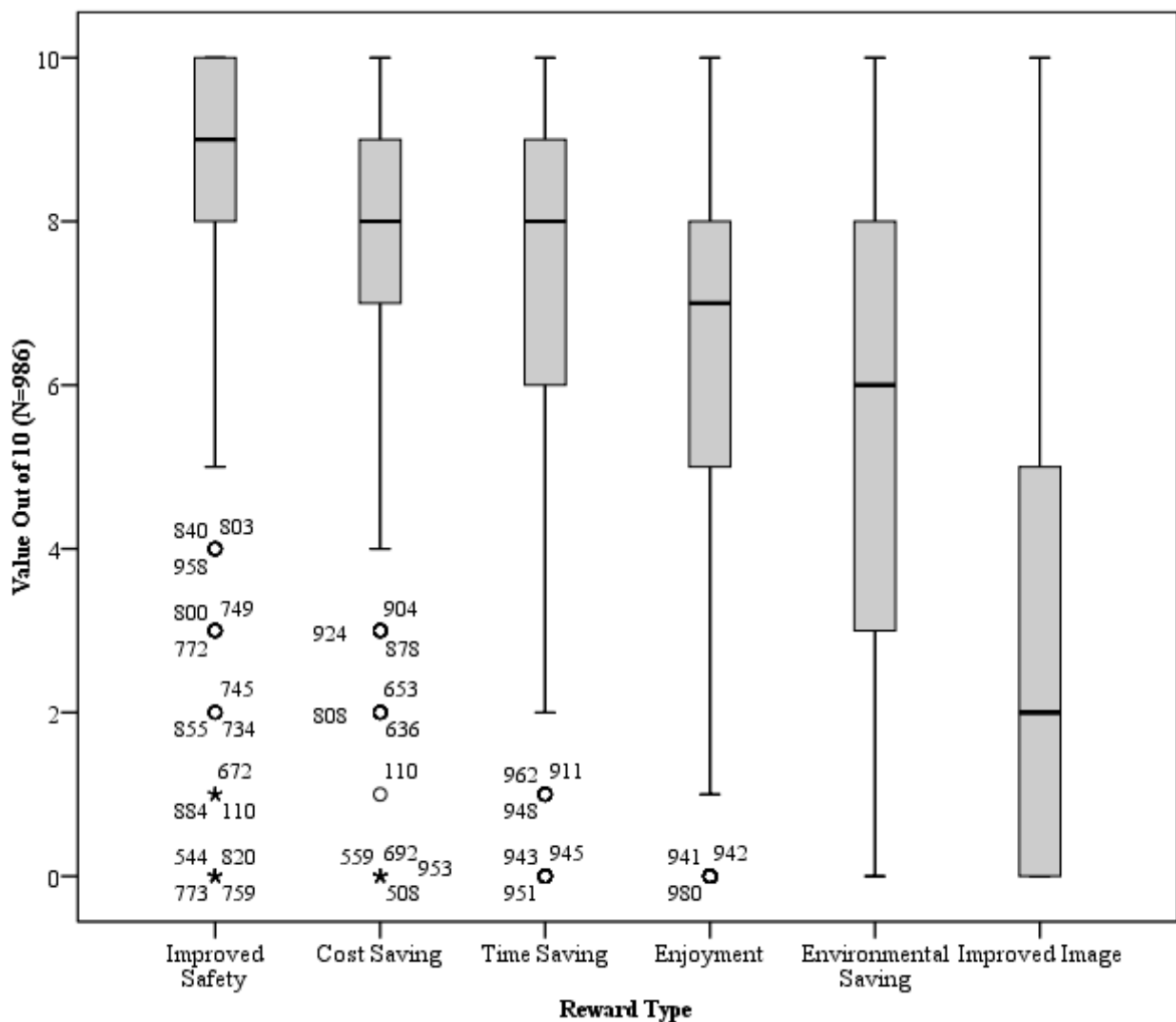
Figure 5-5 shows a breakdown of the perceptions of the different rewards. This shows that there is a clear hierarchy in the perceived value in the various rewards with improvements in safety being valued the most by the participants and improvements in their social image being the least valued. It also shows that the variance in the responses to the rewards with the lowest median value is higher than those with a high median response.

**Figure 5-4 Reward Histogram**



Appendix G contains histograms that show the distribution of the perceptions of each individual reward. They show that for the three most valuable rewards; improved safety, a cost saving and a time saving the distribution is a skewed normal distribution around the score 10. The opposite is true for the least valuable reward – an improvement in social image – whose distribution is a skewed normal distribution around the score 0. However, the distributions for the perceived value of an improvement to a person’s enjoyment and a reduction in carbon emissions are not distributed normally but are virtual level across all of the scores. This shows that there is no general consensus on how valuable these rewards are and people are just as likely to find them really valuable as they are to find them worthless. This could have a significant impact on future ITS that offer either improved enjoyment or a reduction in carbon emission as the reward for using their systems, as some people will see incredible value in such a reward while others will find no value at all.

**Figure 5-5 Value of Different Types of Reward**



Like the level of privacy concern, it was predicted that a participant's demographic background would significantly influence their perception of the value of the rewards offered by a new ITS. Table 5-3 shows the demographic background of the four reward quartiles. Table 5-4 shows the results of a Chi Squared test of independence on the impact someone's demographic background has on the value they hold in various rewards. The results of the Chi Squared test indicate that a person's age, education level and culture background all play significant roles in shaping a person's perception of the value of a reward.

By looking at the breakdown of the reward percentiles, it becomes clear that for the European survey sample, the over 55s place more value on the rewards on offer, that the highly educated place less value on the rewards on offer, and that citizens of the United Kingdom and Greece find the rewards more valuable than citizens in Austria (there is no clear trend for citizens of the Netherlands). It should also be noted that while the Chi Squared test ruled it insignificant, the demographic breakdown of the reward quartiles showed that females place higher value on the rewards on offer, and people who have previously experienced privacy invasions found the rewards less valuable than those who have not experienced a privacy invasion. These results support the hypothesis that a person's demographic background will influence their perception of the value of the reward a future ITS is offering.

*H2a: A user's perception of the reward on offer will be impacted by their demographics such as their age, gender and cultural background. – SUPPORTED*

### 5.3.2. Data Sensitivity

The types of information that the participants of the survey were asked to consider were their bank details, embarrassing secrets, medical record, income details, purchase history, location history, driving behaviour data, nationality, musical preferences and local weather conditions. Figure 5-6 shows a histogram of the mean perception of the sensitivity of all the data types. This histogram shows that the participants mean perception of the sensitivity of the data is distributed normally around a mean score of 5.8.

**Table 5-4 Demographic and Privacy Concern Breakdown of the Reward Perception Quartiles**

Percentile	Education											
	Age (Over 54)	Gender (Female)	(University Level)	Wage (Under £/€20000)	Wage (Over £/€60000)	UK (Yes)	ND (Yes)	GR (Yes)	AT (Yes)	Minority (Yes)	Privacy Invasion (Yes)	Concern Cluster (75%)
0-25% (N = 260)	21.9	37.5	54.1	47.8	8.3	23.5	20.0	17.7	38.8	8.5	35.5	23.8
25-50% (N = 243)	30.3	48.5	56.5	40.0	9.7	23.9	23.9	19.3	32.9	6.2	39.4	25.9
50-75% (N = 245)	29.3	44.6	55.8	41.1	8.7	25.3	24.9	27.3	22.4	6.5	28.3	24.1
75-100% (N = 238)	32.3	53.4	41.3	51.5	9.9	32.4	21.8	37.0	8.8	7.6	28.2	29.4

**Table 5-5 Chi Squared Test for Independence for the Influence of Demographics and Privacy Concern on the Reward Perception**

Variable	p	Significant?
Age	<0.0001	Yes
Gender	0.170	No
Education	0.014	Yes
Income	.0531	No
Country	<0.0001	Yes
Minority	0.069	No
Experience	0.440	No
Privacy Index	<0.0001	Yes

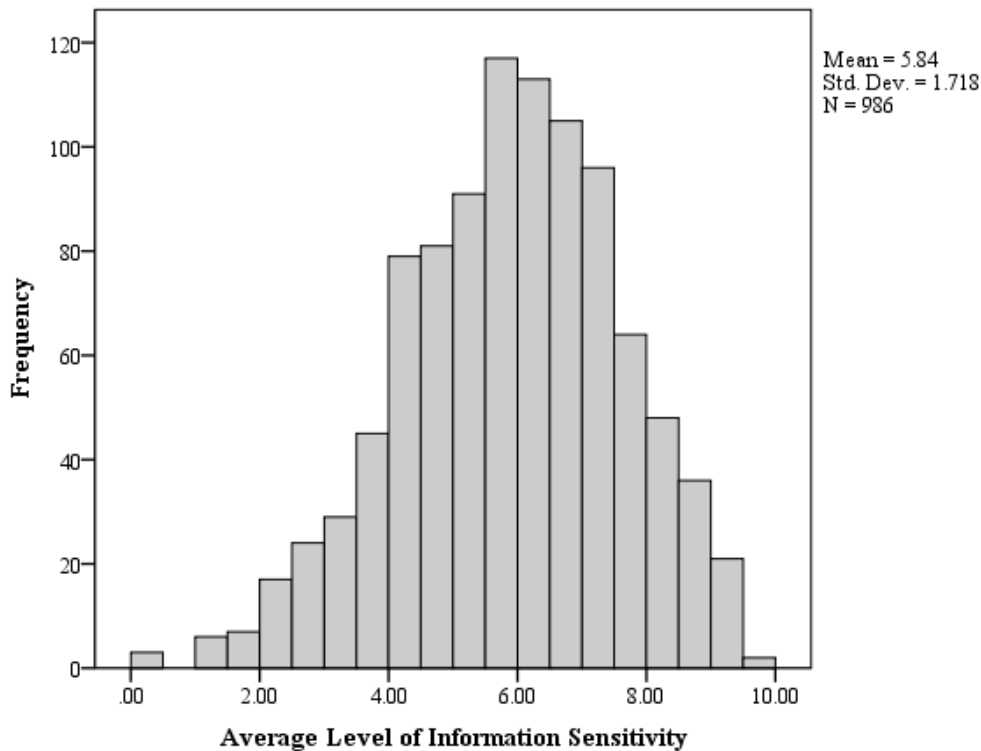
**Figure 5-6 Information Sensitivity Histogram**

Figure 5-7 shows the distribution of the values attributed to the different data types. This shows that there is a clear hierarchy in the perceived sensitivity of different types of personal information that could be required by future ITS. The most sensitive information includes information about participants' bank details and secrets, whereas the least sensitive personal information includes information about the participants' musical preferences and local weather conditions. This supports the findings of Rose J, Rehse O and B Röber (2012). It should be noted that the two data types that are likely to be most sought after by future ITS – location history and driving behaviour – have a middle-level median value. Figure 5-7 and the graphs in Appendix H, show that in a similar way to the value of enjoyment and helping the environment, the sensitivity of the participants' location and driving behaviour data have a flat distribution. This indicates that whilst some people would be very reluctant to disclose this information, others would have no problem at all. The flat distribution also suggests that future ITS users will find it hard to calculate how sensitive this information is and that no general consensus has been formed, unlike for all of the other information types where the distributions were all normally distributed and skewed towards either 0 or 10.

A lack of knowledge from the participants as to how and why information about their driving behaviour, purchase and location histories will be used could contribute to the large variance in the perceptions of how sensitive this information is. This is something that future research could explore further and in particular whether educating future ITS users about how their personal information will be used will impact the perception they have on the sensitivity of a particular data type.

Figure 5-7 Sensitivity of Information Types

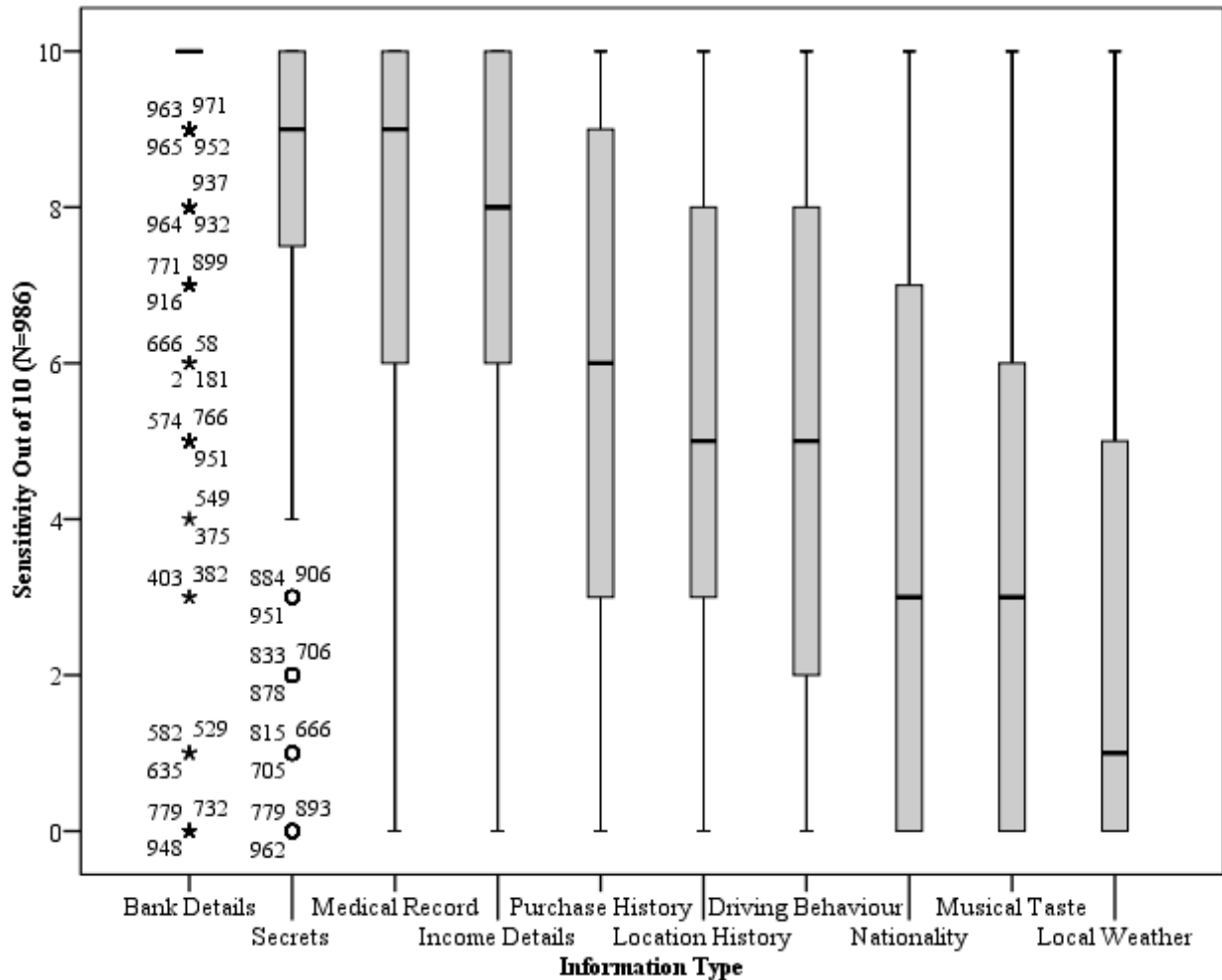


Table 5-6 shows the demographic background of the four data sensitivity quartiles and Table 5-7 shows the results of a Chi Squared test of independence for the impact demographics have on how sensitive the participants found their personal information to be. The results of the Chi Squared test suggest that only a person's age and culture background have a significant influence; both variables have already been significant in influencing the participants' level of concern and perception of reward value.

**Table 5-6 Demographic and Privacy Concern Breakdown of the Data Sensitivity Perception Quartiles**

Percentile	Age	Gender (Female)	Education	Wage (Under £/€20000)	Wage (Over £/€60000)	UK (Yes)	ND (Yes)	GR (Yes)	AT (Yes)	Minority (Yes)	Privacy Invasion (Yes)	Concern Cluster (75%)
	(Over 54)		(University Level)									
0-25% (N = 246)	34.2	43.1	51.9	43.2	11.8	39.8	22.0	17.5	20.7	7.3	22.8	28.5
25-50% (N = 253)	25.9	43.4	50.0	44.8	5.7	28.1	24.5	20.9	26.5	4.7	37.8	23.7
50-75% (N = 245)	24.8	45.5	56.8	42.6	8.5	20.8	23.3	24.5	31.4	11.0	38.6	28.6
75-100% (N = 242)	29.6	51.5	49.1	50.5	9.1	15.7	20.7	38.0	25.6	5.8	32.4	22.3

**Table 5-7 Chi Squared Test for Independence for the Influence of Demographics and Privacy Concern on the Perception of Data Sensitivity**

Variable	p	Significant?
Age	0.006	Yes
Gender	.180	No
Education	.260	No
Income	.544	No
Country	0.009	Yes
Minority	0.569	No
Experience	0.225	No
Privacy Index	<0.0001	Yes

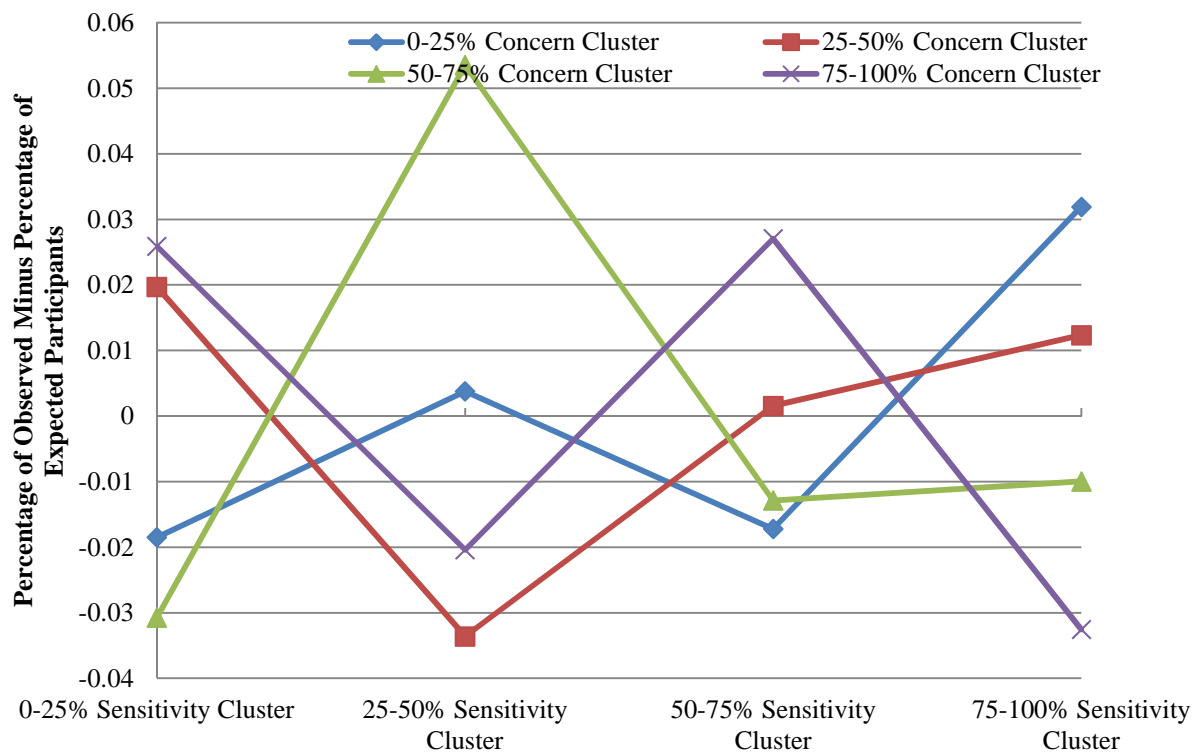


By looking at the breakdown of the sensitivity percentiles, it becomes clear that the over 55s find their personal information less sensitive than the under 55s, which is contrary to the impact age has on the level of privacy concern. Participants from the United Kingdom had the lowest level of data sensitivity whereas the Greek and Austrian participants had a high level of data sensitivity. Again there is no clear trend for citizens of the Netherlands.

It should also be noted that while the Chi Squared test ruled it insignificant, the demographic breakdown of the sensitivity quartiles shows that females find their personal information more sensitive than men. Participants who have previously experienced privacy invasions were also more sensitive regarding their personal information. Both these variables have previously been proven to have the same effect on a person's level of privacy concern. It is therefore clear that a person's demographic background does impact their perception of how sensitive their personal information is, which supports Hypothesis 2b.

*H2b: A user's perception of the data sensitivity will be impacted by their demographics such as their age, gender and cultural background. – SUPPORTED*

**Figure 5-8 Percentage of Observed Participants Minus Percentage of Expected Participants in each Sensitivity Quartile Split by Their Privacy Concern Quartile**



The research method also expected there to be a correlation between a future ITS user's level of privacy concern and their data sensitivity. In Table 5-7, the results of the Chi Squared test of independence show that the link between the two is significant. Figure 5-8 compares the observed minus expected number of participants for each sensitivity and concern segment. This figure shows that there are fewer participants in the low sensitivity and low concern level quartiles than expected, whilst there are more than expected participants in the high sensitivity and low level of concern segments. The opposite is also true of the high concern quartile. Figure 5-8 also shows that there are no clear trends for the middle concern quartiles. As these are only single effect values, more underlying influences could be discovered by looking at the two-way interactions between the variables. This is something that is explored in the next two chapters.

It would have been expected that people who are concerned about privacy in general would also find their personal information sensitive. However, the results of the European survey actually indicate that the opposite is true. Unfortunately the reasoning behind this remains unclear. In the research model, it was hypothesised that as level of concern increases the perception of how sensitive information is would also increase. This has been disproved by the results of the European survey.

*H3a: A user's perception of the data sensitivity will be linked to the user's general level of privacy concern. – NOT SUPPORTED*

### *5.3.3. Trust in Data Holder*

How safe the participants perceive their personal information to be in the hands of various data holders was also measured in Part B of the European survey. They were asked to consider the following data holders; family members, close friends, medical and legal professionals, work colleagues, the government, private companies, journalists, strangers and criminals. Figure 5-9 shows a histogram of the mean perception of safety for all the different data holders. This histogram shows that the participants mean perception of the sensitivity of the data is distributed normally around a mean score of 4.3.

Figure 5-10 shows the mean value attributed to the different data types. This shows that there is a clear hierarchy in the perceived level of trust the participants had in the different data holders. They perceive their information to be the most secure with family members and close friends and least secure with criminals and strangers. It is unlikely that any future ITS will actually give information to the data holders that are perceived as being the most secure, but some could give data to complete strangers and this could prove to be to the detriment of future ITS. The next two chapters will explore this in more detail.

Figure 5-9 Trust in Data Holder Histogram

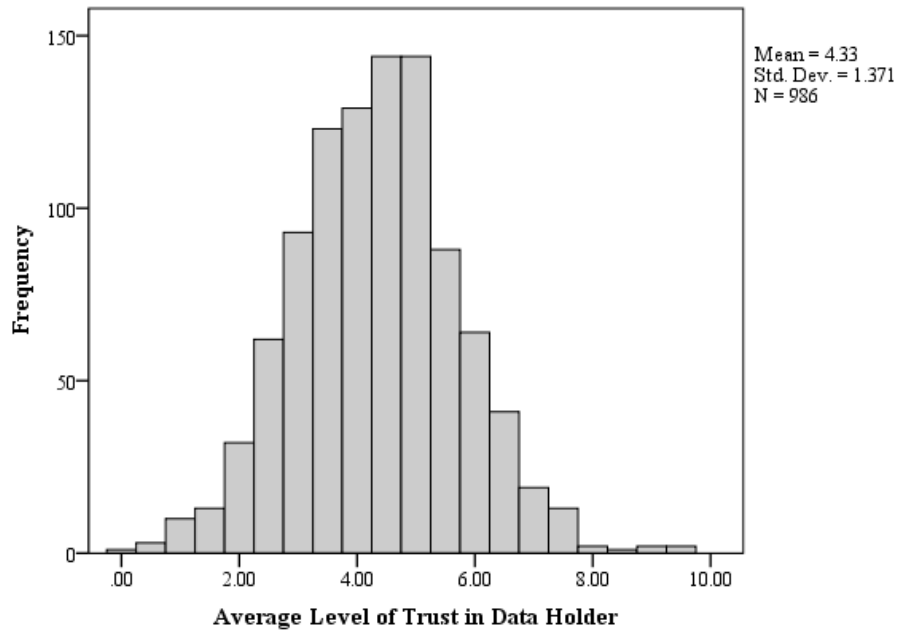
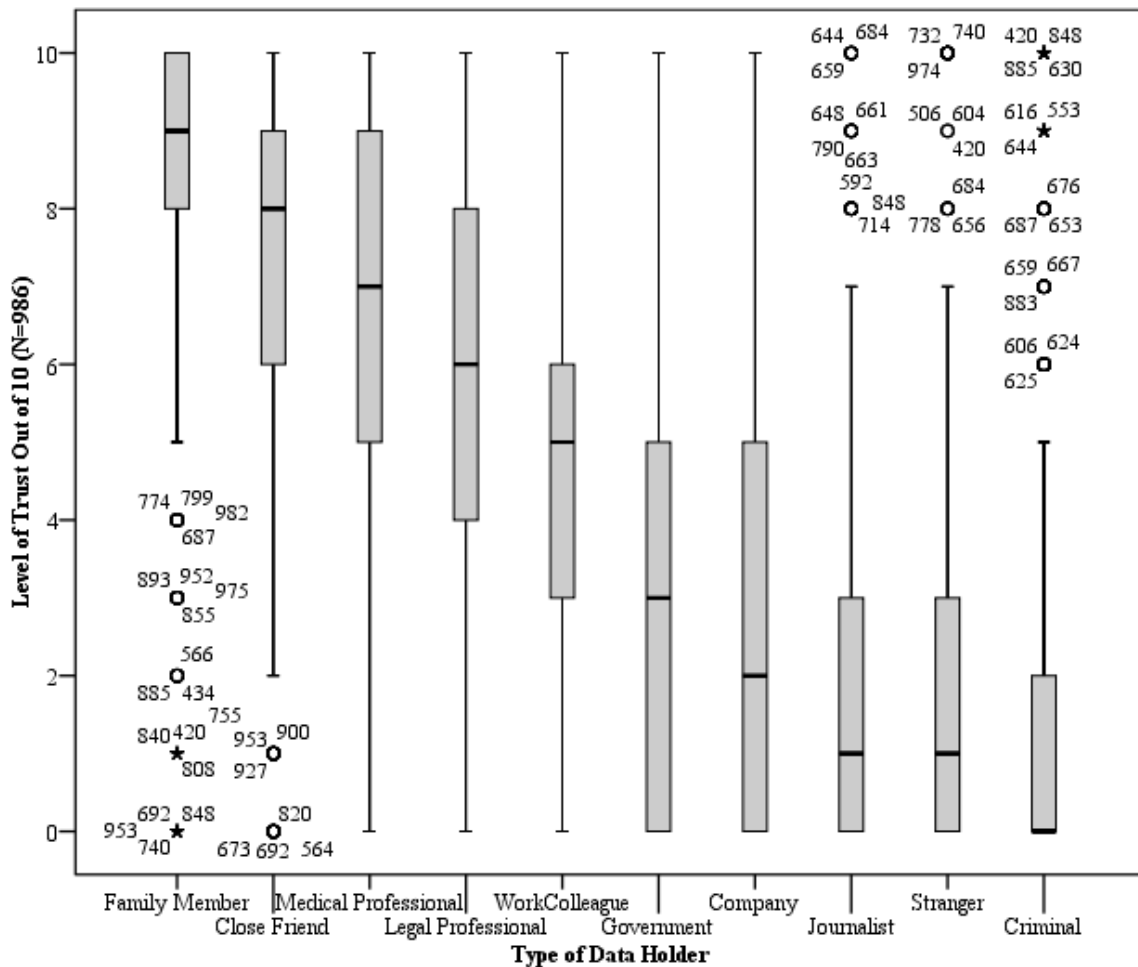


Figure 5-10 Trust in Individual Data Holders



Appendix I shows the distribution for the specific data holders. Compared to the previous two privacy variables, the distribution of the perceptions of all of the data holders are significantly flatter. This indicates that the participants' views on how secure their personal information is with different people are much more varied and harder for the participants to judge with any great consistency. The demographic background of the four data holder quartiles are shown in Table 5-8. Table 5-9 shows the results of a Chi Squared test of independence on the impact demographics have on how safe the participants feel their personal information will be with various data holders. The results of the Chi Squared test again show that a person's age and culture background have a significant influence on the privacy variable.

The breakdown of the data holder percentiles (Table 5-7) show that participants from the United Kingdom and the Netherlands perceive their personal information to be safer in the hands of others than the participants from Greece and Austria. Participants who had experienced previous invasions were also less trusting of the data holders having their information. By looking at the over 55 age category alone, no clear trend is apparent. It is likely that other age categories have very different perceptions of the data holders. Although they are not statistically significant, the data holder quartiles also suggests that less educated people are more trusting, that high earners are more trusting and that non-minorities are less trusting. These results present enough evidence to support Hypothesis 2c.

*H2c: A user's perception of how safe their information is with different data holders will be impacted by their demographics such as their age, gender and cultural background. – SUPPORTED*

Unlike for the perception of data sensitivity, the results of the Chi Squared test for independence in Table 5-8 showed that there was no statistically significant relationship between a participant's level of concern and their perception of how safe their information is with different data holders. Figure 5-11, however, shows that although the perceptions of the three most concerned quartiles have very similar perceptions of the data holders the least concerned segment have very different perceptions of how safe their information is with the different data holders. This quartile has a more than expected number participants in the low data holder trust segment, and a less than expected number of participants in the high level of data holder trust segment. This is opposite to the results that would have been expected and could purely be showing nothing more than that some of the participants scored low on all of the scale questions throughout the questionnaire. As a consequence, the results of the European survey do not support Hypothesis 3b.

*H3b: A user's perception of how safe their information is with different data holders will be linked to the user's general level of privacy concern. – NOT SUPPORTED*

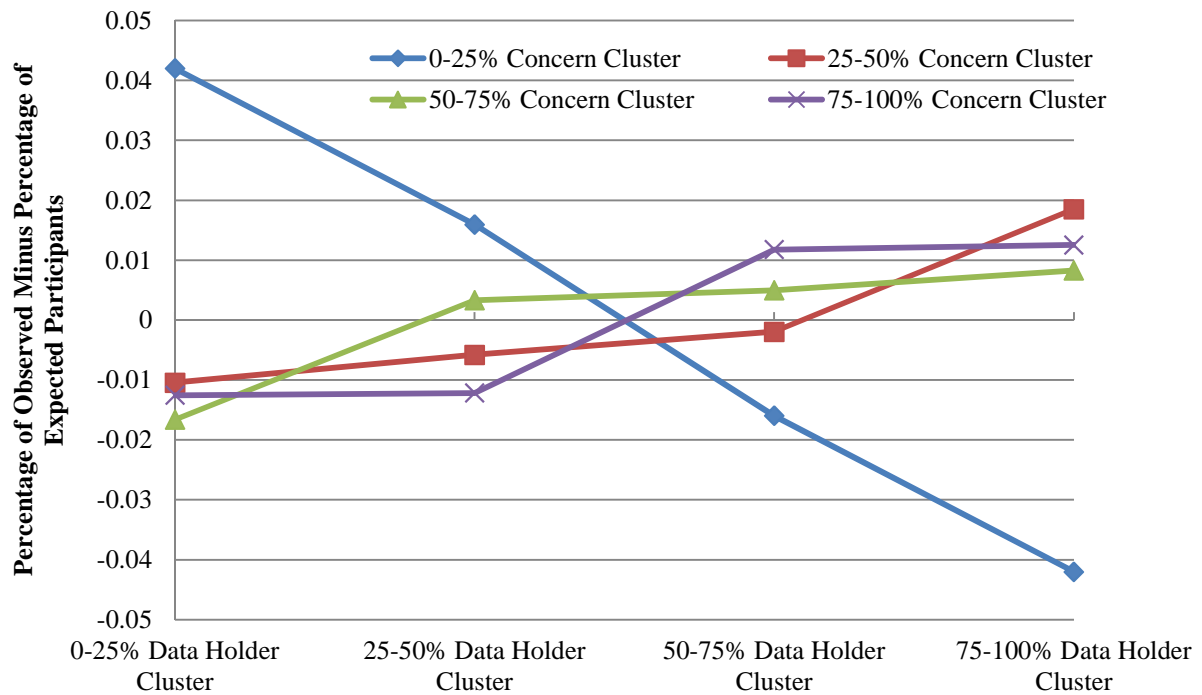
**Table 5-8 Demographic and Privacy Concern Breakdown of the Data Holder Trust Quartiles**

Percentile	Age	Gender (Female)	Education	Wage (Under £/€20000)	Wage (Over £/€60000)	UK (Yes)	ND (Yes)	GR (Yes)	AT (Yes)	Minority (Yes)	Privacy Invasion (Yes)	Concern Cluster (75%)
	(Over 54)		(University Level)									
0-25% (N = 257)	27.9	43.7	52.8	49.8	9.2	21.8	10.1	33.9	34.2	4.3	37.7	24.5
25-50% (N = 237)	29.8	46.5	56.3	42.7	9.2	24.9	17.7	30.4	27.0	7.6	36.5	24.5
50-75% (N = 260)	27.7	43.0	51.1	43.9	5.9	27.7	24.2	20.8	27.3	8.8	31.2	26.9
75-100% (N = 232)	29.0	50.7	47.8	44.0	12.5	30.6	39.7	15.1	14.7	8.2	25.8	27.2

**Table 5-9 Chi Squared Test for Independence for the Influence of Demographics and Privacy Concern on the level of Data Holder Trust**

Variable	p	Significant?
Age	<0.0001	Yes
Gender	0.053	No
Education	0.062	No
Income	0.318	No
Country	0.002	Yes
Minority	0.141	No
Experience	0.043	Yes
Privacy Index	0.184	No

**Figure 5-11 Percentage of Observed Participants Minus Percentage of Expected Participants in each Data Holder Quartile Split by Their Privacy Concern Quartile**



#### 5.3.4. Trust in Transfer Method

The final section of Part B of the European survey investigated how safe the participants perceive their personal information to be whilst being transferred by various different methods. They were asked to consider the following transfer methods; face-to-face in private, face-to-face in public, postal mail, landline telephone, mobile telephone, text message, wired email and wireless email. Figure 5-12 shows a histogram of the mean perception of safety for all the different transfer methods. This histogram shows that the participants mean perception of the sensitivity of the data is distributed normally around a mean score of 4.6.

Figure 5-13 shows the distribution of the perceptions of the different data types. Unlike for the other privacy variables, this does not show a clear hierarchy in the perceived level of trust. Instead, the results suggest that other than face-to-face meeting in private, all of the other transfer methods were perceived as being very equal in terms of security. This suggests that the participants find it very difficult to differentiate between the actual levels of security of each transfer method so they perceive them all to be the same.

Figure 5-12 Trust in Transfer Method Histogram

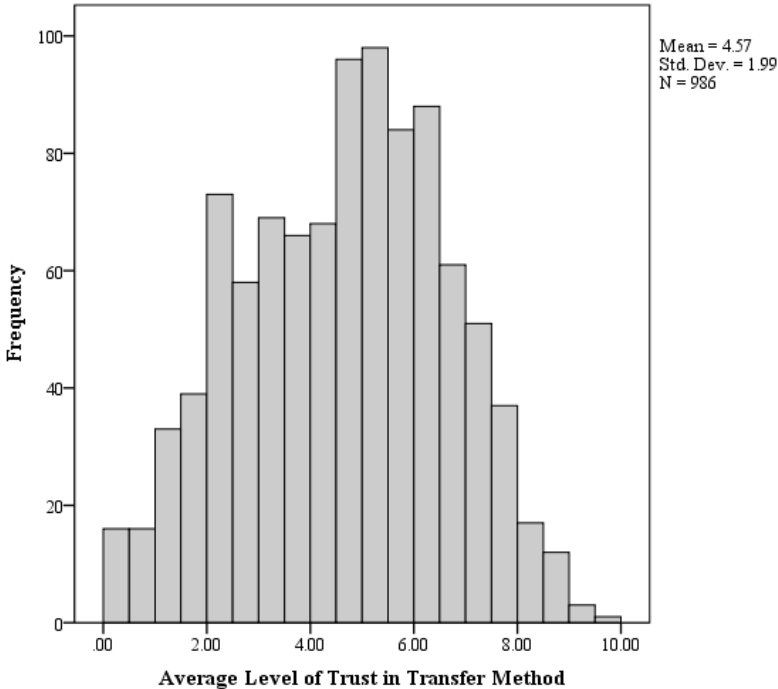
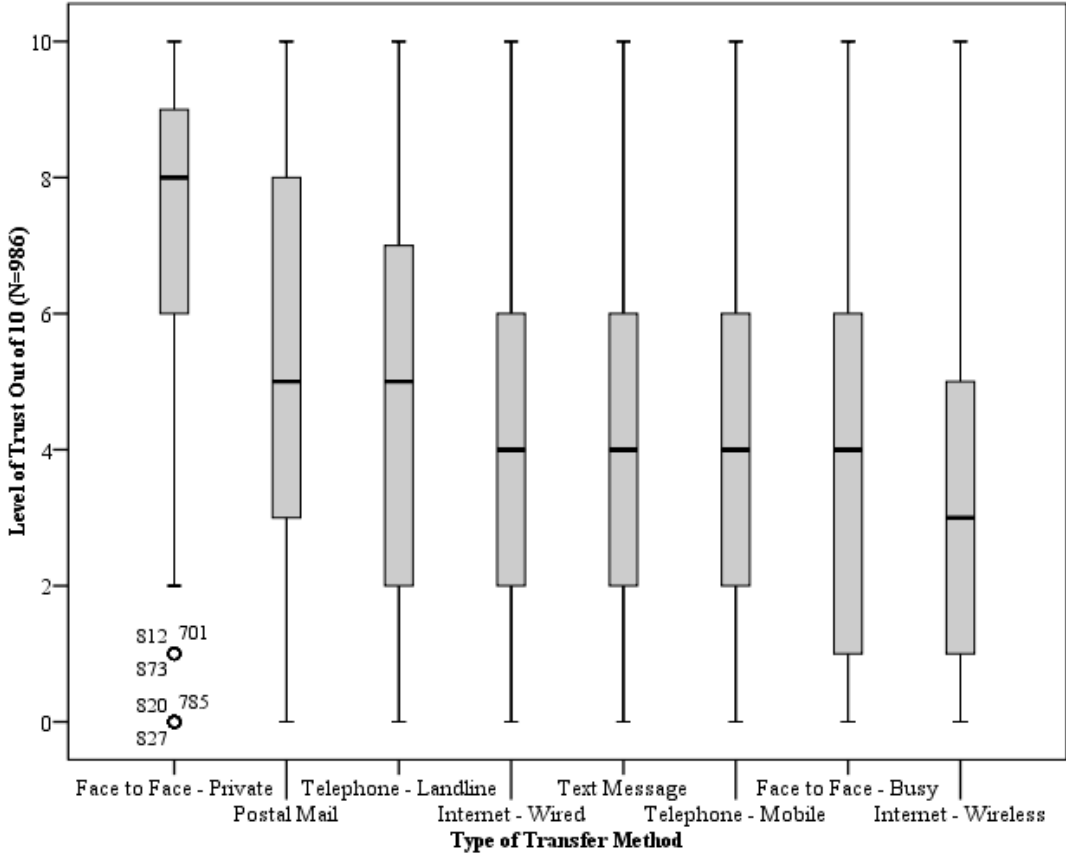


Figure 5-13 Trust in Individual Transfer Methods



This point is supported further by the distributions of the individual transfer methods found in Appendix J. Unlike for the other privacy variables, all of the transfer methods except face-to-face in private have a flat normal distribution centred on a score of roughly four out of ten. Again, this demonstrates that there is a lot of variance in the participants' perceptions and it is possible that because of doubt over the actual relative security of each transfer method, they simply scored each somewhere in the middle.

The Cronbach's alpha for the perceptions of the different transfer methods was 0.847. Cronbach's alpha provides a measure of the internal consistency of a test or scale, a score between 0 and 1 is given. A Cronbach's alpha greater than 0.7 suggests that a good level of consistency exists between the different variables (Kline 2000). For comparison, the Cronbach alpha of the perception of the reward type was 0.470, the perception of the information type 0.762 and the perception of the different data holders 0.729. This shows that if a participant perceived one transfer method to be safe then they were likely to feel that another transfer method is also safe. This supports the theory that the participants struggled to differentiate between the different transfer methods more than the other privacy variables.

The scores of 0.762 and 0.729 for the sensitivity of data and trust in data holders respectively suggests that participants scored fairly consistently across all the different information and data holder types, but not quite to the same degree as for the different types of transfer method. The Cronbach's alpha for the perception of the different rewards, on the other hand, showed that different participants scored some rewards high in value and others low in value. This may be a result of participants finding it easier to clearly differentiate between the different types of rewards compared to the other privacy variables.

Table 5-10 has broken down the demographic backgrounds of the four transfer method quartiles, while Table 5-11 shows the results of a Chi Squared test of independence for the impact demographics have on how safe the participants feel it is to transfer their personal information via various different method. The results of the Chi Squared test again show that a person's age and cultural background have a significant influence. They also show that both a person's gender and level of income were related in a statistically significant way to their perception of how safe a transfer method is.



Table 5-10 indicates that participants from the Netherlands are more trusting of the transfer methods than participants from Greece and Austria, whilst the response from participants in the United Kingdom was very mixed. Participants aged over 55 were shown to be less trusting of the different transfer methods, as were females and those on a low income. Although the Chi Squared test reports they are not statistically significant, the quartile breakdown also indicates; that less educated people are less trusting, that minorities are less trusting and that those with experience of previous privacy invasions are also less trusting of the transfer methods. These results present enough evidence to support Hypothesis 2d.

*H2d: A user's perception of how safe a transfer method is will be impacted by their demographics such as their age, gender and cultural background. – SUPPORTED*

The results of the Chi Squared test for independence in Table 5-11 show that there is a statistically significant relationship between a participant's level of concern and their perception of how safe the various transfer methods are. However, from Figure 5-14, which is only looking at single effects, it is not possible to see any trends between the level of a participant's concern and their perception of the safety of the various transfer methods. Even though the Chi Squared test for independence suggests the two variables are statistically linked, due to the randomness of Figure 5-14, the results of the European survey do not support Hypothesis 3c.

*H3c: A user's perception of how safe a transfer method is will be linked to the user's general level of privacy concern. – NOT SUPPORTED*

#### 5.4. Summary

The analysis of Parts A and B of the European survey have both supported and gone against some of the hypotheses set out in Chapter 3. It has been shown that there is a clear link between a participant's demographics and both their general level of privacy concern and also their perceptions of all four privacy variables, to such an extent that Hypotheses 1 and 2 can be fully supported. To the contrary, the analysis of the results did not provide any evidence that supports a direct link between a participant's general level of privacy concern and their perception of the privacy cost variables. Hypothesis 3 has therefore been disproved to such an extent that for a couple of the privacy variables, the results suggest the opposite of what was expected could actually be true.

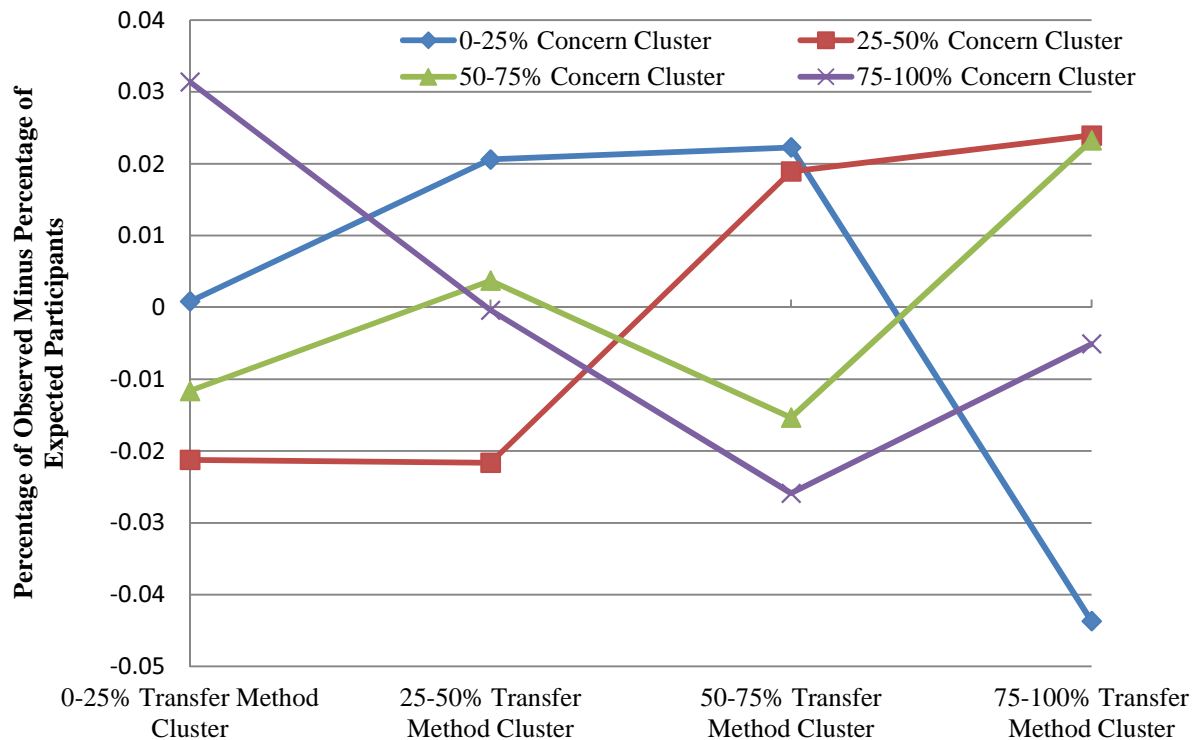
**Table 5-10 Demographic and Privacy Concern Breakdown of the Transfer Method Trust Quartiles**

Percentile	Age	Gender (Female)	Education	Wage (Under £/€20000)	Wage (Over £/€60000)	UK (Yes)	ND (Yes)	GR (Yes)	AT (Yes)	Minority (Yes)	Privacy Invasion (Yes)	Concern Cluster (75%)
	(Over 54)		(University Level)									
0-25% (N = 260)	35.1	51.4	47.8	49.8	9.7	25.8	16.2	27.3	30.8	3.5	36.9	28.8
25-50% (N = 245)	26.8	43.3	49.1	47.5	6.0	21.6	20.0	28.6	29.8	9.4	37.1	25.7
50-75% (N = 239)	26.7	43.7	54.0	40.1	8.6	25.5	23.4	24.7	26.4	5.4	30.4	23.0
75-100% (N = 242)	25.6	44.5	57.2	43.5	12.0	31.8	34.1	19.8	16.9	10.7	26.6	25.2

**Table 5-11 Chi Squared Test for Independence for the Influence of Demographics and Privacy Concern on the level of Transfer Method Trust**

Variable	p	Significant?
Age	<0.0001	Yes
Gender	0.050	Yes
Education	0.062	No
Income	0.019	Yes
Country	0.033	Yes
Minority	0.143	No
Experience	0.413	No
Privacy Index	<0.0001	Yes

**Figure 5-14 Percentage of Observed Participants Minus Percentage of Expected Participants in each Transfer Method Quartile Split by Their Privacy Concern Quartile**



Analysis of the demographic variables that impact a person's level of concern shows that a person's cultural background, their age and whether they are in the ethnic minority are the key primary influencers. It was also shown, however, that there are significant two-way interactions between the demographics which will need to be considered when moving forward with this research. A person's cultural background and age were also found to have a statistically significant relationship with the perception of all of the privacy variables.

From the analysis of the other demographic variables, several influences can be inferred. The elderly are less trusting of the various transfer methods, but they find their personal information less sensitive and place greater value on the reward on offer. Females are less trusting of the transfer methods and find their personal information more sensitive, but perceive greater value in the rewards and are more trusting of potential data holders. It has also been shown that the highly educated are more trusting of the transfer methods, hold less value in the reward offered and are less trusting of potential data holders.

The impact cultural background had on both a participant's general level of privacy concern and the perception of the privacy variables was very interesting. For both, the countries sampled appear to be split into two pairs of roughly similar views, the United Kingdom and the Netherlands versus Austria and Greece. The only cultural dimension that is similar in both pairs is their score in the individualism dimension, in which the United Kingdom and the Netherlands score highly and Austria and Greece score lowly (Hofstede 2001).

It should also be noted that according to a survey conducted by Privacy International (2007) the countries have the following scores associated to the level of privacy protection that exists in each country. The United Kingdom scored 1.4/5, the Netherlands 2.1/5, Austria 2.3/5 and Greece 3.1/5 where a score of 5 equates to their being no invasive policies and a score of 1 means that there is extensive surveillance in that country. This shows that the two countries with the highest level of invasive policies appear to have similar views as one another.

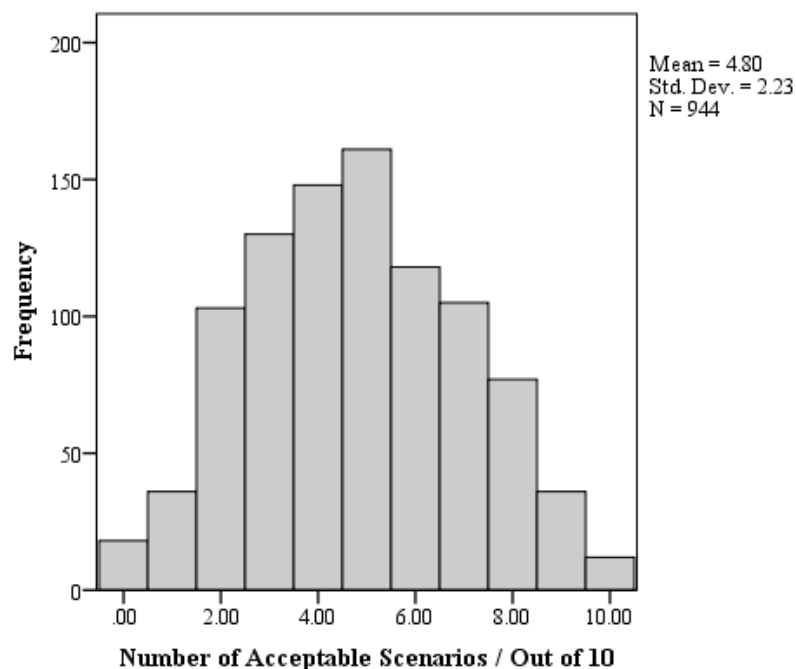
## 6. Behavioural Intention

### 6.1. Introduction

In an ideal world, a future ITS would not cause any privacy concerns, only use data that is not sensitive, only give this data to trusted data holders and only use trusted transfer methods. However, this is not the case for all of the ITS that are currently in use around the globe and is very unlikely to be the case for most future ITS as well. As the conclusion to the literature review in Chapter 2 pointed out, it is likely that a significant amount of future ITS users will still disclose their personal information even if they have privacy concerns, to take advantage of a reward that is on offer.

The research model created at the end of the literature review suggests that it is likely that a future ITS user's demographic make-up, their level of privacy concern and their perception of the privacy variables will all influence their privacy decision-making. As discussed in Chapter 4, Part C of the European survey asked the participants to state whether they would find ten different privacy scenarios acceptable or not. All of the scenarios comprised of privacy variables that the participants had already been asked for their perceptions of. Four of the scenarios were based around potential future ITS scenarios, three were general scenarios and three were test scenarios which are actually common place in everyday life already. Table 6-1 shows the individual privacy scenarios.

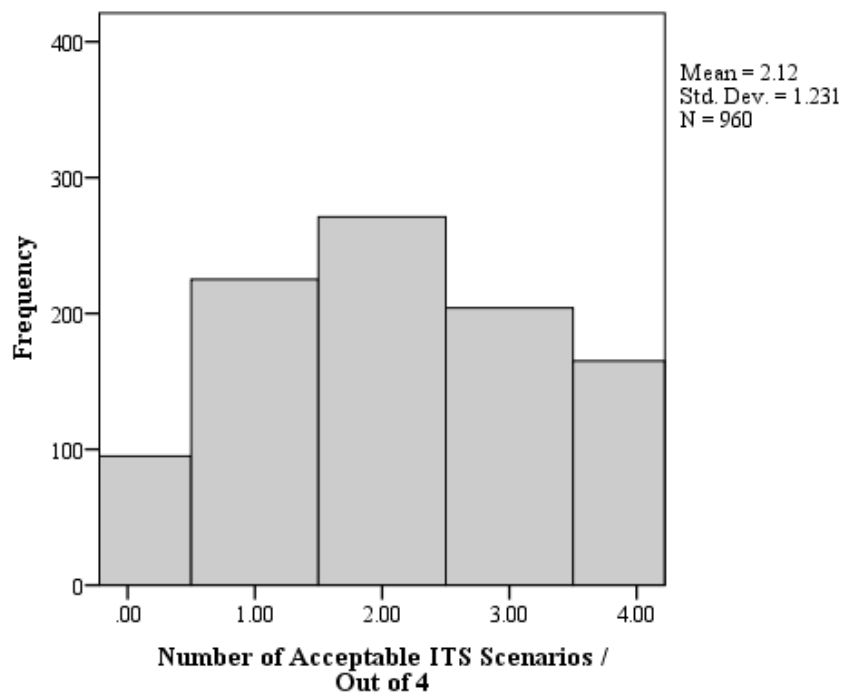
**Figure 6-1 Histogram of Number of Acceptable Scenarios**



**Table 6-1 Summary of Questionnaire Scenarios and the Variables they are Testing**

Type of Scenario	Question
ITS	During a car journey would you tell a company the road and weather conditions in your location via a wireless network if it would help to reduce your impact on the environment?
ITS	Would you tell the government by text message exactly where you plan to travel if it reduced your travel time?
ITS	During a car journey would you tell a stranger your location over a wireless network if it improved the safety of you and your family during the journey?
ITS	Would you let a private company know about your driving behaviour (speed at which you travel, how you travel etc) if it reduced your insurance premiums?
Gen	Would you tell a journalist in a private meeting your musical preferences in return for a rise in your social standing?
Gen	Would you tell a close friend your embarrassing secrets in a letter sent by postal mail if you thought it would bring you a lot of enjoyment?
Gen	Would you tell your medical conditions to a random doctor via a mobile phone if you thought it would improve your health?
Test	Would you give the details of everything that you purchase to a private company by email in return for a financial gain?
Test	Would you send your credit card details over an internet connection to a private company to book a room at a hotel in order to receive a discount online?
Test	Would you allow a security guard to search you and your luggage if it might improve your safety?

Figures 6-1 and 6-2 show histograms of the number of total acceptable scenarios and acceptable ITS scenarios respectively. The number of total acceptable scenarios is distributed normally around a mean of 4.8 acceptable scenarios and the number of acceptable ITS scenarios are distributed normally around a mean of 2.1 acceptable scenarios. Figure 6-3 shows the acceptability rate of the ten individual privacy scenarios. Scenarios B, F, G and I are the ITS scenarios, D, E and J are the general privacy scenarios and the three remaining scenarios are the test scenarios. It is interesting to note that none of the scenarios have a stated acceptability rate of greater than 70% or lower than 15%, this shows that none of the scenarios were either universally acceptable or rejected. This will hopefully enable the underlying factors influencing the variability in the acceptability rates to be discovered.

**Figure 6-2 Histogram of Number of Acceptable ITS Scenarios**

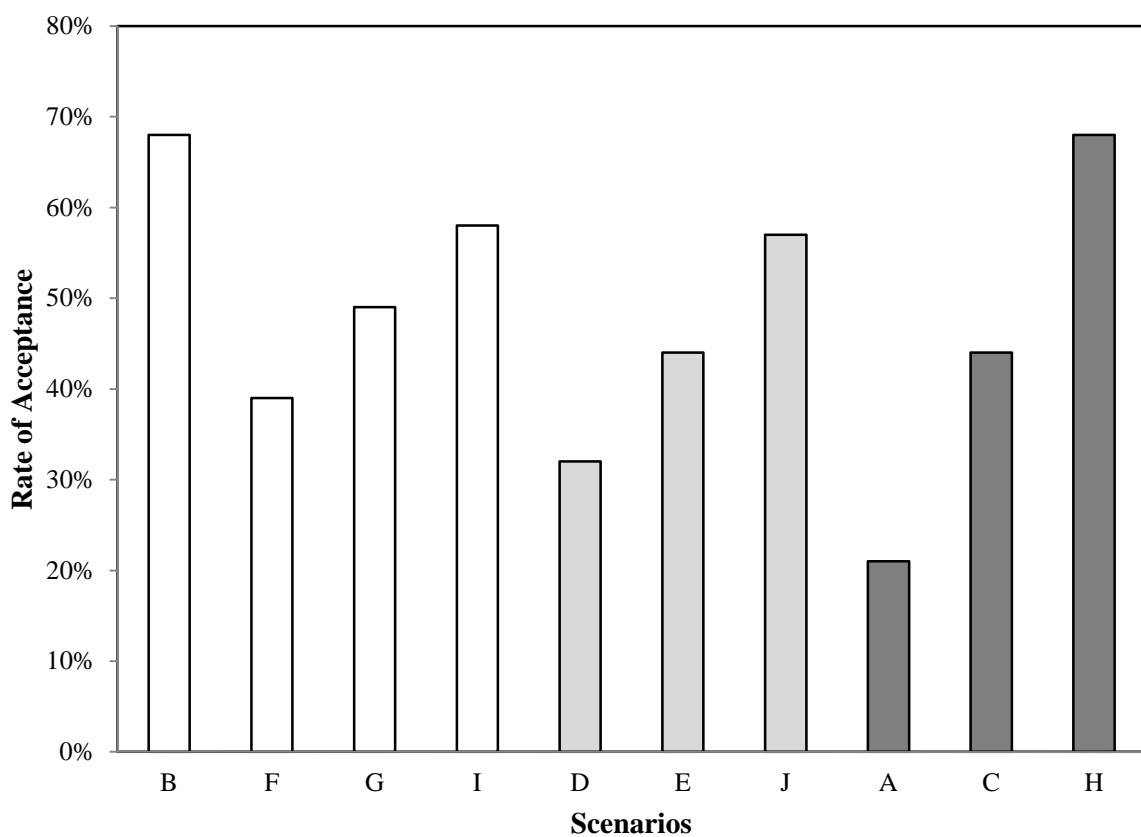
## 6.2. Participant Segmentation

Hierarchical cluster analysis has been used to further investigate the stated behavioural intention of the participants. Complete linkage clustering was used as the method of hierarchical cluster analysis with the intervals measured in Squared Euclidean Distance. This methodology was chosen as it helps produce compact clusters of approximately equal diameters (Everitt et al. 2001). Analysis of the rescaled distance cluster combine on the resultant dendrogram (Appendix K) showed that it is appropriate to split the participants into four well defined clusters.

Table 6-2 shows a breakdown of the number of acceptable scenarios for each cluster. It becomes clear from this table that Clusters 1 and 2 have much higher total acceptability rates than Clusters 3 and 4. It is also interesting to note that Cluster 2 finds the ITS scenarios more acceptable than Cluster 1 and likewise with Cluster 4 over Cluster 3.

From this analysis, Cluster 1 can be classified as being willing to trade their personal information, but they are not overly keen on ITS. Cluster 2 can be classified as being willing to trade their personal information and being keen on what the ITS have to offer. Cluster 3 can be classified as being unwilling to trade their information and not keen on the ITS scenarios. Cluster 4 can be classified as being unwilling to trade their information but more keen on the ITS scenarios than Cluster 3. As a consequence, going forward it will be important to compare the differences between Cluster 2 and Cluster 3 as they hold the participants that are most and least likely to find a future ITS scenario acceptable in privacy terms.

**Figure 6-3 Histogram of Number of Acceptable ITS Scenarios**



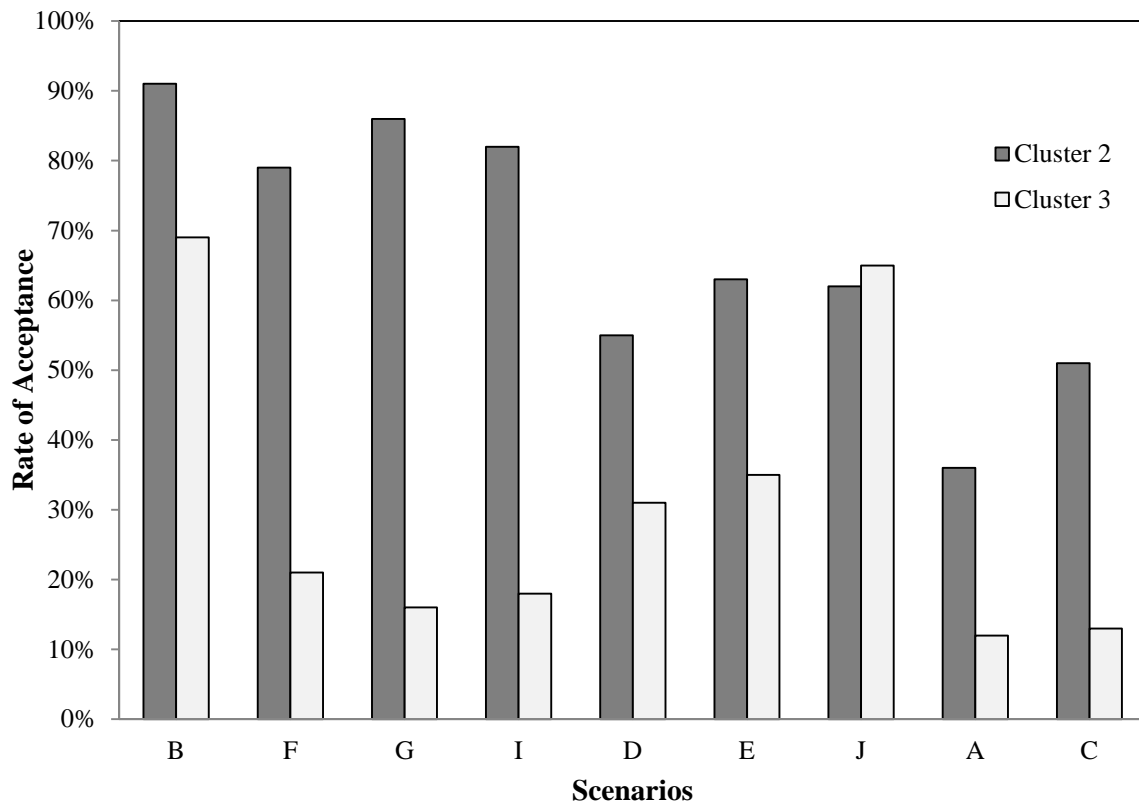
**Table 6-2 Breakdown of Acceptable Scenarios for Each Cluster**

Cluster	Mean Number of Acceptable Scenarios Out of 10	Mean Number of Acceptable ITS Scenarios Out of 4
1	5.4	2.1
2	6.9	3.3
3	3.3	1.2
4	3.5	1.7



Figure 6-4 shows a comparison of the acceptability rates of each privacy scenarios for Clusters 2 and 3. The first fact that becomes apparent from this figure is the high ITS (scenarios B, F, G, I) acceptability rates for Cluster 2, with all being above 75%, whereas, other than for scenario B, Cluster 3 has acceptability rates for the ITS Scenarios of less than 25%; a difference of more than 50% with Cluster 2.

**Figure 6-4 Comparison of the Two Extreme Clusters: Cluster 2 and Cluster 3**



### 6.3. Influence of Demographics on Behavioural Intention

The starting point to look at the influence of demographics on the participants' stated behavioural intention is to compare a demographic breakdown of Cluster 2 with Cluster 3. Table 6-3 does just that. There are several big differences between the make-up of these two clusters. The first is the cultural background of the two clusters, Cluster 3 (unwilling to trade with ITS) has significantly less participants in it from the United Kingdom than Cluster 2, but significantly more participants from the Netherlands. Although there is some difference in the number of participants from Austria and Greece, the differences are nowhere near as dramatic. Considering that the participants from the United Kingdom expressed similar views to the participants from the Netherlands for their stated level of concern and their perception of the privacy variables, this is surprising.

Table 6-3 Demographic and Breakdown of the Behavioural Intention Clusters

Percentile	Age (Over 54)	Gender (Female)	Education (University Level)	Wage (Under 20,000)	Wage (Over 60,000)	UK (Yes)	ND (Yes)	GR (Yes)	AT (Yes)	Minority (Yes)	Privacy Invasion (Yes)
Cluster 1 (N = 244)	26.0	47.5	57.5	46.4	8.0	31.6	24.2	23.0	21.3	8.2	35.7
Cluster 2 (N = 230)	26.7	43.6	55.8	46.4	10.0	31.7	10.0	27.4	30.9	8.3	26.8
Cluster 3 (N = 217)	29.0	47.6	45.5	45.6	5.7	15.7	30.4	29.0	24.9	4.1	34.4
Cluster 4 (N = 253)	33.5	44.9	49.2	43.4	9.2	27.3	26.9	20.6	25.3	7.5	33.7

There are also big differences in the number of educated people and high income earners in the two clusters, with highly educated, high earners proving to be significantly more likely to disclose their personal information to an ITS than low educated, non-high earners (the level of low earners is similar in both clusters). Table 6-2 also shows that there are more females and over 55s in Cluster 3, but again, the difference for these two variables is not as large as for some of the other demographic variables. So in summary, a comparison of the demographic make-up of Clusters 2 and 3 suggests that the most likely people to state they are willing to use future ITS are young, highly educated and high earning males from the UK. On the reverse side, the least likely people to state they would trade their personal information with a future ITS are elderly, low-educated Dutch females.

Many of these outcomes were predicted in the research model. In particular, it was predicted that people from the United Kingdom would be more willing to trade their personal information as they already live in a society where surveillance is prevalent and the citizens have a high level of individualism. The reluctance of the Dutch, however, is very interesting, as the Netherlands has a stereotype of being a very liberal and open community which would suggest that people are willing to share their personal information. This is a point reflected in the Dutch sample having a high level of trust in both the data holder and transfer method. During the data collection in the Netherlands, however, it became apparent that privacy is a big issue for people (even with regard to transport), especially when compared to the citizens in the UK and Greece, so it is not so much of a surprise that the results of the survey appear to reflect this observation.

What would not have been predicted, however, is that highly educated people and high earners would be the most willing to trade their personal information with a future ITS. It is the case that either the participants perceive the rewards on offer by these systems to be of more value than others or that they have had more experience of using existing ITS such as satellite navigation systems or automatic toll booths and therefore had less fear as a result. Both possible factors could be caused by the potential fact that some of the highly educated, high earning individuals would be more familiar than an average person with ITS due to the nature of their current job. This could be particularly true of the Greek sample because as discussed earlier (Section 4.5.3) the web-based questionnaire was initially sent to a distribution list that include some institutes that are research ITS.

To further validate these observations, Table 6-4 shows the results of a Chi Squared test of independence for the relationship between a participant's demographics and the number of ITS scenarios they state are acceptable. These tests validate the influence a participant's cultural and educational background has on the number of ITS scenarios that they state are acceptable. Figure 6-5 also confirms that participants from the United Kingdom are pro-ITS and those from the Netherlands are against it. The results of the European survey therefore provide support for Hypothesis 4 of the research model.

*H4: A user's stated behavioural intention with regard to the action they would take when faced with a privacy scenario will be impacted by their demographics such as their age, gender and cultural background. – SUPPORTED*

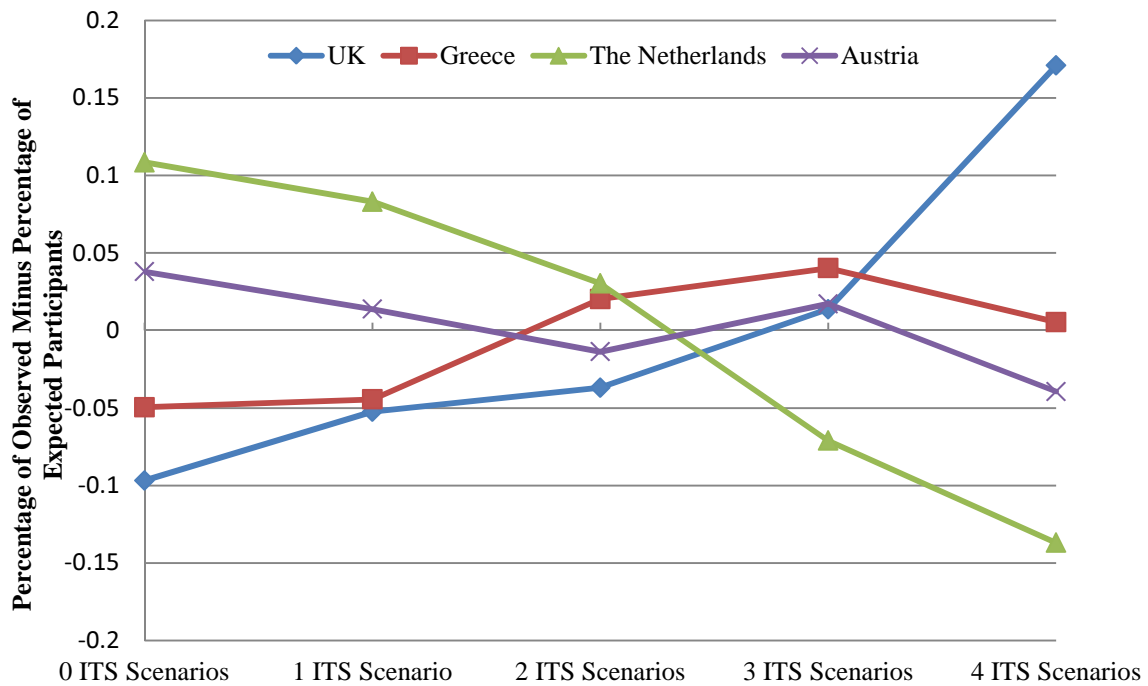
**Table 6-4 Chi Squared Test for Independence for the Influence of Demographics on the Number of Acceptable ITS Scenarios**

Variable	p	Significant?
Age	0.222	No
Gender	0.126	No
Education	0.012	Yes
Income	0.138	No
Country	0.000	Yes
Minority	0.567	No
Experience	0.023	Yes

#### 6.4. Influence of Concern on Behavioural Intention

By comparing the number of participants who are in the highest concern quartile and the behavioural intention Clusters 2 and 3 (see Table 6-5) no obvious trend is apparent, as both clusters are within 0.5% of each other, so in order to further investigate the relationship between a future ITS user's level of concern and their likely stated behavioural intention, a Chi Squared test of independence has again been used. Table 6-6 shows that the result of the Chi Squared test indicate that there is no statistically significant relationship between the participants' level of concern and their stated behavioural intention when they are faced with an ITS scenario.

**Figure 6-5 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Stated Acceptable ITS Scenarios by Their Country**



**Table 6-5 Concern Level and Privacy Variable Perception Breakdown of the Behavioural Intention**

Percentile	Most Concerned Quartile (%)	Highest Reward Quartile (%)	Most Sensitive Quartile (%)	Most Trusting Holder Quartile (%)	Most Trusting Transfer Quartile (%)
Cluster 1 (N = 244)	28.3	23.4	21.7	25.4	23.4
Cluster 2 (N = 230)	24.8	21.3	17.8	26.5	28.7
Cluster 3 (N = 217)	25.3	20.7	30.0	18.4	25.3
Cluster 4 (N = 253)	26.1	30.4	25.3	24.9	21.3

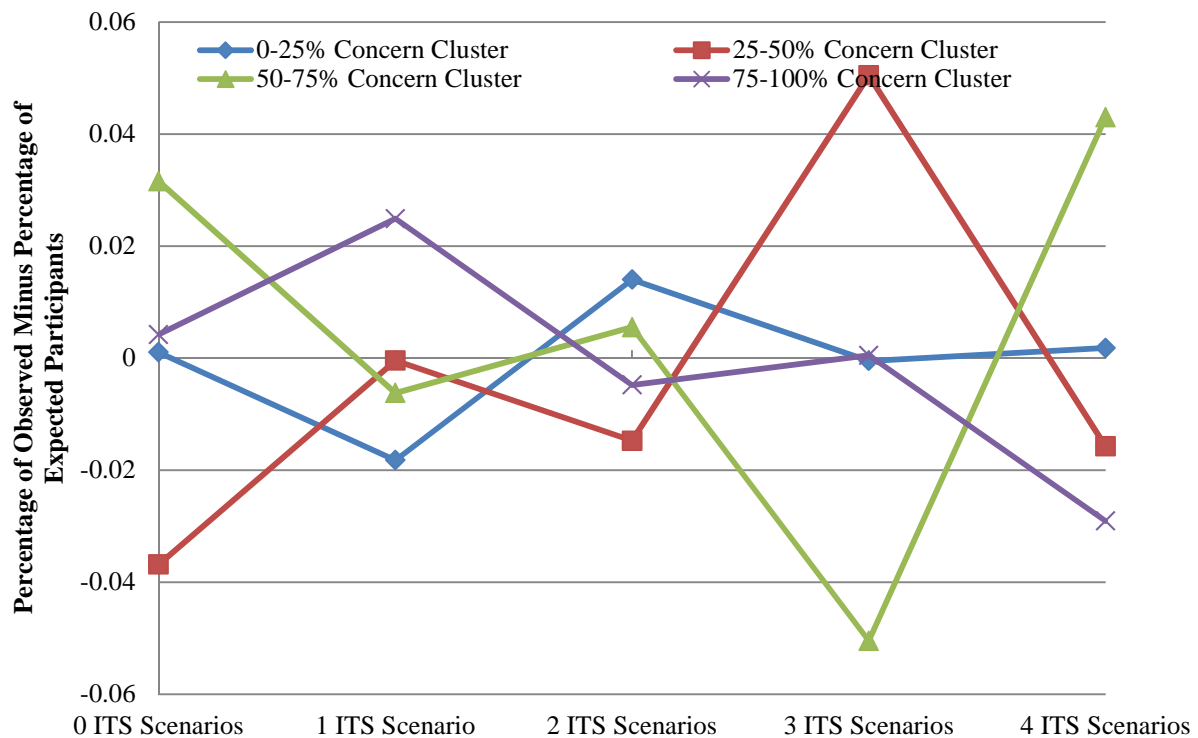
**Table 6-6 Chi Squared Test for Independence for the Influence of Level of Concern and Perception of Privacy Variables on the Number of Acceptable ITS Scenarios**

Variables	p	Significant?
Concern	.748	No
Reward	.310	No
Sensitivity	.000	Yes
Holder	.013	Yes
Transfer	.011	Yes

This lack of relationship is further supported by Figure 6-6, which shows that the number of acceptable scenarios for each concern cluster is very randomly distributed. As a consequence, the results of the European survey presents evidence which does not support Hypothesis 5 in the research model.

*H5: A user's stated behavioural intention with regard to the action they would take when faced with a privacy scenario will be impacted by their general level of privacy concern. – NOT SUPPORTED*

**Figure 6-6 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Stated Acceptable ITS Scenarios by Their Level of Concern**



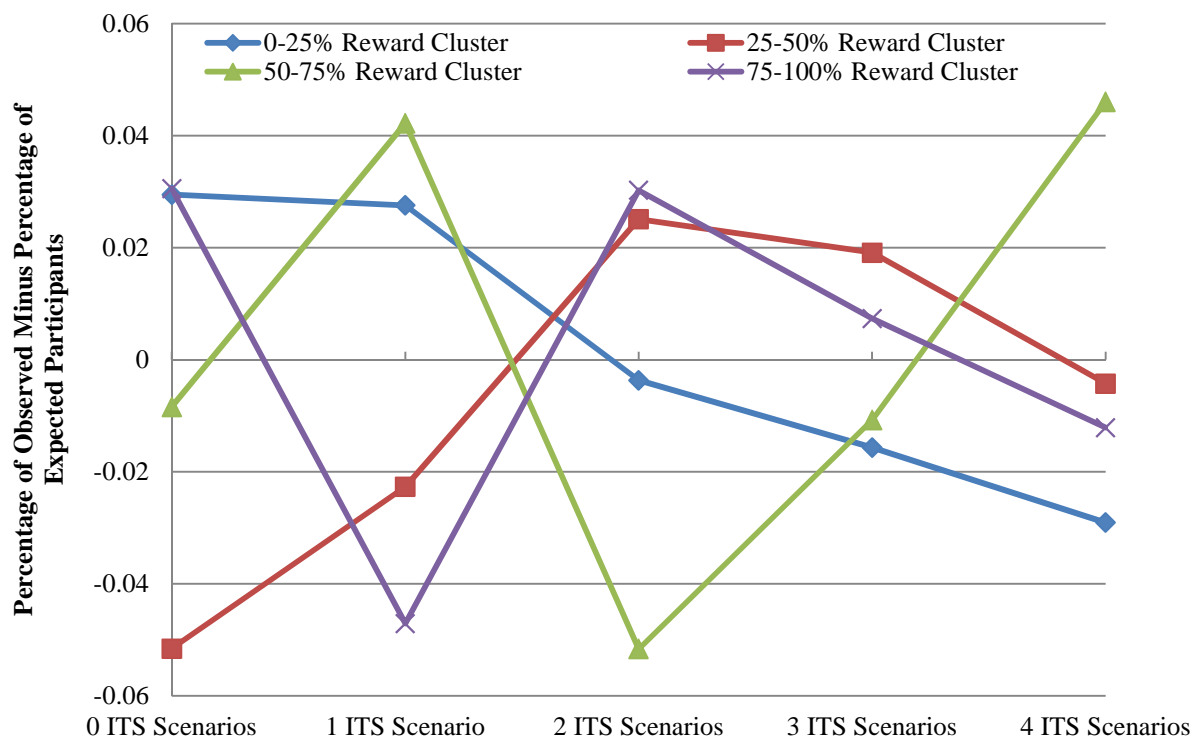
## 6.5. Influence of Privacy Variables on Behavioural Intention

Hypotheses 6a-d all advocate that a future ITS user's perception of the privacy variables will influence their stated behavioural intention. This section will investigate the impact of each individual variable, and the next section (6.5), will investigate the impact of all four privacy variables combined.

### 6.5.1. Rewards

It is expected that a participant who perceives the reward offered in a privacy scenario to hold a high value will be more likely to state that they would be willing to disclose their personal information than a participant who places a low value on the same reward. Table 6-5, however does not support this theory, because Cluster 4 contains the largest percentage of participants who also feature in the highest perceived reward cluster. It was shown earlier that Cluster 4 was in fact the cluster which contained some of the most privacy protecting participants, which is completely contradictory to the stated hypothesis. The results of the Chi Squared test in Table 6-6 and Figure 6-7 also both show that the results of the European survey indicate that there is no statistically significant relationship between the two variables.

**Figure 6-7 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Stated Acceptable ITS Scenarios by Reward Cluster**



It should be noted at this point that, unfortunately, none of the scenarios in Part C of the European survey offered no reward in return for the participant disclosing their information. The problem with this is that it is therefore not clear whether participants are as likely to disclose their personal information if no reward at all is offered, as if they were offered £1 million in return, which is what these results indicate, but seems very unlikely in the real world. Instead, it is likely that behavioural factors such as prospect theory (Kahnemann and Tversky 1979) result in the value of the reward being not being as important as the fact that one is being offered. In addition to the non-zero reward, the low Cronbach alpha score for the perceptions of the rewards suggest that using a mean of all of the perceptions of the rewards types in the different scenarios — as this research has done — is not ideal. Given these two factors, not enough evidence has been presented to either support or disprove Hypothesis 6a.

*H6a: The perceived value of the reward on offer will have a positive impact on a user's behavioural intention.* – UNCLEAR

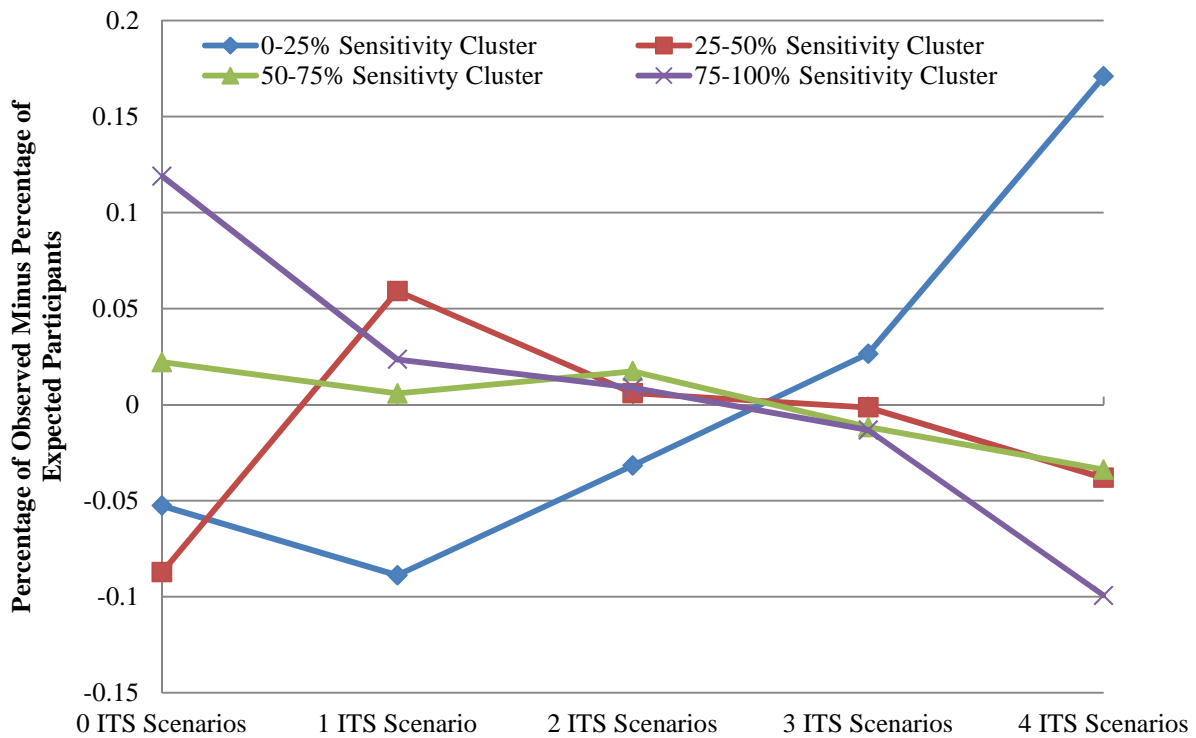
#### *6.5.2. Data Sensitivity*

It was anticipated after the review of existing literature that if a participant perceived the type of personal information required by the privacy scenario to be sensitive, they would be less likely to state that they would be willing to disclose it. Table 6-5 shows that this is indeed the case; Cluster 2 (most willing to disclose) only contained 17.8% of the participants who had a high sensitivity and Cluster 3 (least willing to disclose) contained 30.0%. The results of the Chi Squared test (Table 6-6) also report that the relationship between data sensitivity and behavioural intention is highly significant. Figure 6-8 clearly shows that as a future ITS user's perception of how sensitive the data required increases, the acceptability rate of the privacy rate decreases. These results substantially support Hypothesis 6b.

*H6b: The level of sensitivity associated with a data type will negatively impact a user's behavioural intention.* – SUPPORTED



**Figure 6-8 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Stated Acceptable ITS Scenarios by Data Sensitivity Cluster**



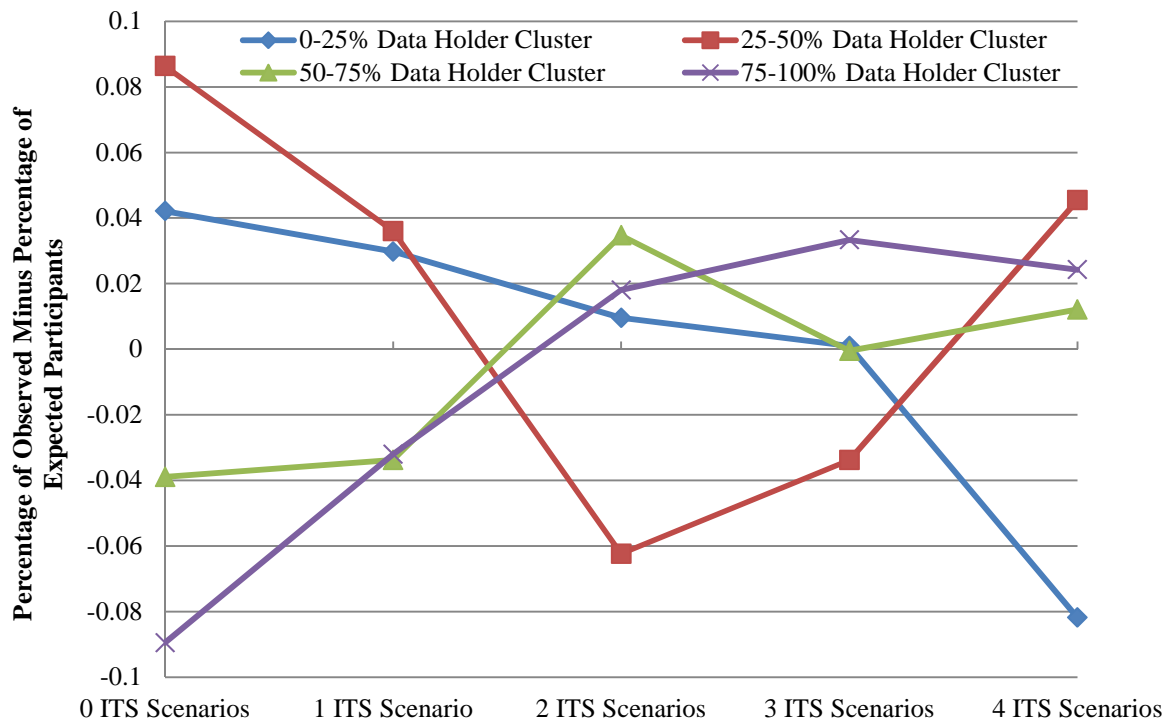
### 6.5.3. Data Holder

The third privacy variable that the European survey tested was the participants' perceptions of how safe their personal information would be in the hands of various different data holders. The research model states that as the level of perceived security increased so would the acceptability of the privacy scenario. Table 6-5 supports this theory because it shows that Cluster 2 (most willing to disclose) contained 26.5% of participants that were in the top percentile with regards to how secure they felt their information was with various data holders, whereas Cluster 3 (least willing to disclose) only contained 18.4%.

Again, to investigate this further a Chi Squared test was used (Table 6-6) to show that there was a statistically significant relationship between the perceived data holder security and the stated willingness to disclose personal information to an ITS. Figure 6-9 then confirms the direction of the relationship to be as expected; as the perception of security increases, so does the rate of acceptability. The results of the European survey therefore support Hypothesis 6c.

*H6c: The level of trust a user has in the new data holder will have a positive impact on the user's behavioural intention. – SUPPORTED*

**Figure 6-9 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Stated Acceptable ITS Scenarios by Level of Trust in Data Holder**



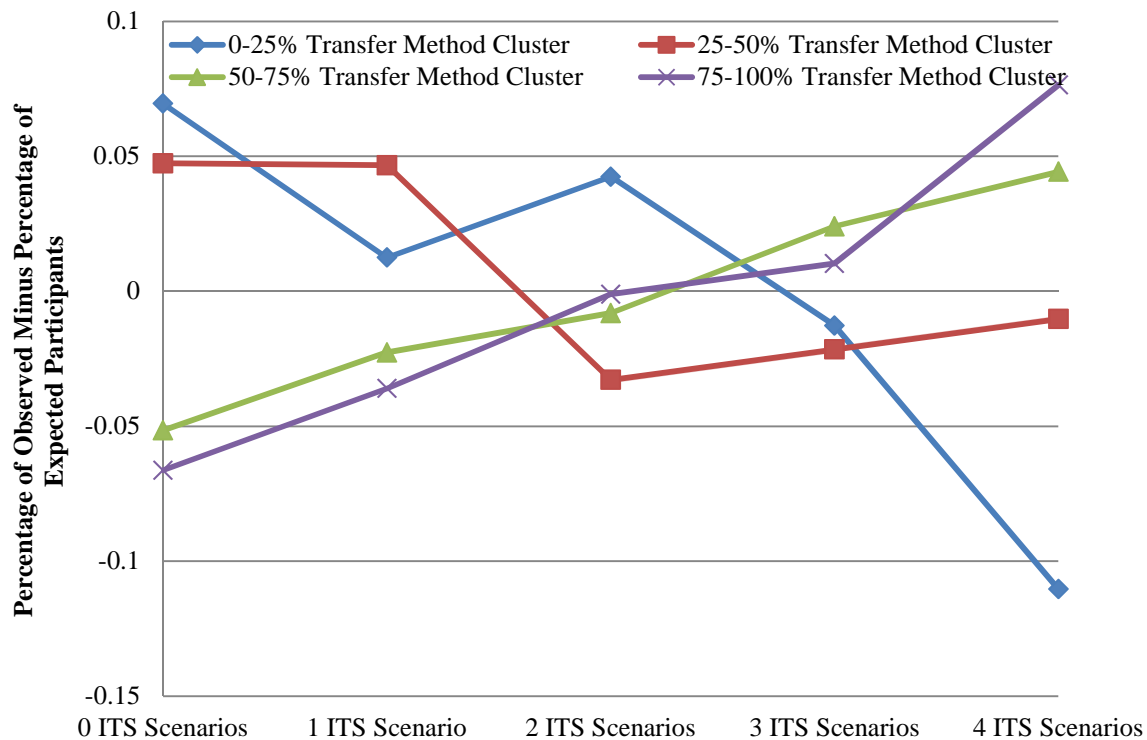
#### 6.5.4. Transfer Method

The final privacy variable is the perception of the method by which the personal information will be transferred from the existing to new data holder. As with the perception of the data holder security, it is expected that the more secure a future ITS user feels the transfer method is, the more likely they will be to disclose their personal information.

Table 6-4 alone does not support this theory, however, because it does not show a significant difference between that amount of participants in Clusters 2 and 3 who were also in the top transfer method security quartile. The result of the Chi Squared test (Table 6-6) does, however, indicate that the two variables are significantly related. Figure 6-10 further supports the theory as it suggests that participants who believed the transfer methods to be secure were more likely to find the ITS privacy scenarios more acceptable and vice versa. This provides enough evidence to support the research model's Hypothesis 6d.

*H6d: The level of trust a user has in the data transfer method will have a positive impact on the user's behavioural intention. – SUPPORTED*

**Figure 6-10 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Stated Acceptable ITS Scenarios by Level of Trust in Transfer Method**



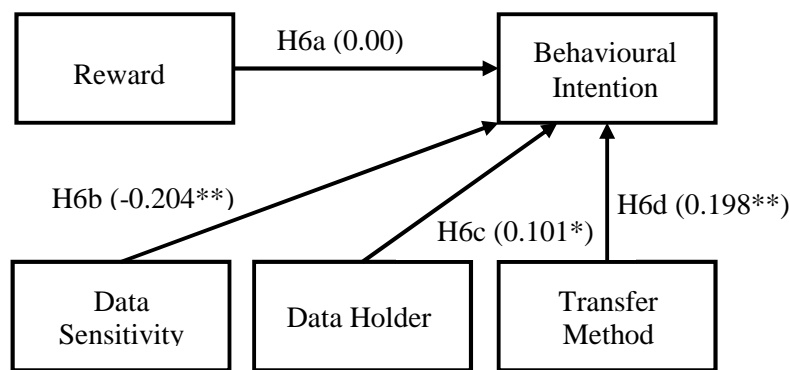
## 6.6. Predicting Behavioural Intention

So far this chapter has not considered how a future ITS user's level of privacy concern, demographics or perceptions of the privacy variables might interact with one another and influence their stated behavioural intention when presented with a privacy scenario. Chapter 5 showed that two-way interactions had a significant impact on the ability to predict a future users level of privacy concern. It is therefore likely that considering them will also help improve the ability to accurately predicted a future ITS user's stated behavioural intention.

Figure 6-11 shows the Pearson's  $r$  correlation coefficients (Johnson and Wichern 1992) between each of the privacy variables and behavioural intention. It shows that the cost variables were all significant and had the directional influences predicted in the research model. It also shows that no correlation was found between the perception of the reward on offer and the participant's behavioural intention.

Enter method, multiple linear regression (Efroymson 1960) was used to measure the one-way interactions between the four variables privacy variables and the demographic variables and the resultant model had an  $R^2$  value of 0.149. This suggests that a combination of the one-way interaction between these variable accounts for approximately 15% of the variance in the participants stated privacy behaviour. Table 6-7 shows that all of the privacy cost variables play a significant role, as does the participants nationality, education level, gender and level of general privacy concern. Nationality (being Dutch) and data sensitivity were shown to be the biggest predictors of stated privacy behaviour.

**Figure 6-11 Correlations between Privacy Variables and Behavioural Intention**



**Table 6-7 Variables in Multiple Liner Regression Model of Acceptable Number of ITS Scenarios**

Variable	Standardized Beta	t	Sig.
Constant		8.249	.000
Privacy Invasion	-.033	-.958	.338
Income Level	.013	.378	.706
Education Level	.084	2.490	.013
Gender	-.069	-2.072	.039
Reward	.043	1.161	.246
Data Sensitivity	-.186	-5.188	.000
Data Holder	.141	3.573	.000
Transfer Method	.088	2.346	.019
Privacy Concern	-.083	-2.424	.016
Greece	-.018	-.422	.673
Netherlands	-.275	-6.861	.000
Austria	-.082	-1.935	.053

As it is not practical to look at every two-way interaction and the potential impact it could have on stated behaviour, backwards stepwise logistic regression has been used to model the combined effect of using all the variables discussed so far in this chapter and their two-way interactions to predict if a participant would find three or more ITS scenarios acceptable or not. Unfortunately, it was not possible to include two-way interaction involving income level as there was too many missing values (to be discussed in the next chapter).

By simply predicting that every participant would find three or more of the ITS scenarios acceptable, you would be correct 57.3% of the time. By using the binary logistic regression model shown in Table 6-8, which has a Cox & Snell  $R^2$  value of 0.248 and a Nagelkerke  $R^2$  value of 0.333, you would be correct 71.2% of the time. Although the  $R^2$  values suggest that roughly 70% of the variance in a future ITS user's privacy decision-making is still unaccounted for, if the model was used to predict the stated privacy intention of every citizen within Europe, an improvement in accuracy of 13.9% will be very significant (circa 91 million extra correct predictions).

Table 6-8 also shows how important it was to consider the two-way interactions between the variables. Only the participants' perceptions of data sensitivity and transfer method security were significant enough on their own to be included within the model. It should also be noted that although the hypotheses relating to both a participant's level of concern and perception of the reward have proved unsupported both when combined with another variable (including one another), they are significant predictors of stated privacy intention. This also means that all of the variables explored in this chapter, demographics, level of privacy concern and perception of the privacy variable can be used to improve predictions of a future ITS user's stated behavioural intention, although a lot of the variance in the participants decision-making is still unaccounted for. This suggests that the participants are acting with at least some elements of rationality. The improvement in the ability to correctly predict a future ITS user's stated privacy intention because of the interaction between the stated variables is high enough to support Hypothesis H7 within the research model.

*H7: A user's stated behavioural intention will primarily be derived from their demographics, general level of primary concern and a trade-off between their perceptions of the reward on offer against the risk associated with a scenario. – SUPPORTED*

**Table 6-8 Variables in Binary Logistic Model of Acceptable ITS Scenarios**

<b>Variable</b>	<b>Wald</b>	<b>df</b>	<b>Sig.</b>
Data Sensitivity	26.694	3	.000
Transfer Method Security	18.528	3	.000
Country * Privacy Concern	15.688	9	.074
Country * Data Holder Security	16.620	9	.055
Education * Reward Value	22.553	12	.032
Education * Data Holder Security	24.982	12	.015
Privacy Concern * Reward Value	15.647	9	.075
Privacy Concern * Data Sensitivity	15.828	9	.071
Privacy Concern * Transfer Method Security	29.006	9	.001
Country * Education	27.854	12	.006
Country * Gender	8.556	3	.036

### 6.7. Summary

The analysis of Part C of the European survey has shown support for some of the hypotheses set out in Chapter 3, but not others. The cluster analysis conducted at the beginning of this chapter clearly added weight to the fact that a person's stated privacy behaviour is linked to their demographic background. Cluster 2, which is comprised of those users that were most willing to disclose their personal information to the hypothetical ITS, had a high proportion of young, British, highly educated, high income males and those who have not experienced a previous privacy invasion.

Conversely, Cluster 3 which is comprised of those participants that stated they were the least willing to disclose their personal information, had a high proportion of elderly, Dutch, low educated, low/middle income females who have experienced a previous privacy invasion. The demographic makeup of these two extreme clusters supports the findings of the vast majority of the previous research into the impact of demographics on people's privacy decision-making highlighted in Chapter 3. The only variable that was not supported was that this research found that participants with a high level of education and/or high income level were more willing to disclose their personal information. This is the opposite to what would be expected from the majority of the historic research.

This could be potentially caused by the fact that some of the highly educated high earners sampled would have had a higher than average (than the wider population) exposure to the ITS field. Other than the impact of education/income level all of the other demographic research that was conducted predominately in the field of ecommerce appears to hold true for the transportation field. As a consequence this research has supported Hypothesis 4.

With regards to Hypothesis 5, which stated that the level of a future ITS user's privacy concern will be linked to their stated privacy intention, the results of the European survey were not able to support this. Instead, this chapter has shown that the link between the participants' level of privacy concern and their stated behavioural intention with regards to the ITS scenarios was random and no correlations existed.

This chapter then moved on to explore the link between the participants' perceptions of the four privacy variables and their stated behavioural intention. The results showed that a participant's perception of the three of the cost variables (data sensitivity, the data holder and the transfer method) were significantly correlated with their intention. The participants who regarded their personal information as more sensitive, had less trust in the data holders and less trust in the transfer method were less likely to find the ITS scenarios acceptable. Surprisingly, the results of the European survey found no correlation between the participants' perceptions of the reward on offer and their stated intention. This was contrary to the expectation that they would weigh off their perception of the reward on offer against their perception of the cost variables in a form of cost benefit analysis. Whilst unexpected, this outcome could be explained by some theories from the field of behavioural economics such as prospect theory (Kahneman and Tversky 1979) and suggest that the participants' decision-making was influenced by some irrationality.

The final hypothesis that this chapter tested (Hypothesis 7) was whether a future ITS user's stated behavioural intention would primarily be driven by a combination of their demographics, general level of privacy concern and their perception of the four privacy variables. Using these variables and their two-way interactions in a logistic regression model, it was possible to significantly improve the accuracy of predicting future ITS user's stated behavioural intention. The model, however, did not account for 70% of the variance which suggests that whilst the variables used all had an influence on a user's stated behavioural intention, other elements such as irrational behaviour were unaccounted for.





## **7. Actual Behaviour**

### **7.1. Introduction**

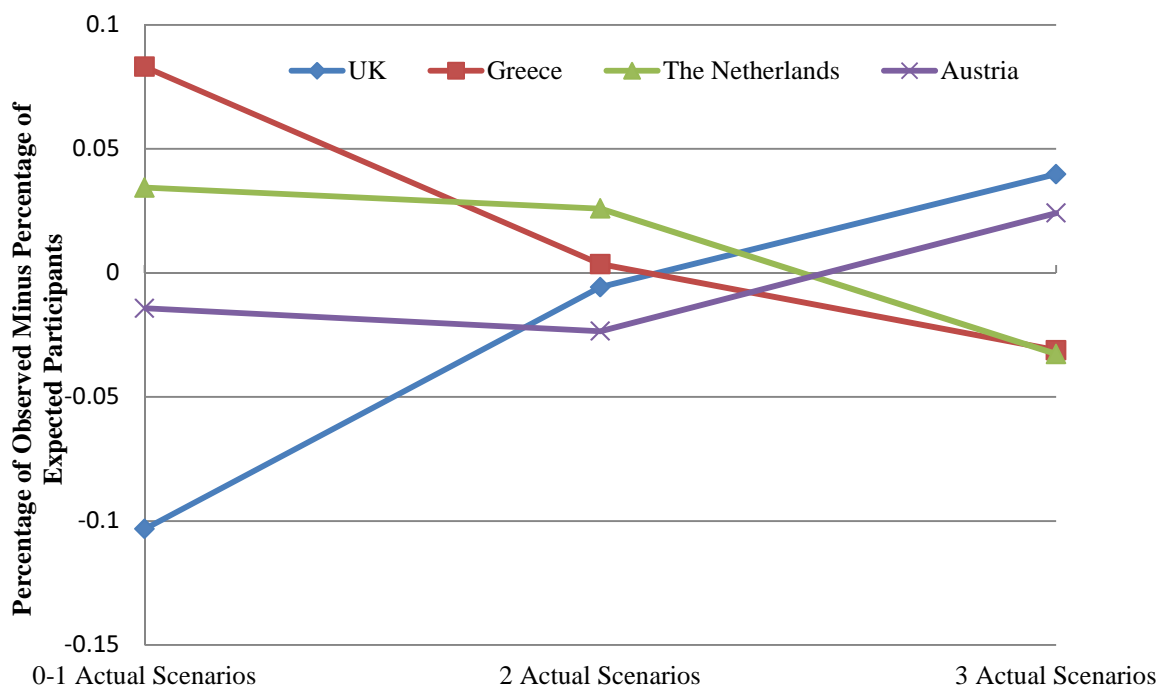
The previous two chapters have looked at the future ITS user's likely level of privacy concerns, perceptions of the privacy variables and their stated behavioural intention. While some developers would find it desirable for a future ITS to cause no privacy concerns, the main aim of this research is to investigate the point at which people will actually act in a privacy preserving manner. Therefore, this chapter will explore future ITS user's actual privacy behaviour and explore what factors play a significant role in shaping this behaviour.

As discussed in the methodology chapter, the best method of exploring future ITS user's actual behaviour would be to actually observe their real behaviour when confronted with a real ITS privacy scenario. Unfortunately, many of the ITS that are likely to be contentious have not yet been fully developed and existing ITS are likely to create less privacy concerns than some of the future technologies. This chapter will therefore explore the participants' actual behaviour for a range of different non-transport related scenarios. The links between this actual behaviour and the participants' demographics, perception of the privacy variables, general level of privacy concern and their stated behavioural intention will be explored. This will then allow the results of this chapter to be combined with the previous two so that predictions about the likely uptake of future ITS can be made by knowing a future user's stated behavioural intention, their demographics, their general level of privacy concern and their perception of the privacy variables.

To facilitate this, Part D of the European questionnaire asked the participants how they acted in everyday privacy scenarios. Prior to this, Part B of the questionnaire asked the participants their stated behaviour in three similar hypothetical scenarios. Table 7-1 shows the actual and test scenarios found in Parts D and B of the European questionnaire respectively (see Appendix B). Whilst the actual and test scenarios are not identical, the pairs of scenarios had very similar privacy variables; they offered similar rewards, required similar information types, gave this information to similar data holders and used similar transfer methods. The reasoning behind this was that if future ITS users' stated behaviour intention and perception of the privacy variables for similar but not identical ITS scenarios is to be used predict whether future ITS are to be acceptable. Then it should be the case that the outcomes of existing real life privacy scenarios should be able to be predicted from the stated behaviour and perceptions of the privacy behaviour for similar but not identical scenarios. This chapter will also investigate the other factors that could impact the participants' willingness to give away their personal information in the actual scenarios.

**Table 7-1 Actual and Test Scenarios**

Scenario Type	Question
Actual Scenario 1	Do you use store loyalty cards (Nectar Card, Tesco Clun Card, Air Miles Card etc.)
Test Scenario 1	Would you give the details of everything that you purchase to a private company by email in return for a financial gain?
Actual Scenario 2	Have you ever purchased anything with a credit card on the internet?
Test Scenario 2	Would you send your credit card details over an internet connection to a private company to book a room at a hotel in order to receive a discount?
Actual Scenario 3	Have you ever been through / Would you be willing to go through airport security?
Test Scenario 3	Would you allow a security guard to search you and your luggage if it might improve your safety?

**Figure 7-1 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Actual Acceptable Scenarios by Their Country**

**Table 7-2 Demographic Breakdown of the Actual Behaviour Clusters**

<b>Percentile</b>	<b>Age (Over 55)</b>	<b>Gender (Female)</b>	<b>Education (University Level)</b>	<b>Wage (Under £/€20,000)</b>	<b>Wage (Over £/€60,000)</b>	<b>UK (Yes)</b>	<b>ND (Yes)</b>	<b>GR (Yes)</b>	<b>AT (Yes)</b>	<b>Minority (Yes)</b>	<b>Privacy Invasion (Yes)</b>
0-1 Acceptable Scenarios (N = 154)	38.2	45.8	45.3	56.7	3.2	16.2	25.9	33.2	24.7	6.5	32.2
2 Acceptable Scenarios (N = 366)	27.5	48.5	46.8	51.0	10.4	26.0	25.1	25.1	23.8	6.0	31.6
3 Acceptable Scenarios (N = 452)	27.6	43.4	58.0	37.3	10.4	30.5	19.2	21.7	28.5	7.5	35.2

**Table 7-3 Chi Squared Test for Independence for the Influence of Demographics on the Number of Actual Acceptable Scenarios**

<b>Variables</b>	<b>p</b>	<b>Significant?</b>
Age	0.004	Yes
Gender	0.386	No
Education	<0.0001	Yes
Income	0.001	Yes
Country	0.005	Yes
Minority	0.860	No
Experience	0.680	No

## 7.2. Influence of Demographics on Actual Behaviour

Table 7-2 starts looking at the influence of demographics on the participants' actual behaviour by comparing the demographic breakdown of participants who found 0-1, 2 and 3 of the actual behaviour scenarios acceptable. There are large differences between the consistencies of the three groups. The first is the cultural background of the groups. Figure 7-1 demonstrates that the British and Austrians were shown to be more willing to disclose their person information in the real life scenarios, while the Dutch and Greeks were less willing. This is an interesting result because the impact culture has on actual behaviour is slightly different from the impact it had on the stated behavioural intention, where the Austrians in particular were shown to less willing to disclose their personal information.

There are also big differences in the number of educated people and high income earners in the three groups, with highly educated, high earners proving to be significantly more likely to disclose their personal information in this regards. The result are similar to the impact of income/education level on stated privacy intention. Table 7-2 also shows that over 55s were less willing to disclose their personal information than the under 55s. So in summary, a highly educated, high earning young British person is the most likely to disclose their personal information and a low educated, low earning elderly Greek person the least likely.

Interestingly, the participants' gender, ethnicity and whether they had experienced any previous invasions appear to play no role in influencing their actual privacy behaviour. These observations are further validated by the results of a Chi Squared test of independence for the relationship between a participant's demographics and the number of scenarios the participants actually found acceptable. Table 7-3 shows these results. These results show that the relationships between the participants' age, country, education and income level were all statistically significant. It is therefore fair to say that a future ITS user's actual behaviour will be impacted by their demographics.

*H8: A user's actual behaviour will be impacted by their demographics such as their age, gender and cultural background. – SUPPORTED*

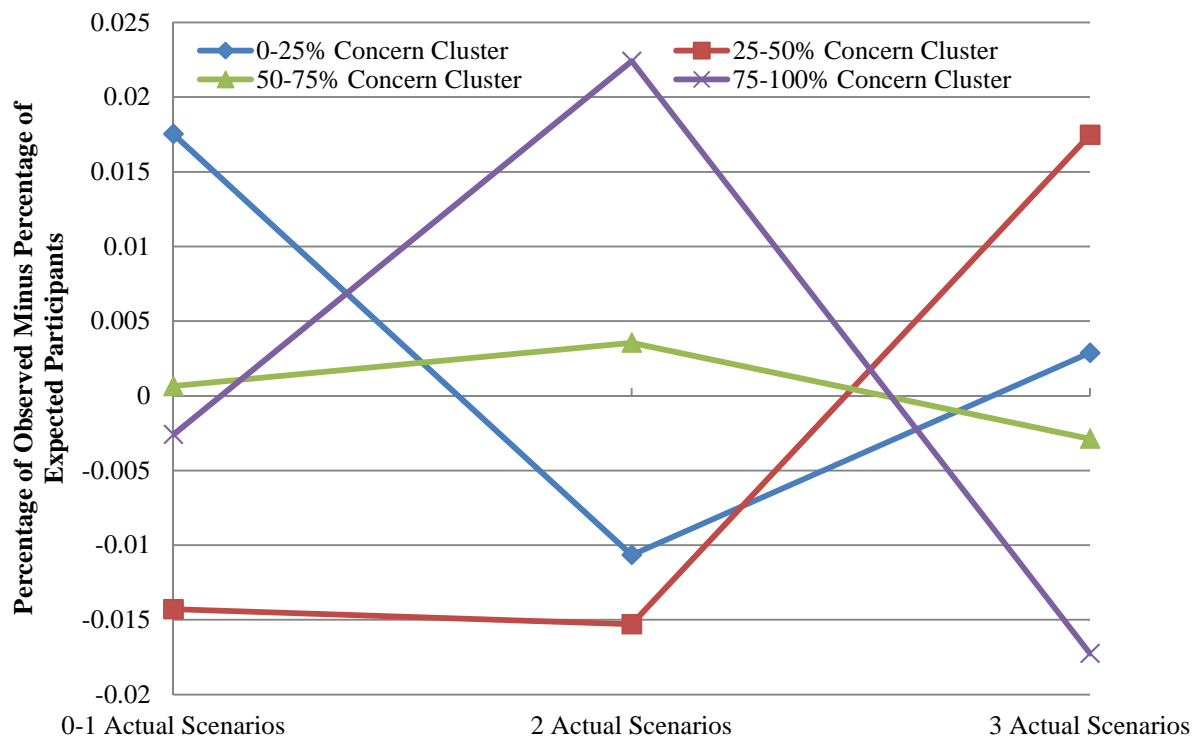
### 7.3. Influence of Concern on Actual Behaviour

Figure 7-2 shows how the percentage of observed minus the percentage of expected participants for each concern cluster varies with the acceptable number of actual scenarios. This figure shows that although there are more observed participants who found all three actual scenarios acceptable in the 0-25% and 25-50% than the 50-75% and 75-100% clusters, there are no consistent trends across the other actual scenario groups.

This lack of relationship is further confirmed by the results of a Chi Squared test of independence, which can be seen in Table 7-4. The results of the test show that there is no statistically significant link between the participants' level of privacy concern and their actual behaviour. As a consequence, the results of the European survey present evidence which disproves Hypothesis 9 in the research model.

*H9: A user's actual behaviour will be impacted by their general level of privacy concern. - NOT SUPPORTED*

**Figure 7-2 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Actual Acceptable Scenarios by Their Level of Privacy Concern**



**Table 7-4 Chi Squared Test for Independence for the Influence of Demographics on the Number of Actual Acceptable Scenarios**

<b>Variables</b>	<b>p</b>	<b>Significant?</b>
Privacy Index	.790	No
Reward	.182	No
Sensitivity	.784	No
Holder	.390	No
Transfer	.000	Yes

#### 7.4. Influence of Privacy Variables on Actual Behaviour

Hypotheses 10a-d all advocate that a future ITS user's perception of the privacy variables will influence their actual privacy behaviour. This section will investigate the impact of each individual variable.

##### *7.4.1. Rewards*

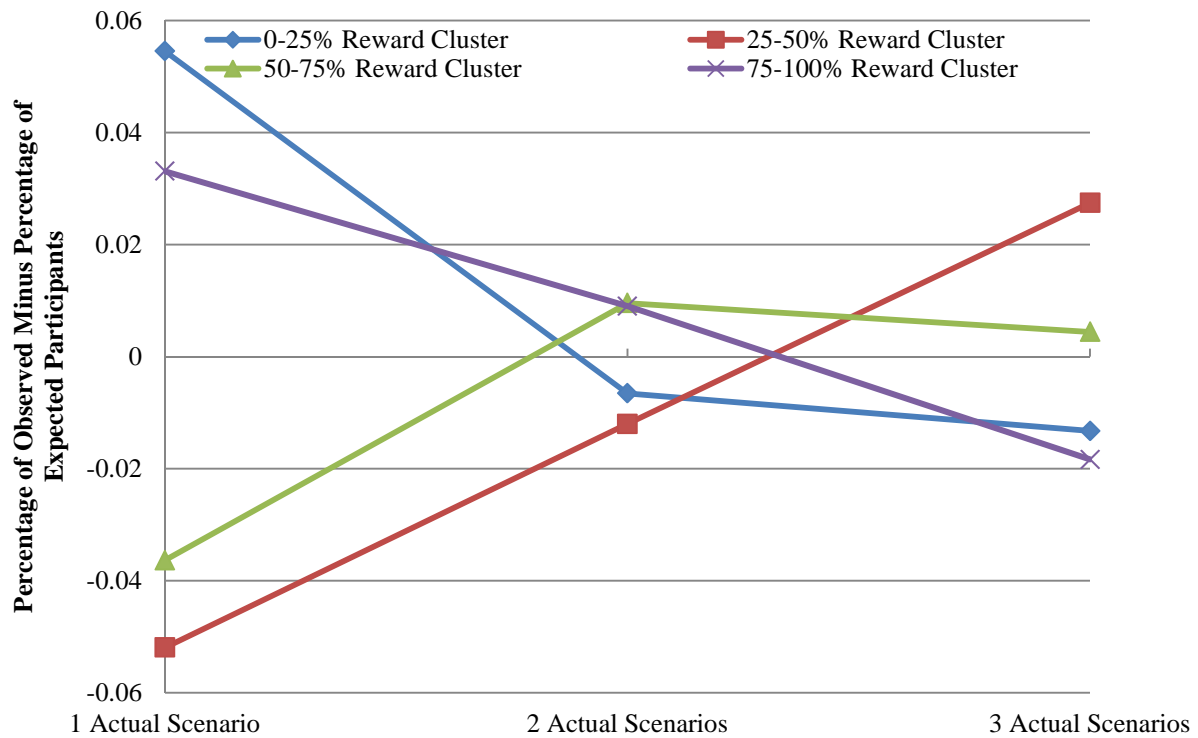
It was expected that a participant who perceived the reward offered in a privacy scenario to hold a high value will be more likely to be willing to disclose their personal information. Table 7-4, however does not support this theory because the results of the Chi Squared test show that the results of the European survey indicate that there is no statistically significant relationship between the two variables. Figure 7-3 further disproves Hypothesis 10a, as it shows that that the relationship between the perception of the reward on offer and actual behaviour is fairly random.

*H10a: The perceived value of the reward on offer will have a positive impact on a user's behavioural intention. – NOT SUPPORTED*

##### *7.4.2. Data Sensitivity*

It was anticipated after the review of existing literature that if a participant perceived the type of personal information required by the privacy scenario to be sensitive, then they would be less likely to state that they would be willing to disclose it. Table 7-4 shows that this is not actually the case, as the results of the Chi Squared test report that the relationship between data sensitivity and actual behavioural is not statistically significant. Figure 7-4 clearly confirms the lack of relationship between the perception of data sensitivity and actual behaviour, these results do not support Hypothesis 10b.

**Figure 7-3 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Actual Acceptable Scenarios by Their Reward Cluster**



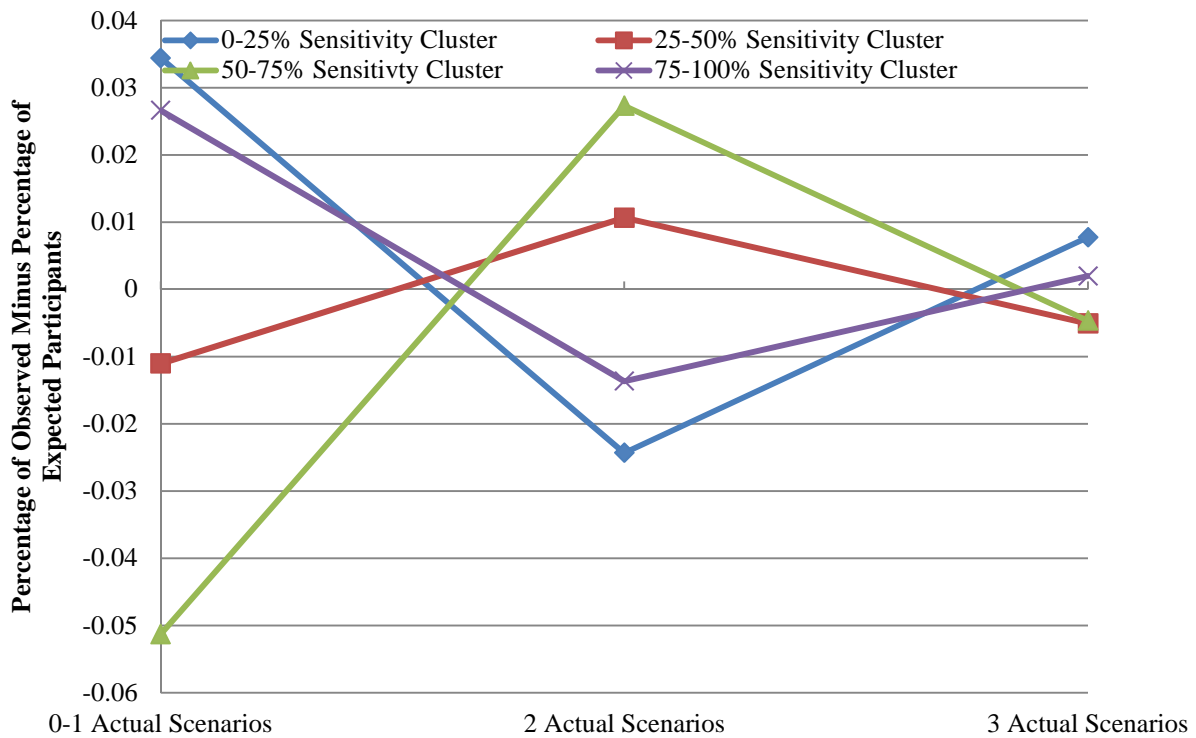
*H10b: The level of sensitivity associated with a data type will negatively impact a user's behavioural intention. – NOT SUPPORTED*

#### 7.4.3. Data Holder

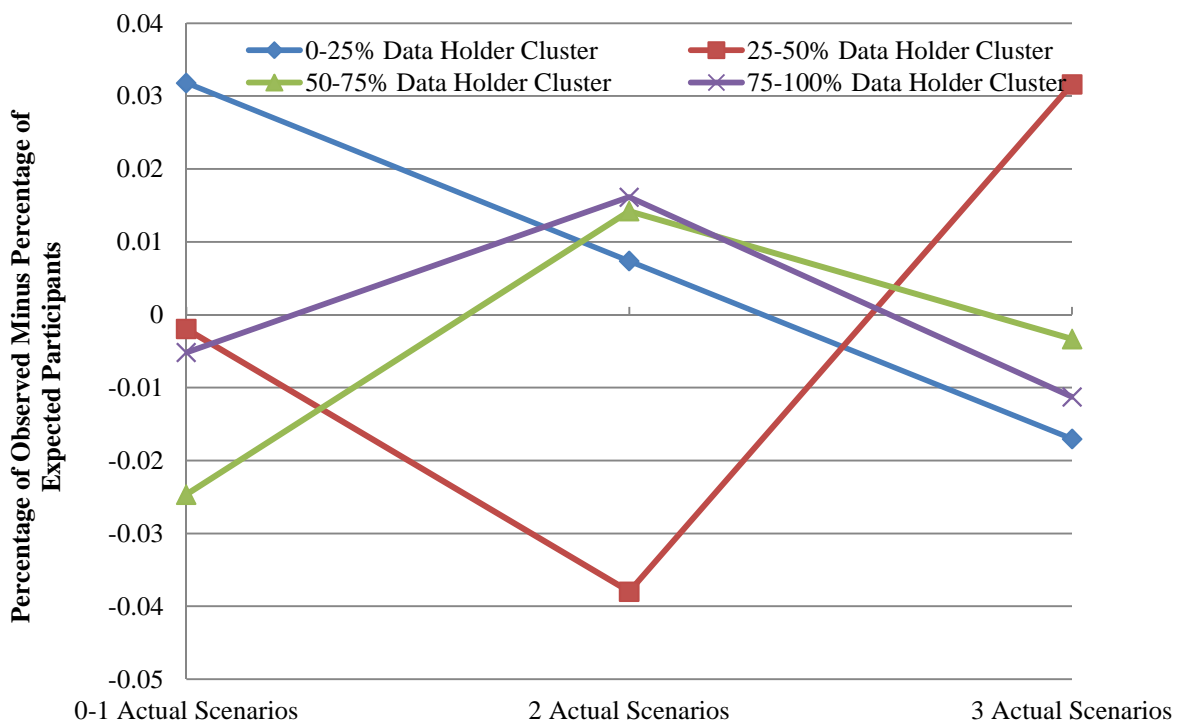
It was also expected after the literature review that if a participant had a high level of trust in the data holder, then they would be more willing to disclose their personal information. Table 7-4 shows that the results of the European survey suggest that this is not actually the case. The results of the Chi Squared test report do not show a relationship between the two variables. The lack of correlation between the two variables is clearly highlighted further in Figure 7-5. As a consequence, the results of the European survey do not support Hypothesis 10c.

*H10c: The level of trust a user has in the new data holder will have a positive impact on the user's behavioural intention. - NOT SUPPORTED*

**Figure 7-4 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Actual Acceptable Scenarios by Their Data Sensitivity Cluster**



**Figure 7-5 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Actual Acceptable Scenarios by Their Data Holder Trust Cluster**



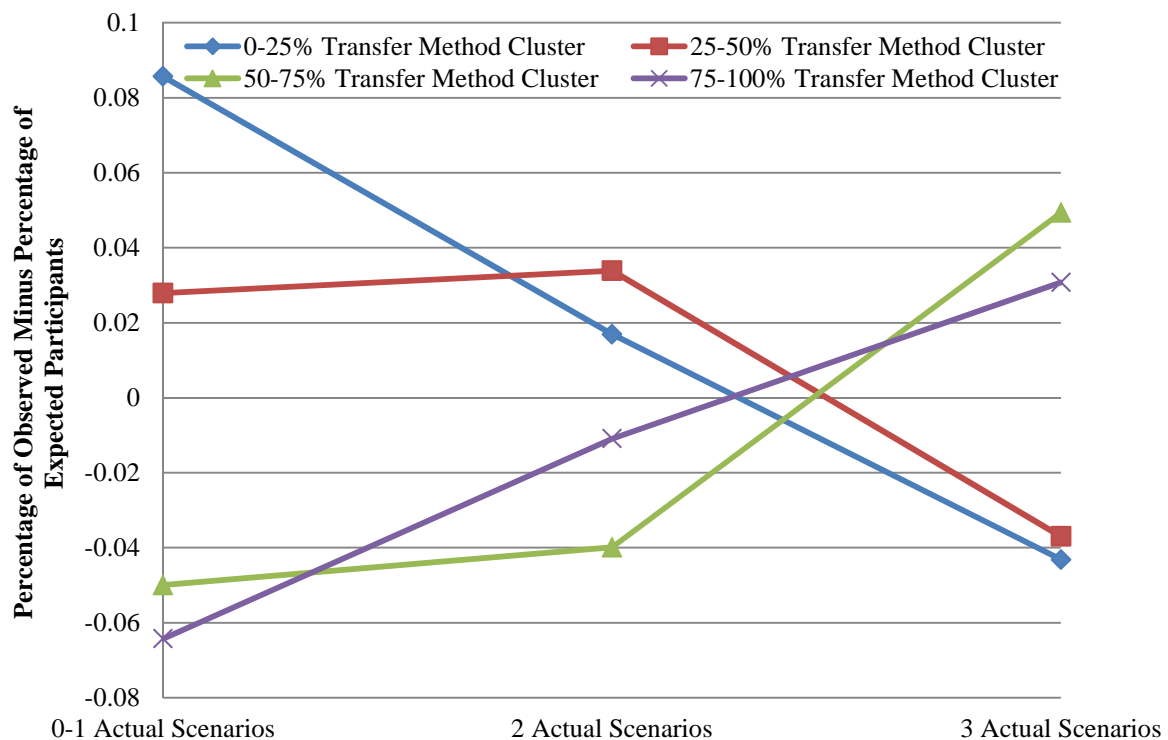


#### 7.4.4. Transfer Method

Unlike the perceptions of the previous three privacy variables, the results of the European survey suggest that a future ITS user's perception of how safe the transfer method is will be significantly correlated with the user's actual privacy behaviour and Hypothesis H10d is supported. This fact is supported not only by Figure 7-6 which shows how the most trusting participants turned out to be the ones that found most of the real life privacy scenarios acceptable, but also by the results of the Chi Squared test of independence found in Table 7-4. This outcome is particularly interesting because the literature review at the beginning of this outcome showed how virtually all of the research on privacy within the transport field to date has been on making the method of transfer an individual's personal information as secure as possible. This indicates that this previous research has been put to good use and is seeking to improve an area that is directly related an individual's actual privacy behaviour.

*H10d: The level of trust a user has in the data transfer method will have a positive impact on the user's behavioural intention. – SUPPORTED*

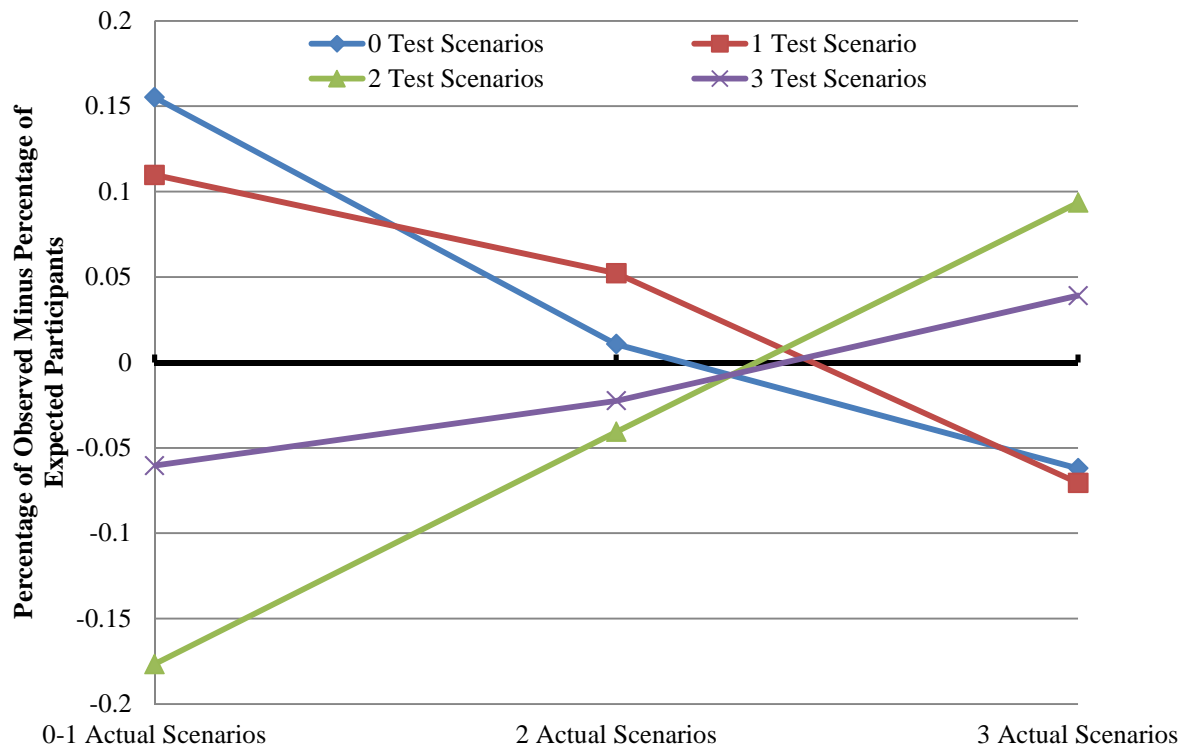
**Figure 7-6 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Actual Acceptable Scenarios by Their Transfer Method Trust Cluster**



### 7.5. Influence of Behavioural Intention on Actual Behaviour

Hypothesis 11 of the research model predicts that a future ITS user who states they intend to exchange their personal information is actual more likely to do so when the opportunity presents itself in real life. To test this (see Table 7-1), the European questionnaire asked the participants how they intended to act when faced with a privacy scenario and then investigated their actual behaviour in those same scenarios. Figure 7-7 compares the percentage of observed minus the percentage of expected participants for the acceptable number of test scenarios against the actual number of acceptable scenarios. This figure clearly shows that a participant who found none of the test scenarios acceptable are the most likely to have withheld their personal information in the real life scenarios.

**Figure 7-7 Percentage of Observed Minus Percentage of Expected Participants for Each Number of Actual Acceptable Scenarios by Their Stated Number of Acceptable Scenarios**



A Chi Squared test for independence shows that the results of the European survey indicate that there is statistically significant relationship between a participant's total number of acceptable test scenarios and the total number of actual scenarios they find acceptable, the p value for this test is 0.000. Table 7-5 looks at the acceptability rates for the individual scenarios. From this table you see for each of the three scenarios the relationship between the test and actual answers are all statistically significant. In each scenario, it is also the case more participants are willing to disclose their information in reality when compared to their stated intention.

**Table 7-5 Actual and Test Scenarios**

Scenario Type	Question	Acceptability Rate	p	Significant
Actual Scenario 1	Loyalty Card	77%	0.004	Yes
Test Scenario 1		33%		
Actual Scenario 2	Internet Shopping	86%	0.000	Yes
Test Scenario 2		46%		
Actual Scenario 3	Airport Security	96%	0.000	Yes
Test Scenario 3		17%		

The number of participants who stated they would not disclose their personal information but actually did ranged between 54-83% across the three scenarios, whereas the number of participants who stated that they would disclose their personal information but in reality withheld it only ranged between 4-23% across the three scenarios. This adds weight to the argument presented in the literature review (Chapter 3) that people are actually more likely to disclose their personal information than their level of privacy concern and stated intention suggests. This evidence also supports Hypothesis 11 in the research model.

*H11: A user's actual behaviour will be significantly impacted by their stated behavioural intention. - SUPPORTED*

## 7.6. Predicting Actual Behaviour

This chapter so far has not considered how a participant's level of privacy concern, their demographics, their perceptions of the privacy variables and their stated behavioural intention might interact with one another and enable predictions to be made about a participant's actual behaviour when confronted with a privacy scenario. Figure 7-8 shows the Pearson's  $r$  correlation coefficient between the four privacy variables and actual behaviour. This shows that only one of the privacy variables (transfer method) was shown to have a statistically significant relationship with actual privacy behaviour. Even when demographics are included, the ability to predict actual privacy behaviour by considering only one-way interactions appears to be limited. An enter method, multiple linear regression model of all of the privacy variables, demographics and stated behaviour had a  $R^2$  value of 0.065 therefore accounting for approximately 6.5% of the participant actual privacy behaviour. Table 7-6 shows that only; gender, perception of the transfer method and the participants' stated behavioural intention had a statistically significant relationship with actual behaviour, with stated behavioural intention being the best single predictor.

Figure 7-8 Correlation between Privacy Variables and Actual Behaviour

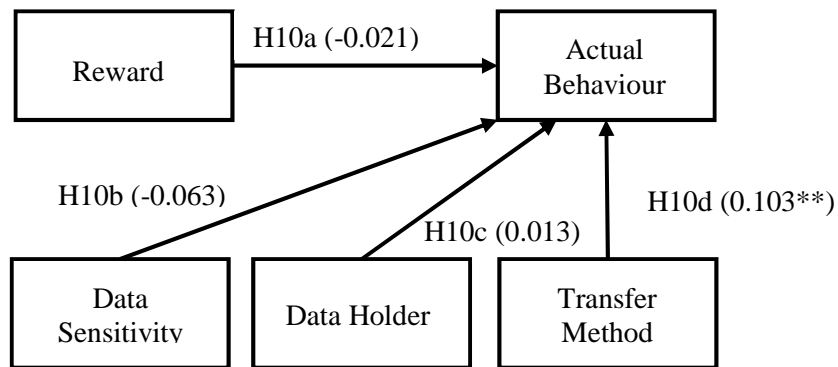


Table 7-6 Variables in Multiple Linear Regression Model of Acceptable Number of Actual Scenarios

Variable	Standardized Beta	t	Sig.
Constant		12.355	.000
Privacy Invasion	.018	.486	.627
Income Level	.043	1.181	.238
Education Level	.040	1.108	.268
Gender	-.077	-2.156	.031
Reward	-.026	-.661	.509
Data Sensitivity	-.005	-.132	.895
Data Holder	-.016	-.372	.710
Transfer Method	.103	2.541	.011
Privacy Concern	.021	.560	.575
Stated Behaviour	.161	4.209	.000
Greece	.021	.473	.637
Netherlands	-.070	-1.623	.105
Austria	.027	.592	.554

In Chapters 5 and 6 it was shown that two-way interactions played a significant role in improving the ability to predict a future user's level of privacy concern and stated behavioural intention, respectively. It is therefore likely that considering them will also help improve the ability to accurately predict a future ITS user's actual behaviour. Unfortunately, it is not practical to look at every two-way interaction and the potential impact it could have on an individual's actual privacy behaviour. Instead, backwards stepwise likelihood ratio logistic regression has been used to model the combined effect of using all the variables discussed so far in this chapter and their two-way interactions to predict if a participant would actually disclose their personal information in all three of the privacy scenarios set out earlier in this chapter. As with the previous logistic regressions, it was not possible to include two-way interaction involving income level as there were too many missing values.

By simply predicting that every participant would disclose their personal information in all three of the real life situation, you would be correct 52.3% of the time. By using the binary logistic regression model shown in Table 7-7, which has a Cox & Snell  $R^2$  value of 0.345 and a Nagelkerke  $R^2$  value of 0.460 you, would be correct 76.0% of the time. An  $R^2$  value of 0.460 is fairly high for behavioural research such as this, and suggests that the model accounts for roughly 46% of the variance in a participant's actual privacy behaviour. If the model was used to predict the actual behaviour of every citizen within Europe, an improvement in accuracy of 23.7% will be very significant (circa 155 million extra correct predictions).

Table 7-7 shows although the hypotheses relating to a participant's level of concern and the perception of three of the privacy variables proved unsupported when considered in isolation, when their two way interactions were considered in the logistic regression model, the participants demographics, their general level of privacy concern, their perception of all of the privacy variables and their stated behavioural intention all added to the accuracy of the model. Although roughly half of the variance in the participants' actual behaviour is still unaccounted for, it is still fair to say that the participants were at least to some degree attempting to act rationally and trying to weigh up the reward on offer against the potential costs of disclosing their personal information. However, the fact that half of the variance is still unaccounted for suggests that the participants are acting with at least a small amount of irrationality. However, the improvement in the ability to correctly predict a future ITS user's stated privacy intention because of the interaction between the stated variable is high enough to support Hypothesis 12 within the research model.

*H12: A user's actual behaviour will primarily be derived from their stated behavioural intention, demographics, general level of primary concern and a trade-off between their perceptions of the reward on offer against the risk associated with a scenario. – SUPPORTED*

**Table 7-7 Variables in Binary Logistic Model of Actual Privacy Scenarios**

<b>Variables</b>	<b>Wald</b>	<b>df</b>	<b>Sig.</b>
Income Level	14.629	4	.006
Education	9.973	4	.041
Age	14.528	5	.013
Concern Level	11.419	3	.010
Perception of Reward	13.664	3	.003
Perception of Data Holder	8.310	3	.040
Country * Level of Concern	19.413	9	.022
Country * Perception of Reward	19.271	9	.023
Country * Sensitivity of Data	19.713	9	.020
Country * Perception of Data Holder	23.301	9	.006
Country * Perception of Transfer Method	22.044	9	.009
Education * Level of Concern	21.266	12	.047
Education * Perception of Transfer Method	23.346	12	.025
Level of Concern * Perception of Reward	17.272	9	.045
Level of Concern * Sensitivity of Data	18.788	9	.027
Country * Education	39.418	12	.000
Country * Experience of Invasion	7.375	3	.061
Country * Minority	6.352	3	.096
Education * Behavioural Intention	15.434	4	.004
Behavioural Intention * Perception of Transfer Method	10.130	3	.017

### 7.7. Summary

The analysis of the actual behaviour questions within the European questionnaire has shown support for some of the hypotheses set out in the research model but not others. The results added weight to the theory that a person's demographics would influence their actual privacy behaviour and supported Hypothesis 8. In particular, the results showed that the British were the most willing to disclose their personal information and the Greeks were the least likely to do so. It also found that younger the participant is, the more likely they were to disclose their information. This supports the findings of previous research highlight in the literature review (Fox et al. 2000 and Wallis 2007). Contrary to what was expected from the literature review, however, the results of the European survey suggest that people with a high income and/or high level of education are more willing to disclose their personal information than those with lower incomes and education levels.

The results of the European survey also went against some of the findings in the literature review and found that there was no correlation between a participant's general level of privacy concern and their actual privacy behaviour. It had been expected that those participants that expressed a high level of privacy concern would be more likely to withhold their personal information, but analysis of the results showed that the relationship between the two variables was statistically insignificant. Hypothesis 9 is therefore not supported.

It was also discovered that three of the privacy variables (the reward on offer, how sensitive the information was and who the information was going to) had no direct impact on a person's actual privacy behaviour, disproving Hypotheses 10a-c, although the logistic regression model did show that when each of these variables was combined with another variable (such as the participant's country) they added to the predicting ability of the model. Hypothesis 10d, however, was supported, because the results showed that the relationship between the level of trust a user had in the transfer method and their actual behaviour in the three privacy scenario was statistically significant. This is a noteworthy result because most of the privacy-related work that has been conducted to date within the transportation field has been centred around making the ITS communications as secure as possible. The results of the European survey indicate that this work could play a crucial role in improving the penetration rate of future ITS.

Another significant result discovered in this chapter was that there is a direct link between a participant's stated behavioural intention and their actual behaviour. Not only does this support Hypothesis 11, but the results also show that far more people are likely to trade their personal information in real life than when faced with a hypothetical scenario. For future ITS, this means that likely uptake rate of a technology is probably going to be higher than a survey of stated intentions would suggest. The results also showed that only a range of 4-23% of people who state they would disclose information would not in reality, compared to a range of 54-83% for people answering 'no' to the stated intention question changing their mind in reality.

The final hypothesis tested in this chapter was Hypothesis 12, which predicted that a future ITS user's actual behaviour will primarily be derived from their stated behavioural intention, demographics, general level of primary concern and a trade-off between their perceptions of the reward on offer against the risk associated with a scenario. Whilst it was not possible to test this for a future ITS, the indication from the three real life scenarios was that a combination of the afore mentioned variables would account for approximately 46% of the variance in the participants actual privacy behaviour and would allow predictions about the acceptability of a scenario to be made with approximately 76% accuracy. Although this supports Hypothesis 12, it also adds weight to some of the theories stated in the literature review which suggest that future ITS user's will not be capable of acting completely rationally, but would possibly act in a predictably irrational manner instead.

Another interesting discovery to note are the similarities and differences in the factors that were shown to impact the participants stated behavioural intention with regards to the hypothetical ITS scenarios and their actual behaviour in the real life scenarios. The first similarity is that in both cases young highly educated, high-income British people were the most likely to exchange their personal information. The results of the stated intention questions showed that the Dutch stated they would give away the least amount of information, but in reality, the Greeks disclosed the least but the margin was minimal. Both cases found that the general level of privacy concern and the perception of the reward on offer had no direct relationship with the participants' privacy decision-making, but do add to the accuracy of the logistic regression models when combined with other variables.

The three privacy cost variables were found to have a direct relationship to the participants' stated behavioural intention, whilst analysis of the real scenarios showed that only the participants' perception of the transfer method had a direct impact on their actual behaviour. Another disparity between the participants' stated and actual behaviour was that more variables and their two-way interactions were found to improve the logistic regression model for actual behaviour. This suggests that factors which did not improve the regression models for a participant's stated behaviour such as the participant's age, income level and perception of the reward on offer actually play a significant role in helping to predict the outcome of a real life scenario.



## 8. Will Privacy be a Barrier to Future ITS?

### 8.1. Introduction

This chapter will bring together everything that has been discussed in this thesis so far and specifically address the question ‘Will Privacy be a Barrier to Future ITS?’. It will do this by first looking at the outcomes of the research model. The links between privacy concern, behavioural intention and actual behaviour will then be discussed. The Chapter then moves on to address the individual factors that could impact the acceptability of a future ITS, before highlighting the gaps in knowledge that this research has been able to fill. This knowledge is then used to pinpoint future ITS that might be deemed unacceptable in privacy terms and suggest methods for reducing their privacy impact. The final sections of this chapter then looks at the limitations of this research and areas in which future research could help to further develop a deeper understanding of human privacy decision-making in regards to future ITS.

### 8.2. Research Model Outcome

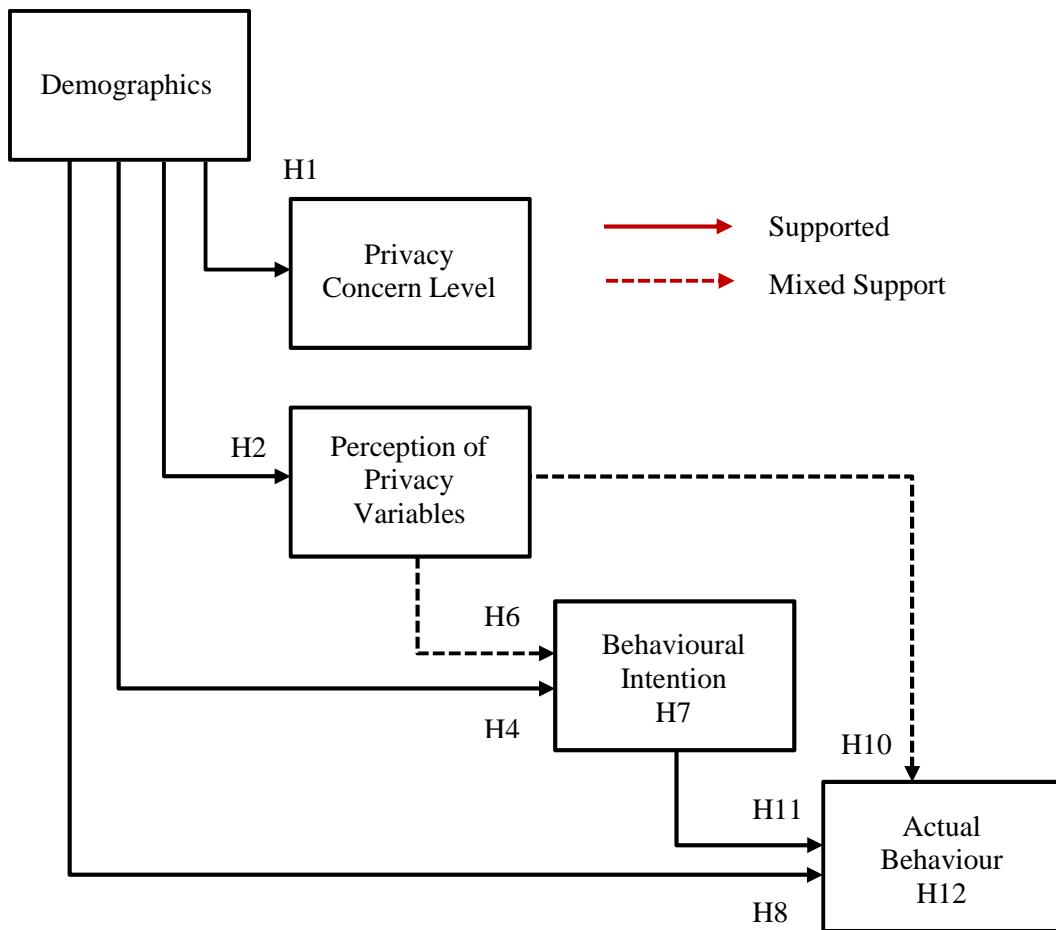
Chapters 5 to 7 tested the research model developed in Chapter 3 by analysing the results of the European survey which sought to investigate the underlying influencing factors of a person’s behaviour when faced with a privacy scenario. Table 8-1 and Figure 8-1 shows whether the results of the European survey supported the hypotheses made as part of the research model in Chapter 3. The first thing that becomes clear by looking at the summary of the European survey results is that a user’s level of general concern is not directly linked with their perception of the privacy variables, their stated behavioural intention or most importantly their actual privacy behaviour. Whilst this was unexpected it does support the consensus that although a future ITS user could be concerned about disclosing their personal information they might still disclose their personal information anyway.

It should be noted that although there was no direct link between the level of concern and the participant’s actual behaviour, the inclusion of a participant’s level of concern and its interaction with other variables improved the level of accuracy of the Logistic Regression model for actual behaviour in Chapter 7. This means that if a user’s level of concern is known, predictions about their likely future behaviour will be more accurate. As well as the impact of the level of a user’s concern, not all of the hypotheses made in the research model about the impact of a future ITS user’s perceptions of the privacy variables would have on actual behaviour were supported. A direct link was only found between the survey participants’ perception of how secure the transfer methods were and their actual behaviour. This was surprising because all of the cost privacy variables were found to be significantly link with the participant’s stated behavioural intention.

**Table 8-1 Table Showing Whether the Results of the European Survey Support the Research Model Hypotheses**

Hypothesis	Supported	Comments
H1: A user's level of privacy concern will be impacted by their demographics.	YES	Some demographics and their two-way interactions proved significant.
H2: A user's perception of the four privacy variables will be impacted by their demographics.	YES	Some demographics proved significant for all four privacy variables.
H3: A user's perception of the three privacy cost variables will be linked to the user's general level of privacy concern.	NO	The level of concern was not significant connected with any of the privacy cost variables.
H4: A user's stated behavioural intention will be impacted by their demographics.	YES	Some demographics proved significant.
H5: A user's stated behavioural intention will be impacted by their general level of privacy concern.	NO	The level of concern was not significant.
H6: A user's stated behavioural intention will be impacted by their perceptions of the privacy variables	MIXED	The perception of the reward has no significance but all of the privacy cost variables are significant.
H7: A user's stated behavioural intention will primarily be derived from their demographics, general level of primary concern and a trade-off between their perceptions of the reward on offer against the risk associated with a scenario.	YES	The variables and their two-way interactions account for 33.3% of the variance in the participant's stated behaviour intention.
H8: A user's actual behaviour will be impacted by their demographics.	YES	Some demographics proved significant.
H9: A user's actual behaviour will be impacted by their general level of privacy concern.	NO	The level of concern was not significant.
H10: A user's actual behaviour will be impacted by their perception of the privacy variables	MIXED	All but transfer method No
H11: A user's actual behaviour will be impacted by their stated behavioural intention.	YES	The stated behavioural intention proved very significant.
H12: A user's actual behaviour will primarily be derived from their stated behavioural intention, demographics, general level of primary concern and a trade-off between their perceptions of the reward on offer against the risk associated with a scenario.	YES	The variables and their two-way interactions account for 46.0% of the variance in the participant's actual privacy behaviour.

Figure 8-1 Supported Research Model Relationships



Whilst the participants' perceived value of the reward on offer was not directly linked to either their stated behavioural intention or their actual privacy behaviour, the logistic regression model used in Chapter 7 did actually find that these variables did indeed add to the accuracy of the model. One limitation of this research is that no null reward was offered in the privacy scenarios which could have impacted the outcomes of this research. It is interesting to note the fact that all of the privacy cost variables are shown to influence a person's stated behavioural intention. This is especially noteworthy as the most useful predictor of actual behaviour was shown to be the participant's stated behavioural intention.

What the results of the European survey also show clearly is how a future ITS user's demographic background is likely to play a significant role in shaping not only their actual privacy behaviour but also their level of concern, perceptions of the privacy variables and their stated behavioural intention, all of which in turn have been shown to help predict a person's actual behaviour. It was shown that the impact of some of the demographic variables (age, gender and experience) was consistent across the different privacy stages; elderly females who had experience previous privacy invasions had a higher level of privacy concern, stated that they found their personal information more sensitive, found both the future data holder and transfer method less secure and were more likely to state that they will act in a privacy preserving manner, whereas, some demographics such as; cultural background, income and education levels varied across the different privacy stages.

### 8.3. The Links between Concern, Behavioural Intention and Actual Behaviour

As discussed in the previous section, the results of the European survey further highlighted the disconnect that was observed in previous research (Hui et al. 2007 and Berendt et al. 2004) between an individual's privacy concern and the actual privacy behaviour. The impact of this for future ITS developers is that they need to be less worried about users expressing a high level of privacy concern, but instead should focus on whether potential future users state whether they would use their future ITS or not.

This is because the results of the European survey have shown that there was a very significant link between a participant's stated behavioural intention and their actual privacy behaviour. It was actually the case that the participants were more likely to disclose their personal information in real life than their stated behavioural intention suggested. This again supported the findings of the literature review and suggests that the uptake of a future ITS in reality will be higher than a survey of stated intentions would suggest. These results also show the importance of future ITS developers addressing the factors that impact the user's stated behaviour as it is very unlikely that a future ITS user will state they will disclose their personal information and then in reality withhold it. It is also a lot easier for future ITS developers to measure a group of future ITS users' stated behaviour in relation to their future system than their actual behaviour.

## 8.4. What Will Impact the Acceptability of a Future ITS in Privacy Terms

The results of the literature review and European survey have shown the main factors that will influence a future ITS user's stated and actual behaviour are their demographics, cultural background and their perception of the privacy cost variables. This section will look at each of these factors and discuss how they could impact the acceptability of a future ITS.

### *8.4.1. Demographics of users*

A future ITS user's demographics are likely to have a significant influence on their privacy decision-making. This research has shown that age, gender, income and education levels all have an influence on how willing a future ITS user will be to actually disclose their personal information. Young highly educated, high earning males were shown to be the most likely to find future ITS privacy scenarios acceptable, whereas elderly, less educated females with a low income were shown to be the least. Whilst some ITS developers might be developing systems that they intend a whole population to use, others may be targeting more focused groups. The implication of the demographic variance means that a system that was designed for, and deemed acceptable by, tech savvy young males might not be deemed acceptable by elderly females with little experience of using the new technologies. If this system is then rolled out for intended use by a whole population the voluntary uptake rate will be significantly lower than if the system was designed with elderly females in mind. If the system required a high penetration rate to operate efficiently then this could be the difference between the new ITS being a success or a failure.

### *8.4.2. Cultural background of users*

This research has shown that a future ITS user's cultural background is likely to have a substantial impact on their willingness to disclose their personal information. The standout result is that participants from the UK were the most willing to disclose their personal information in both the behavioural intention and actual behaviour scenarios. Interestingly the United Kingdom participants contradicted this by also being the most concerned country of the four sampled. This further highlights the severity of the disconnect that exists between a future ITS user saying that they are concerned about privacy and then actually withholding their information when faced with a privacy scenario.

The next observation that can be made is that the United Kingdom has the highest score out of the four countries in Hofstede's individualism dimension (89)(Hofstede 2001). The majority of the evidence from previous research on this topic suggests that countries with a high level of individualism will be more willing to share their personal information. Whilst the results for the United Kingdom support these findings, the fact that the participants from the Netherlands (Individualism =80) were the nation least willing to disclose their personal information in the actual behaviour scenarios and the second least likely in the behavioural intention scenarios suggests that other factors may also be influencing the cultural impact on privacy.

The link between the results of the European survey and the Privacy International Privacy Policy Index (Privacy International 2007) could also offer a clue to why different cultures act differently when faced with the same privacy scenario. The Privacy International survey ranks the countries in the following order in terms of having the most invasive government policies; the United Kingdom, the Netherlands, Austria and then Greece. These results replicate the willingness of participants from each country to disclose their personal information in the actual privacy scenarios, with the participants from the United Kingdom being the most willing and the participants from Greece the least. This phenomenon is also backs up the theory promoted in the literature review that the reason why road pricing was deemed acceptable in London but not Hong Kong was due to the fact that citizens in London were already used to being monitored by a large amount of CCTV cameras.

The results of the behavioural intention scenarios that focused specifically on future ITS do not support this trend (although the British were again the most willing to disclose their personal information) as the Greek sample was the second most willing group of participants. One potential reason for this is that these questions related to a specific industry (transport) whereas the Privacy International survey was focus on a more macro level.

It is likely that both a country's cultural dimensions and its current level of state surveillance will influence the privacy behaviour of its citizens. However, it could be debated that the privacy views of the public will influence the state's level of invasion, especially in a democratic country. What is clear though is that future ITS user's from different cultural backgrounds could act very differently when faced with a privacy scenario. Bearing this in mind, future ITS developers will need to adjust the privacy requirements of their proposed systems depending on which country the technology is being launched in. If it is planned for a future ITS system to be implemented across the whole of the European Union then the developers would be wise to focus on the privacy demands of the Dutch and Greek public and not the British.

#### *8.4.3. Sensitivity of the data required*

It has been shown that the sensitivity of the data required by a future ITS greatly influenced the participants' stated behavioural intention with regard to future ITS. Surprisingly though data sensitivity was not shown to have a direct influence on the acceptability of the actual privacy scenarios used in the European survey. The participants' perception of how sensitive different types of information could be split into three distinct tiers. Highly sensitive data included embarrassing secrets, financial data and medical records. The least sensitive tier included local weather conditions, musical preferences and the participants' nationality. The most critical data types for future ITS, driving behaviour and location history, were both in the middle tier. This tier was different from the other two because the participants had very mixed views on the sensitivity of the data with some finding these data types highly sensitive, while others found it not sensitive at all.

The different impact data sensitivity had on behavioural intention and actual behaviour shows that the participants were influenced by different factors when they were faced with a real and hypothetical privacy scenario. Considering that the participants were more likely to disclose their personal information in the actual scenarios, this could mean that in reality they cared less about how sensitive the information they were giving away was than their stated behaviour would suggest. However, a future ITS developer should still attempt to use the least sensitive data wherever possible to reduce the number of individual who will state they will not use their ITS, (even though in reality the results of this research suggest that data sensitivity may not be critical).

#### *8.4.4. Level of trust in the new data holder*

As with data sensitivity, the results of this research have shown that the perceptions of how safe a participant's personal information is in hands of various different data holders can be split into three distinct tiers. The unsecure category includes strangers, journalists and criminals. The middle category includes work colleagues, the government and private companies. The most secure data holders were perceived to be family, friends and medical and legal professionals. Again, most future ITS would use data holders who fall into the middle category as they will be operated either by governments or private companies.

Again, in a similar manner to data sensitivity, the level of trust in the data holder was shown to have a large influence on stated behaviour but to have no direct influence on the actual behaviour scenarios in the European survey. This further highlights that participants must use a different thought process when faced with real and hypothetical scenarios. Although it may not prove to be critical in reality, ITS developers may want to consider getting a legal professional, or someone who will face real and substantial consequences if any abuses occur, to look after the personal information, especially if a high penetration rate is required.

#### *8.4.5. Level of trust in transfer method*

Unlike for data sensitivity and the level of trust in the data holder, there were not any distinct tiers in the perceived safety of different transfer methods. Instead, all of the different transfer methods apart from a private face to face meeting were perceived to be roughly as secure as one another. This is particularly interesting because virtually all of the research that has been conducted into privacy within the transportation field has gone into making the transfer method as technologically secure as possible. Yet the participants found it very difficult to differentiate between the level of security provide by a message sent by physical mail and a message sent over a wired internet connection.

Another difference between the perception of the transfer method and the perceptions of data sensitivity and the future data holder is that it was shown to influence both behavioural intention and actual behaviour. For ITS developers this insight could be crucial as this is that only factor that was shown to directly impact actual behaviour that they have control over. This is also the area in which the most privacy research effort has gone into and so long as this is successfully portrayed to future ITS users', using secure transfer methods should have a positive impact on improving the penetration rate of future ITS.

### 8.5. Reducing privacy impact

From looking at the main influencers of privacy decision-making highlighted in the previous section, a future ITS developer can address several key aspects of a future ITS that could improve a future user's willingness to disclose their personal information. Other than targeting users from specific demographic and cultural backgrounds who would be more likely to disclose their personal information (young British males), the main way a future ITS developer can influence the user's willingness is by addressing the privacy cost variables.



This research has shown that the cost variable with the greatest effect on a user's actual behaviour will be their perception of how secure the transfer method is. You only having to look at the financial industry and e-banking in particular, to see that people are willing to transfer even the most sensitive of information (financial data) to fairly untrusted data holders (private company) because they perceive the method of transfer to be secure. The key to ensuring that the transfer method is perceived as being secure is to not only make the communication as technologically secure as possible, but to also make future users aware of just how secure the transfer methods are. Essentially, it does not matter how secure a transfer method actually is if future users are not told about it because they will presume the worst (Malhotra et al. 2004).

One method that could potentially help future ITS users understand exactly how secure the transfer method is, is to get an independent body to test how secure your system is and to compare it not only to other ITS but also more common privacy scenarios. Whilst some privacy audits do exist (Warren and Charlesworth 2012) these are aimed more at ensuring that current regulations are being met than informing the end user in a clear, concise and quick manner. Some research though has looked at using 'privacy nutrition labels' to highlight key information to users (Kelley et al. 2010). New cars already get a Euro NCAP safety rating to help inform drivers just how safe different types of vehicles are (Euro NCAP 2013). It is therefore feasible that a similar rating system could be used to rate how secure your personal information is with future ITS.

Whilst the results of the European survey did not show that a user's perception of the data sensitivity and how much they trusted the new data holder had direct impact on the participants' actual behaviour, they did show that they had a significant impact on a participant's stated behavioural intention with regards to future ITS. A participant's stated behavioural intention was then shown to be strongly linked with their actual behaviour. Therefore if a future ITS developer alters these two cost variables, it is likely that they will also alter the willingness of future users to disclose their personal information.

As a consequence, where possible future ITS developers, in addition to improving future users' perception of the transfer method, should also use the least sensitive data possible and the most trusted data holder. In order to use the least sensitive data possible future ITS developers may be forced to downgrade the reward they are offering as a result. However, the results of this research and research within the field of behavioural economics (Kahneman and Tversky 1979) suggest that when faced with an actual decision, the perception of the cost variables will outweigh the reward.

## 8.6. New Knowledge

The first new thing that this research learnt was that most of the demographic influences that had been discovered in previous research in other fields appear to have the same effect in the transportation field, except for the influence of education level and income level. A participants willingness to disclose information to future ITS was shown to increase as these two variables increase, which is the opposite of what was expected. One possible explanation for this is that educated high earners sampled have had more exposure to existing ITS, so due to their previous positive experiences they are less concerned about future ITS.

It has also been shown by this research that a future ITS user's cultural background will have a dramatic effect on their privacy behaviour in relation to future transport technologies. Citizens from the Netherlands were shown to be the most privacy preserving and citizens from the United Kingdom the most willing to disclose their personal information of the four culturally diverse countries that were sampled. This research also showed that a future user's stated level of privacy concern will have little impact on their actual willingness to use a future ITS.

In addition, the results found that there was a difference between stated and actual behaviour. It was shown that in real life users were potentially more impacted by irrationality and heuristics, as they were more willing to give away more information than their stated behavioural intention would suggest. Potentially the most significant new finding from this research was that the most powerful tool ITS developers have for improving the willingness of future ITS users to disclose their personal information is by reducing the perception of the three privacy cost variables. The perception of the transfer method was shown to be particularly crucial. In direct contrast, it was shown that improving the reward on offer in a scenario would potentially have little impact on the overall acceptability of the technology.

In summary, the two key strides forward that this research are; firstly identifying the most likely demographic groups to reject future ITS due to privacy fears (elderly, less educated, low earning Dutch women) and; secondly, highlighting that the key variables that future ITS developers can alter to reduce the privacy impact of their technologies are the future ITS users' perceptions of the privacy cost variables (the type of data used, which data holders the information is given to and most influentially the method used to transfer the information).

## 8.7. Limitations

Whilst this research has taken strides forward in terms of improving the knowledge of how privacy will impact future ITS, there are still some limitations to this research. The most substantial limitation of this research is that it has only looked at the ‘what’ and not the ‘why’ with regards to the factors that will influence future ITS users’ privacy decision-making. In particular this research failed to look in any detail at ‘why’ the survey participants’ level of trust varied not only with their demographics but also different data holders and transfer methods. In a similar way, the impact social norms and other heuristics had on the participant’s perception of the privacy variables and their stated and actual privacy behaviour was not explored.

Although knowing the ‘why’ would add significantly to existing knowledge, this research prioritised identifying ‘what’ variables influenced privacy decision-making over developing a detailed understanding of ‘why’ these variables influenced privacy decision-making. To develop a detailed understanding of ‘why’, every variable that was shown to influence privacy decision-making would have been too large a scope for this particular piece of research but it would definitely have added to existing knowledge at the disposal of future ITS developers.

In addition to concentrating on the ‘what’ there were potentially also some limitations with the methodology used. It was argued in Chapter 4 that as this research model had been derived from existing literature that quantitative data would prove the most useful for interrogating the research model. This is likely to be an accurate judgement but if this research had also conducted some qualitative research it would have added not only to the understanding of ‘why’ the factors identified influenced privacy decision-making but would also have verified that the research had covered all of the potential influencing factors. Some qualitative data could also have helped future ITS developers identify exactly what they would need to do to reduce data sensitivity and increase trust in the data holder and transfer method.

Another potential limitation of the methodology used in this research was that it was not possible to use exactly the same questionnaire distribution method in each country. This was caused by a combination of not gaining access to appropriate mailing lists in all of the countries except the UK and weather conditions during the Dutch survey. Even with differences in the questionnaire, distribution methods the differences in the demographic distributions of each countries sample was small due to the multi-modal distribution and the targeting on demographic groups to balance out each countries sample.

Although it limited the differences in demographic groups sampled in each country, the use of the multi-modal distribution did mean that in some of the countries a high proportion of the participants expressing their views did so through the use of technology. As discussed in the Methodology Chapter (Chapter 4) it was not ideal to have participants expressing views on whether privacy concerns would prevent them from using future technologies through technology. However, it was also decided that it was better to get a sample population that represented the demographics of the wider country and potential miss some of the views of people too concerned about privacy to use technology than to have large demographic groups missing.

With regards to the questionnaire that was distributed, in hindsight, there were potentially a couple of limitations to its design. Firstly, none of the scenarios offered ‘no reward’ in return for the participant disclosing their personal information. In the initial design phase it was thought that the differences in the value of the rewards offered in the various would cover a wide enough range to see the impact the reward offered in a privacy scenario had on privacy decision-making. However, this was not the case and no link was found between the reward being offered and a participant’s likeliness to find a scenario acceptable. Without having a scenario offering ‘no reward’ this research was unable assess if there was a difference in the acceptability rate of a scenario offering ‘no reward’ and one offering a reward. Theories from the field of behavioural economics such as prospect theory (Kahnemann and Tversky 1979) suggest that whilst any reward is better than no reward, the increase in the impact of the reward value diminishes as the value of the reward increases, so it may be the case that as long as a future ITS offers some form of reward the actual value of that reward will not have a significant impact on the acceptability of the technology. Unfortunately from this research it is not possible to draw any conclusions on this.

The second change that would be made to the questionnaire design in hindsight is that the three general scenarios would be replaced with three further ITS scenarios. The three test scenarios could then be used to not only explore then link between stated and actual behaviour but also to compare the participants stated behaviour in scenarios relating to transport and general life. By having seven instead of four ITS related scenarios it would have been possible to explore whether different strands of ITS would be more likely to be acceptable to future ITS users than others. For example it would have been interesting to see whether ITS used for automated travel pricing generated more concerns than systems that are focused on creating real time traffic information, as the real life examples explored in Chapter 2 would suggest. Instead, the four ITS scenarios used remained more high level and generic in an attempt to ensure that a wide range of different privacy variables that could be used in real future ITS were investigated.

The final limitation of this research was that it could have explored further whether future ITS users would be likely to express any irrational yet predictable behaviour with regards to the future technologies. The binary logistic regression model used to predict the participants' actual behaviour (Table 7-7) showed that the variables explored in the research model only accounted for approximately 46% of the variance in answers. Although for research of this nature this is a fairly high value, it still means that just over half of the variance in a participants' privacy decision-making is still unaccounted for. The literature review in Chapter 3 suggested that it was very unlikely that future ITS users would act in an entirely rational and hence completely predictable nature due to nature of humans having bounded rationality (Aquisti 2004 and Simon 1982). This is something that this research could have potentially explored further by either conducting some physical experiments to see whether any trends of irrational privacy behaviour became apparent or by attempting to directly apply heuristics proven in the field of behavioural economics to the field of privacy within the context future ITS.

#### 8.8. Recommendations for further work

Whilst this research has taken strides forward in helping identify the most critical aspects of privacy decision-making in relation to future ITS, there are still areas that future research could address. The scope for future research revolves around observing actual behaviour and testing the possible improvements. This research was unable to witness the participants' actual behaviour in relation to future ITS, therefore it is likely that new knowledge would be gained from observing actual behaviour. At the very least, it would test that outcomes of this research, with respect to participants being more willing to disclose their personal information in real life than their stated behaviour and privacy concerns suggest.

In general, more research can look into the “why” aspects of the influencing factors of privacy decision-making and how they relate to ITS. This is something that this research has not attempted to address and whilst the factors that influence trust and human decision-making have been explored within the transport field they have not been explored in any depth in relation to privacy. By observing participants' actual behaviour, it would also be easier to accurately examine the influence of irrational decision-making. It will also be possible to test the extent to which acceptability rates can be improved in real life by altering the privacy variables, which is something that this research suggests could be crucial.

In particular, it would be interesting to investigate how a privacy version of the Euro NCAP rating could be used to increase a user's perception of the transfer method and in turn improve their willingness to disclose personal information. One final factor that this research failed to investigate that would add to existing knowledge, is the impact of offering no reward in return for a user's personal information. This research found that user's did not find the type of reward offered critical when faced with a privacy scenario but it did not test the impact of not offering a reward.

### 8.9. Will privacy be a barrier?

In answer to the question 'Will Privacy Barriers Limit the Uptake of Future Intelligent Transport Systems?', this research suggests that every future ITS will have some users who refuse to disclose their personal information. This means that the compulsory implementation of these systems will ensure that some members of public will travel with less freedom than they did before the ITS was implemented, which as Cruickshanks and Waterson (2011) highlight, means that the privacy fears highlighted at the very beginning of this thesis have a chance of coming to fruition, so making the use of an ITS system compulsory for everyone should be avoided where ever possible.

With regards to non-compulsory systems, the answer is not so simple and will rely heavily on the uptake rate required for the future ITS to be successful in practical and economic terms. The chance of privacy being a barrier to future ITS will increase significantly with the uptake rate required for the system to operate. For example, if a hypothetical traffic management system needs at least 90% of road users to be disclosing their location at all times for its algorithms to function correctly, then it is likely that privacy will be a barrier to its successful launch. On the other hand if a hypothetical safety system only requires 5% of total road users to provide their local weather conditions periodically this research suggests that privacy will not act as a barrier to its successful uptake.

With the appropriate consideration during the design stage of a future ITS, a developer should be able to significantly reduce the privacy impact of a system. Whether the penetration rates for a non-compulsory system will be high enough for the ITS to be sustainable will depend primarily on the demographics of the target audience and their perception of how secure the method for transferring their personal information is. Secondary factors are likely to include how sensitive the required data is and the level of trust the future users' have in the new data holder. The reward offered by the system is likely to have little impact on whether users will find the technology acceptable or not.

## **9. Conclusions**

### 9.1. Introduction

The main conclusion from this research is that privacy has the potential to be a barrier to the uptake of some future ITS. However, by appropriately managing the privacy cost variables present in a future ITS (the transfer method, the type of data required and who the information is going to) a future ITS developer should be able to ensure that enough users are willing to disclose their personal information that the system would be viable. It is also fair to say that this research managed to meet the aim and objectives set at the outset of the research project.

### 9.2. Aim

The overall aim of this research was to better understand the factors influencing privacy decision-making and the impact they will have on the success of future ITS. From the combined results of the literature review and the European survey this has definitely been achieved. In particular, this research found that the major factors influencing privacy decision-making are the demographic and cultural background of the user, combined with the cost privacy variables present in a particular ITS.

### 9.3. Objectives

Objective 1: Understand ‘Privacy’ and human privacy decision-making

This research found that the term ‘privacy’ is complex and very hard to define. As a consequence, this work concentrated less on defining privacy and more on investigating the factors that would influence actual privacy decision-making. The key factors that influenced privacy decision-making were found to be the demographic and cultural background of the ITS user, combined with the cost privacy variables.

Objective 2: Compare existing, proposed and hypothetical ITS paying particular attention to their benefits and the level of personal information they require.

It was discovered that the benefits offered and the type of information required by existing and future ITS varied significantly. This is clearly shown in Table 2-1 and Section 2.6. For future ITS systems, the range of benefits offered by a new system will only be limited by the developer’s imagination, ability and the type of information they are able to obtain about current transport conditions.

Objective 3: Understand the factors that will cause the level of personal information required by a future transport technology to become unacceptable.

This research found that regardless of a future ITS user's demographic and cultural background and the reward on offer, if they perceive the transfer method as unsecure, the data required as sensitivity and the new data holder as untrustworthy, then the future system will be deemed unacceptable.

Objective 4: Understand whether views on the acceptable level of intrusion vary from person to person throughout the European Union member states, and discover what the influencing factors are.

It was discovered that the acceptable level of intrusion will vary significantly from person to person throughout the European Union. In particular it was shown that young, British, highly educated, high earning males are the most likely to disclose their personal information to a future ITS, whereas, elderly, Dutch, uneducated, low earning females would be the most likely group of users to find a future transport technology unacceptable.

Objective 5: Draw conclusions about whether different ITS in their current, proposed and hypothetical forms will be deemed acceptable in 'Privacy' terms.

It was shown that when faced with an actual privacy scenario, future ITS users will be more willing to disclose their personal information than both their level of concern and stated behavioural intention would suggest. As a consequence, it is likely that only systems that require sensitive data, are giving it to untrusted data holders and not using secure transfer methods will be deemed unacceptable.

Objective 6: For technologies that are deemed unacceptable, improvements will be suggested.

In order for all ITS to improve their uptake/penetration rates, this research has made the following key recommendation. That ITS developers concentrate on improving the perception of how secure the transfer method is. To achieve this, developers should not underestimate the importance of a good publicity campaign. Acceptability rates will also be increased if the least sensitive information that will allow the system to operate is used and if this information is then only given to trusted data holders only.



## References

Ackerman M, Cranor L and J Reagle (1999) "Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences", Proceedings of the ACM Conference on Electronic Commerce EC'99.

Acquisti A (2004) "Privacy in electronic commerce and the economics of immediate gratification", Proceedings of the 5th ACM conference on Electronic commerce - EC '04, pp 21.

Acquisti A (2010) "The Economics of Personal Data and the Economics of Privacy", *Change* (1) pp.1-50.

Acquisti A and J Grossklags (2005) "Privacy and Rationality in Individual Decision Making", *IEEE Security and Privacy* 3(1) pp 26–33.

Acquisti A and J Grossklags (2007) "What Can Behavioral Economics Teach Us About Privacy?", In Acquisti A., Vimercati S.C., Gritzalis S., Lambrinouidakis C.(eds), *Digital Privacy: Theory, Technologies and Practices*, Auerbach Publications (Taylor and Francis Group) pp 363-377.

Acquisti A, John L and G Loewenstein (2009) "What is privacy worth?", Technical report, Heinz College, Carnegie Mellon University.

Agre P and C Harbs (1994) "Social Choice about Privacy: Intelligent Vehicle-highway Systems in the United States", *Information Technology & People* 7 (4) pp 63 – 90.

Ajzen I (1991) "The theory of planned behaviour" *Organizational behavior and human decision processes* 50(2) pp 179-211.

Ajzen I (2002) "Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior" *Journal of Applied Social Psychology* 32 pp 665-683.

Aldenderfer M and R Blashfield (1984) "Cluster analysis: Quantitative applications in the social sciences", Beverly Hills: Sage Publication.

Al-Hujraat 49:11-12 (Yusufali).

Alpert S (1995) "Privacy and Intelligent Highways: Finding the Right of Way", *Santa Clara Computer and High Technology Law Journal* 11 pp 97.

Ananthanarayanan G, Haridasan M., Mohamed I, Terry D and C A Thekkath (2009) “Startrack: a framework for enabling track-based applications.”, ACM MobiSys.

An-Noor 24:27-28 (Yusufali).

ANPR Tutorial (2012) “The Automatic Number Plate Recognition Tutorial”, [online] [Accessed 07th February 2012] Available from <http://www.anpr-tutorial.com/>

Arbour-Nicitopoulos K, Faulkner G, Buliung R, Lay J and M Stone (2012) “The school run: Exploring carpooling as an intervention option in the Greater Toronto and Hamilton Area (GTHA), Canada”, *Transport Policy* 21 pp 134–140.

Axon S, Speake, J and K Crawford (2012) “At the next junction, turn left: attitudes towards Sat Nav use”, *Area* 44 (2) pp 170-177.

Banisar D and S Davies (1999) “Privacy and human rights: An international survey of privacy laws and practice. Global Internet Liberty Campaign”, [online] [Accessed 8<sup>th</sup> November 2011] Available from <http://www.gilc.org/privacy/survey/>.

BBC (2003) “Smart cards track commuters”, [online] [Accessed 6th July 2014] Available from <http://news.bbc.co.uk/1/hi/technology/3121652.stm>

BBC (2004) “Race watchdog warns on ID cards”, [online] [Accessed 6th July 2014] Available from [http://news.bbc.co.uk/1/hi/uk\\_politics/3809373.stm](http://news.bbc.co.uk/1/hi/uk_politics/3809373.stm)

BBC (2009) “Greece puts brakes on Street View”, [online] [Accessed 10th July 2013] Available from <http://news.bbc.co.uk/1/hi/technology/8045517.stm>

Beaney W (1966) “The Right to Privacy and American Law”, *Law and Contemporary Problems* 31 pp 253- 255.

Bellman S, Johnson E, Kobrin S, and G Lohse (2004) “International Differences in Information privacy concerns: A global survey of consumers”, *The Information Society* 20 pp 313–324.

Bennett C, Raab C and P Regan (2003) "Patterns of individual identification within intelligent transportation systems", *Surveillance as social sorting: privacy, risk, and digital discrimination* pp 153.

Bentham J; edited and introduced by M Bozovic (1995) "The Panopticon Writings", Verso, London.

Berendt B, Günther O and S Spiekermann (2004) "Privacy in E-Commerce: Stated Preferences vs Actual Behaviour", Communications of the ACM.

BeVier L (1995) "Information about Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection", William. & Mary Bill of Rights Journal 4 (2) pp 455-508.

Bhattacharjee A (2002) "Individual Trust in online firms: Scale and development and initial test", Journal of Management Information Systems 19 pp 211-241.

Borins S (1988) "Electronic Road Pricing: An Idea Whose Time May Never Come", Transportation Research Part A: General 22 (1) pp 37-44.

Bradshaw R and S Atkins (1996) "The use of public transport for school journeys in London", Proceedings of Seminar F: Public Transport Planning and Operations, 2-6 September 1996.

Brenton M (1964) "The Privacy Invaders", New York: Coward McCann.

Brereton M, Roe P, Foth M, Bunker J and L Buys (2009) "Designing participation in agile ridesharing with mobile social software", Proceedings of the 21st Annual Conference of the Australian Computer-Human Interaction Special Interest Group: Design: Open 24/7 pp 257-260.

Brown P (1995) "The electronic post-it note: a metaphor for mobile computing applications", IEEE Colloquium on Mobile Computing and its Applications.

Bughin, J (2011) "Digital user segmentation and privacy concerns", Journal of Direct, Data and Digital Marketing Practice 13(2) pp 156-165.

Buhrman J (2007) "Riding with Little Brother: Striking a Better Balance between the Benefits of Automobile Event Data Recorders and their Drawbacks", Cornell Journal of Law & Public Policy 17 pp 201-221.

Bundesverfassungsgericht (2008) "Entscheidungen - Leitsätze - zum Urteil des Ersten Senats vom 11. März 2008", [online] [Accessed 07th February 2012] Available from [http://www.bverfg.de/entscheidungen/rs20080311\\_1bvr207405.html](http://www.bverfg.de/entscheidungen/rs20080311_1bvr207405.html)

- Cairns S, Sloman L, Newson C, Anable J, Kirkbride A and P Goodwin (2004) “Smarter Choices – Changing the Way We Travel Final report of the research project: The influence of soft factor interventions on travel demand”, Department for Transport, London.
- Chan N and S Shaheen (2011) “Ridesharing in North America: Past, Present and Future”, *Transport Reviews* 32 (1) pp 93-112.
- Chen C-M, Shallcross D, Shih Y-C, Wu Y-C, Kuo S-P, Hsu Y-Y, Holderby Y and W Chou (2011) “Smart Ride Share with Flexible Route Matching”, *IEEE Advanced Communication Technology (ICACT): 13th International Conference on Advanced Communication Technology* pp 1506-1510.
- Chartered Institute of Transport (1990) “Paying for Progress. A Report on Congestion and Road Use Charges”, The Chartered Institute of Transport.
- Chartered Institute of Transport (1992) “Paying for Progress. A Report on Congestion and Road Use Charges, Supplementary Report”, The Chartered Institute of Transport.
- Chatterjee A, Wegmann F and M McAdams (1983) "Non-commitment bias in public opinion on transit usage", *Transportation* 11(4) pp 347-360.
- Cohen S (2003) “Maximum Difference Scaling: Improved Measures of Importance and Preference for Segmentation”, *Sawtooth Software Conference Proceedings*, pp. 61-74.
- Cooperative Vehicle-Infrastructure Systems (CVIS) (2007) “CVISproject.org Results of CVIS end-user’s survey”, [online] [Accessed 10th November 2010] Available from [http://www.cvisproject.org/en/public\\_documents/end\\_user\\_survey/](http://www.cvisproject.org/en/public_documents/end_user_survey/)
- Cooperative Vehicle-Infrastructure Systems (CVIS) (2012) “CVISproject.org About Cooperative Systems - Introduction”, [online] [Accessed 13th January 2012] Available from [http://www.cvisproject.org/en/about\\_cooperative\\_systems/introduction/](http://www.cvisproject.org/en/about_cooperative_systems/introduction/)
- COOPERS (No Date) “Co-operative Systems for Intelligent Road Safety”, [online] [Accessed 10th July 2013] Available from <http://www.coopers-ip.eu/>
- Corey S (1937) “Professional attitudes and actual behaviour”, *Journal of Educational Psychology* 28(1) pp 271–280.

- Council of Europe (1950) “Convention for the Protection of Human Rights and Fundamental Freedoms”, [online] [Accessed 13th January 2012] Available from <http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm>
- Couture M and T Dooley (1981) “Analyzing traveler attitudes to resolve intended and actual use of a new transit service”, *Transportation Research Record* 794.
- Creswell J (2009) “Research Design Qualitative, Quantitative and Mixed Methods Approaches, 2nd Ed”, Sage Publications.
- Cruickshanks S and B Waterson (2011) “Are Privacy Fears Associated with Intelligent Transport Systems Justified?”, 43rd Annual UTSG Conference, Milton Keynes.
- Cruickshanks and B Waterson (2012) “Privacy Decision Making in the Travel Panopticon”, Amsterdam Privacy Conference 2012, Netherlands.
- Cruickshanks and B Waterson (2012) “Will Privacy Concerns Associated with Future Transport Systems Restrict the Publics Freedom of Movement?”, *Procedia-Social and Behavioral Sciences* 48 pp 941-950.
- Culnan M and P Armstrong (1999) “Information Privacy Concerns, Procedural Fairness, and Impersonal Trust”, *Organ, Sci* 10(1) pp 104-115.
- Culnan M and J Bies (2003) “Consumer privacy: Balancing economic and justice considerations”, *Journal of Social Issues* 59(2) pp 323–342.
- Cvrcek D, Kumpost M, Matyas V and G Danezis (2006) “A Study on the Value of Location Privacy”, *Proceedings of Workshop on Privacy in the Electronic Society (WPES '06)* pp 109-118.
- Daly E (2010) “Personal Autonomy in the Travel Panopticon”, *Ethics and Information Technology* 12(2) pp 97-108.
- Davies N, Lau M, Speed C, Cherrett T, Dickinson J and S Norgate (2012) “Sixth Sense Transport : Challenges in Supporting Flexible Time Travel”, *Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications (HotMobile '12)* pp 8.

- Deakin E, Trapenberg F and A Skabardonis (2009) "Intelligent Transport Systems Linking Technology and Transport to Help Steer the Future", *Access* 34(Spring) pp 29-34.
- De Fabritiis C, Ragona R and G Valenti.(2008) "Traffic estimation and prediction based on real time floating car data", 11th International IEEE Conference on Intelligent Transportation Systems pp 197–203.
- Department for Transport (2011) "National Travel Survey 2010: Statistical Release", Department for Transport, London.
- Dillman D (2007) "Mail and Internet Surveys: The Tailored Design Method", New York: Wiley.
- Dinev T and P Hart (2006) "An Extended Privacy Calculus Model for E-Commerce Transactions", *Information Systems Research* 17(1) pp 61-80.
- Dötzer F (2005) "Privacy Issues in Vehicular Ad Hoc Networks", *Privacy Enhancing Technologies* pp 197-209.
- Dudek C (2004) "Changeable message sign operation and messaging handbook", Federal Highway Administration, Operations Office of Travel Management.
- Dunn (2012) "Oyster Card accounts regularly accessed by police, TfL admits", [online] [Accessed 6<sup>th</sup> July 2014] Available from <http://www.computerworlduk.com/news/public-sector/3336636/oyster-card-accounts-regularly-accessed-by-police-tfl-admits/>
- Dwyer C, Hiltz S and K Passerini (2007) "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace", *AMCIS 2007 Proceedings* 339.
- Efroymson M A (1960) "Multiple regression analysis", *Mathematical methods for digital computers* 1 pp 191-203.
- Environmental Protection Agency (2003) "Travel and environmental implications of school siting", Washington, DC: US Environmental Protection Agency.
- EURO NCAP (No Date) "Euro NCAP – For Safer Cars Crash Test Safety Ratings", [online] [Accessed 21st November 2013] Available from <http://www.euroncap.com/home.aspx>

European Commission (2012) “European Commission – Research and Innovation – Framework Program 7”, [online] [Accessed 07th July 2013] Available from [http://ec.europa.eu/research/fp7/index\\_en.cfm](http://ec.europa.eu/research/fp7/index_en.cfm)

European Union (1995) “Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data”, [online] [Accessed 10th July 2013] Available from <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>

European Union (1997) “Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (Directive)”, [online] [Accessed 10th July 2013] Available from <http://www.ipc.on.ca/English/Resources/Reports-And-Submissions/Reports-and-Submissions-Summary/?id=384>

European Union (2010) “Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport”, [online] [Accessed 10th July 2013] Available from <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:207:0001:0013:EN:PDF>

Everitt B S, Landau S and M Leese (2001) “Cluster Analysis”, Arnold A member of the Hodder Headline Group, London.

EVITA (No Date) “E-safety vehicle intrusion protected applications”, [online] [Accessed 10th July 2013] Available from <http://www.evita-project.org/>

Ewing R, Schroerer W and W Greene (2004) “Analysis of Factors Affecting Mode Choice”, Transportation Research Record: Journal of the Transportation Research Board, No 1895 pp 55-63.

Flaherty D (1989) “Protecting Privacy in Surveillance Societies: Flaherty, David H. "Protecting privacy in surveillance societies: the Federal Republic of Germany, Sweden, France, Canada, and the United States", University of North Carolina Press.

Finkenzeller K (2010) “RFID handbook: fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication”, Wiley.

- Friedrich M, Jehlicka P and J Schlaich (2008) “Automatic number plate recognition for the observance of travel behaviour”, 8th International Conference on Survey Methods in Transport: Harmonisation and Data Comparability pp 1-17.
- Foucault M (1979) “Discipline and punish: The Birth of the Prison”, A Sheridan, Translation, Vintage Books, New York.
- Fox S, Rainie L, Horrigan J, Lenhart A, Spooner T and C Carter (2000) “Trust and privacy online: Why Americans want to Write the Rules”, Pew Internet and American Life Project.
- Gill M and A Spriggs (2005) “Assessing the Impact of CCTV”, London: Home Office Research, Development and Statistics Directorate 43 pp 60–61.
- Gillmor D (1993) “On the Road to Nosiness?: The Same Gear That Would Smooth out Traffic Jams Could Be Used to Snoop on You”, Detroit Free Press, 18 October, p. A1.
- Glancy D (1995) “Privacy and Intelligent Transportation Technology”, Santa Clara Computer and High Technology Law Journal 11 pp 151-206.
- Glancy D (2004) “Privacy on the Open Road”, Ohio Northern University Law Review 30 pp 295-378.
- Google (2012) “Annual Report 2011 - Filed Jan 26 2012”, [online] [Accessed 25th February 2013] Available from [http://investor.google.com/pdf/2011\\_google\\_annual\\_report.pdf](http://investor.google.com/pdf/2011_google_annual_report.pdf)
- Google Maps (No Date) “Google Maps – Street View”, [online] [Accessed 10th July 2013] Available from <http://maps.google.co.uk/intl/en/help/maps/streetview/>
- GPS Business News (2012) “Mediamobile First to Use Floating Cellular Data from Orange”, [online] [Accessed 10th July 2013] Available from [http://www.gpsbusinessnews.com/Mediamobile-First-to-Use-Floating-Cellular-Data-from-Orange\\_a3428.html](http://www.gpsbusinessnews.com/Mediamobile-First-to-Use-Floating-Cellular-Data-from-Orange_a3428.html)
- Gras M (2002) “The legal regulation of CCTV in Europe”, *Surveillance & Society* 2(2/3) pp 216-230.
- Greenwood P and M Nikulin (1996) “A guide to chi-squared testing”, Wiley-Interscience 280.
- Griffioen, H. (2011) Privacy en vormen van ‘intelligente’ mobiliteit”, Amsterdam University Press [online] [Accessed 10th July 2013] Available from <http://dare.uva.nl/cgi/arno/show.cgi?fid=353338>



Guardian (2003) “Keeping 1984 in the past”, [online] [Accessed 07th February 2012] Available from <http://www.guardian.co.uk/technology/2003/jun/19/newmedia.media>

Guardian (2007) “Worried about being watched? You already are”, [online] [Accessed 07th February 2012] Available from <http://www.guardian.co.uk/technology/2007/feb/15/public.guardianweeklytechnologysection>

Guardian (2008) “MI5 seeks powers to trawl records in new terror hunt”, [online] [Accessed 6th July 2014] Available from <http://www.theguardian.com/uk/2008/mar/16/uksecurity.terrorism>

Home Office (2011) “ID cards no longer valid”, [online] [Accessed 6<sup>th</sup> July 2014] Available from <https://www.gov.uk/government/news/id-cards-no-longer-valid>

Guardian. (2009) “Big Brother is Watching: Surveillance Box to Track Drivers is Backed”, [online] [Accessed 10th November 2010] Available from <http://www.guardian.co.uk/uk/2009/mar/31/surveillance-transport-communication-box>

Guardian. (2011) “Open up the numberplate recognition camera system”, [online] [Accessed 19th March 2013] Available from <http://www.guardian.co.uk/commentisfree/libertycentral/2011/may/17/automatic-numberplate-recognition-cameras-anpr>

Haggerty K and A Gazso (2005) “Seeing beyond the ruins: Surveillance as a response to terrorist threats”, *The Canadian Journal of Sociology* 30(2) pp 169-187.

Hann I-H, Hui K-L, Lee T and I Png (2002) “Online Information Privacy: Measuring the Cost-Benefit Trade-Off”, 23rd International Conference on Information Systems pp 1-10.

Hann I-H, Hui K.-L, Lee T and I Png (2008) “Overcoming online information privacy concerns: An information-processing theory approach”, *Journal of Management Information Systems* 24(2) pp 13–42.

Hau T (1990) “Electronic road pricing: developments in Hong Kong 1983–1989”, *Journal of Transport Economics and Policy* 24 pp 203–214.

Hensher D (2001) “The valuation of commuter travel time savings for car drivers: evaluating alternative model specifications”, *Transportation* 28(2) pp 101-118.

Highways Agency (No Date) “Highways Agency – About Us”, [online] [Accessed 21st November 2013] Available from <http://www.highways.gov.uk/about-us/>

Highways Agency (2012) “About the scheme – M42 Jct 3a – Jct 7 Active Traffic Management”, [online] [Accessed 07th February 2012] Available from <http://webarchive.nationalarchives.gov.uk/+/http://www.highways.gov.uk/roads/projects/4692.aspx>

Hillman M, Adams J and J Whitelegg (1990) “One False Move ...: A Study of Children’s Independent Mobility”, Research Report - Policy Studies Institute, London, 7-7.

Hirshleifer (1980) “Price Theory and Applications, 2nd Edition”, Prentice-Hall, Englewood Cliffs, N.J.

Hixson R (1987) “Privacy in a Public Society: Human Rights in Conflict”, New York: Oxford University Press.

Hofstede G (2001) “Culture's Consequences: comparing values, behaviors, institutions, and organizations across nations, 2nd Edition”, Thousand Oaks, CA: SAGE Publications.

Hofstede G (2005) “Cultures and organizations: software of the mind, 2nd Edition”, New York: McGraw-Hill.

Hui K-L, Teo H-H and T Lee (2007) “The value of privacy assurance: An exploratory field experiment”, *MIS Quarterly* 31(1) pp 19–33.

IBM (1999) “IBM multi-national consumer privacy survey”, [online] [Accessed 10th November 2010] Available from [http://www.ibm.com/services/files/privacy\\_survey\\_oct991.pdf](http://www.ibm.com/services/files/privacy_survey_oct991.pdf)

Independent (2005) “Surveillance UK: why this revolution is only the start”, [online] [Accessed 07<sup>th</sup> February 2012] Available from <http://www.independent.co.uk/news/science/surveillance-uk-why-this-revolution-is-only-the-start-520396.html>

Information Commissioner’s Office (ICO) (2006) “Data Protection Guidance Note: Privacy enhancing technologies (PETs)”, [online] [Accessed 17<sup>th</sup> November 2010] Available from [http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/privacy\\_enhancing\\_technologies.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/privacy_enhancing_technologies.pdf)

Internet Encyclopaedia of Philosophy (IEP) (2004) “Social Contract Theory”, [online] [Accessed 10th November 2010] Available from <http://www.iep.utm.edu/soc-cont/>

Ison S (1996) “Pricing road space: back to the future? The Cambridge experience”, *Transport Reviews* 16 pp 109–126.

Ison S and T Rye (2005) “Implementing Road User Charging: The Lessons Learnt from Hong Kong, Cambridge and Central London, *Transport Reviews*”, *A Transnational Transdisciplinary Journal* 25(4) pp 451-465.

Jakobsson C, Fujii S and T Gärling (2000) “Determinants of Private Car Users’ Acceptance of Road Pricing”, *Transport Policy* 7 pp 153–158.

Jarvenpaa S L and D E Leidner (1998) “Communication and trust in global virtual teams”, *Journal of Computer-Mediated Communication* 3(4).

Johnson R A and D W Wichern (1992) “Applied multivariate statistical analysis (Vol. 4)”, Englewood Cliffs, NJ: Prentice hall.

Jones P and A Hervik (1992) “Restraining car traffic in European cities: An emerging role for road pricing”, *Transportation Research Part A: Policy and Practice* 26(2) pp 133–145.

Kahneman D and A Tversky (1979) “Prospect Theory: An Analysis of Decision Under Risk,” *Econometrica* 47(2) pp 263-292.

Kelley P G, Cesca L, Bresee J and L F Cranor (2010) “Standardizing privacy notices: an online study of the nutrition label approach”, *Proceedings of the SIGCHI Conference on Human factors in Computing Systems* pp 1573-1582.

Kline P (2000) “The handbook of psychological testing (2nd ed.)” London: Routledge pp 13.

Kumaraguru P and L Cranor (2005) “Privacy Indexes: A Survey of Westin’s Studies”, Technical Report CMU-ISRI-5-138, Carnegie Mellon University.

Kunreuther H (1984) “Causes of underinsurance against natural disasters”, *Geneva Papers on Risk and Insurance*.

- LaPiere R (1934) "Attitudes versus actions", *Social Forces* 13 pp 230–237.
- Laufer R and M Wolfe (1977) "Privacy as a Concept and a Social Issue - Multidimensional Developmental Theory", *Journal of Social Issues* 33(3) pp 22-42.
- Leape J (2006) "The London congestion charge", *The Journal of Economic Perspectives* 20(4) pp 157-176.
- Lewin K (1936) "Some social-psychological differences between the United States and Germany", *Character and Personality* 4 pp 265– 293.
- Lewis F L (2004) "Wireless sensor networks", *Smart environments: technologies, protocols, and applications* pp 11-46.
- Li N, Zhang N, Das S and B Thuraisingham (2009) "Privacy preservation in wireless sensor networks: A state-of-the-art survey", *Ad Hoc Networks* 7(8) pp 1501-1514.
- Liu C, Marchewka J, Lu J and C-S Yu (2005) "Beyond concern a privacy-trust-behavioral intention model of electronic commerce", *Information & Management* 42(2) pp 289-304.
- Litman T (2006) "London congestion pricing", *Implications for Other Cities*.
- Lohse G, Bellman S, and E Johnson (2000) "Consumer Buying Behavior on the Internet: Findings from Panel Data", *Journal of Interactive Marketing* 14(1) pp 15–29.
- Lotufo R, Morgan A and A Johnson (1990) "Automatic number-plate recognition", *IEE Colloquium on Image Analysis for Transport Applications* 6 pp 1-6.
- Mackett R (2002) "Increasing car dependency of children: should we be worried?", *Municipal Engineer* 151(1) pp 29- 38.
- Malhotra N and D Birks (2003) "Marketing Research an Applied Approach, 2nd Edition", Prentice Hall, Inc.
- Malhotra N, Kim S and J Agarwal (2004) "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model", *Information Systems Research* 15(4) pp 336-355.

- Manchester Evening News (2010) "Pilots to snub ID card trial", [online] [Accessed 6th July 2014] Available from <http://www.manchestereveningnews.co.uk/news/greater-manchester-news/pilots-to-snub-id-card-trial-910621>
- Mayer R C, Davis J H and F D Schoorman (1995) "An integrative model of organizational trust" *Academy of management review* 20(3) pp 709-734.
- Maynard M and C Taylor (1996) "A comparative analysis of Japanese and U.S. attitudes toward direct marketing", *Journal of Direct Marketing* 10(1) pp34-44.
- McCarthy J (1987) "The Rights of Publicity and Privacy, 2nd edition", Clark Boardman Callaghan.
- McDonald N (2007) "Active transportation to school: trends among US schoolchildren, 1969-2001", *American Journal of Preventive Medicine* 32 (6) pp 509-516.
- McDonald N (2008) "Household interactions and children's school travel: the effect of parental work patterns on walking and biking to school", *Journal of Transport Geography* 16 pp 324-331.
- Mediamobile (2012) "V-Traffic becomes the first service to incorporate Orange's Floating Mobile Data as traffic information source", [online] [Accessed 10th July 2013] Available from <http://www.mediamobile.com/en/media-area/news/60-19012012-v-traffic-premier-service-a-integrer-le-floating-mobile-data-dorange-comme-source-dinformation-traffic.html>
- Meteo France (No Date) "L'info trafic en temps reel avec V-Traffic", [online] [Accessed 10th July 2013] Available from <http://france.meteofrance.com/france/route>
- Metzger M J (2004) "Privacy, trust, and disclosure: Exploring barriers to electronic commerce", *Journal of Computer-Mediated Communication* 9(4).
- Katina M, McNamee A and M Michael (2006) "The emerging ethics of human centric GPS tracking and monitoring", *International Conference on Mobile Business* pp 34-46.
- Milne G R and E M Gordon (1993) "Direct mail privacy-efficiency trade-offs within an implied social contract framework", *Journal of Public Policy and Marketing* 12(2) pp 206-215.
- Moore B (1984) "Privacy: Studies in Social and Cultural History", Random House.

Morris J, Wang F and L Lilja (2001) "School Children's Travel Patterns: A Look Back and A Way Forward", *Transport Engineering in Australia* 7(1&2) pp 15-25.

MSNBC (2007) "E-ZPass records out cheaters in divorce court", [online] [Accessed 07<sup>th</sup> February 2012] Available from [http://www.msnbc.msn.com/id/20216302/ns/technology\\_and\\_science-tech\\_and\\_gadgets/t/e-zpass-records-out-cheaters-divorce-court/#.TzFVF\\_nxg25](http://www.msnbc.msn.com/id/20216302/ns/technology_and_science-tech_and_gadgets/t/e-zpass-records-out-cheaters-divorce-court/#.TzFVF_nxg25)

Murphy R (1996) "Property rights in personal information: An economic defence of privacy", *Georgetown Law Journal* 84 pp 2381–2573.

Nardi P M (2006) "Doing Survey Research: A Guide to Quantitative Methods, 2nd Ed", Pearson Education Inc, USA.

NBC News (2010) "Czech Republic bans Street View", [online] [Accessed 10<sup>th</sup> July 2013] Available from [http://www.nbcnews.com/id/39302384/ns/technology\\_and\\_science/#.UUmZtFeC18E](http://www.nbcnews.com/id/39302384/ns/technology_and_science/#.UUmZtFeC18E)

NEARCTIS (No Date) "NEARCTIS Excellence in co-operative traffic management", [online] [Accessed 11th January 2012] Available from <http://www.nearctis.org>

New York Times (2010) "The Wired Repo Man: He's Not 'As Seen on TV'", [online] [Accessed 07th February 2012] Available from <http://www.nytimes.com/2010/02/28/automobiles/28REPO.html>

Neudorff L, Randall J, Reiss R and R Gordon (2003) "Freeway management and operations handbook", No. FHWA-OP-04-003, Chapter 15

Norris C, McCahill M and D Wood (2002) "The growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space", *Surveillance and Society* 2 (2/3) pp 110–135.

O'Brien M, Jones D, Sloan D and M Rustin (2000) "Children's independent spatial mobility in the urban public realm", *Childhood* 7 (3) pp 257– 277.

O'Donoghue T and M Rabin (2001) "Choice and procrastination", *Quarterly Journal of Economics* 116 pp 121–160.

Oppenheim N (2005) "Questionnaire Design, Interviewing and Attitude Measurement", Continuum, New York.

Orwell G (1949) "Nineteen Eighty-Four", Harmondsworth, Penguin.

OV-chipkaart (No Date) "OV-chipkaart", [online] [Accessed 11th January 2012] Available from <http://www.ov-chipkaart.nl/?taal=en>

Oversee (No Date) "Open vehicular secure platform", [online] [Accessed 11th January 2012] Available from <https://www.oversee-project.com/index.php?id=2>

Ozanne L and D Mollenkopf (1999) "Understanding Consumer Intentions to Carpool: A Test of Alternative Models", Proceedings of the 1999 annual meeting of the Australian & New Zealand Marketing Academy 8081.

Packard V (1964) "The Naked Society", New York, David McCay.

Papageorgiou M, Diakaki C, Dinopoulou V, Kotsialos A and Y Wang (2003) "Review of road traffic control strategies", Proceedings of the IEEE 91(12) pp 2043-2067.

Pee L (2011) "Attenuating Perceived Privacy Risk of Location-Based Mobil Services", European Conference of Information Systems 2011, Helsinki, Finland.

Perrig A, Stankovic J and D Wagner (2004) "Security in wireless sensor networks", Communications of the ACM 47(6) pp 53-57.

Phelps J, Nowak G and E Ferrell (2000) "Privacy Concerns and Consumer Willingness to Provide Personal Information", Journal of Public Policy & Marketing 19(Spring) pp 27-41.

PHYS ORG (2010) "Austria bans Google's street view cars over privacy", [online] [Accessed 11th January 2012] Available from <http://phys.org/news194273855.html>

Politics.co.uk (2008) "Home Office faces new ID cards controversy", [online] [Accessed 6th July 2014] Available from <http://www.politics.co.uk/news/2008/8/7/home-office-faces-new-id-cards-controversy>

Pooley C, Turnbull J and M Adams (2005) "The journey to school in Britain since the 1940s: continuity and change", Area 37 (1) pp 43-53.

Posner R A (1978) "An economic theory of privacy", Regulation May-June pp 19-26.

Posner R A (1981) “The economics of privacy”, *American Economic Review* 71(2) pp 405–409.

Post R (2001) “Three Concepts of Privacy”, *Georgetown Law Journal* 89 pp 2087-2100.

PRECIOSA (No Date) “Privacy Enabled Capability In Co-Operative Systems and Safety Applications”, [online] [Accessed 11th January 2012] Available from <http://www.preciosa-project.org/>

PRESERVE (No Date) “Preparing Secure V2X Communication Systems”, [online] [Accessed 11th January 2012] Available from <http://www.preserve-project.eu/>

Pretty R (1988) “Road pricing: a solution for Hong Kong?”, *Transportation Research Part A* 22 pp 319–327.

Prins C, Broeders D, Griffioen H, Keizer A and E Keymolen (2011) “IGovernment”, Amsterdam University Press p 264

Privacy First (2013) “Privacy First demands privacy-friendly Public Transport chip card”, [online] [Accessed 24th November 2013] Available from <https://www.privacyfirst.eu/focus-areas/public-transport/item/581-privacy-first-demands-privacy-friendly-public-transport-chip-card.html>

Privacy International (2007) “Surveillance Monitor 2007 – International Country Rankings”, [online] [Accessed 24<sup>th</sup> November 2013] Available from <https://www.privacyinternational.org/reports/surveillance-monitor-2007-international-country-rankings>

Privacy International (2011) “Overview of Privacy”, [online] [Accessed 11<sup>th</sup> January 2012] Available from <https://www.privacyinternational.org/article/overview-privacy>.

Privacy International (2011) “Surveillance Monitor 2011: Assessment of surveillance across Europe”, [online] [Accessed 25th June 2014] Available from <https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/ephr.pdf>

PROGRESS Project 2000 (2004) “Pricing Road Use for Greater Responsibility, Efficiency and Sustainability in Cities”, [online] [Accessed 11<sup>th</sup> January 2012] Available from <http://www.progress-project.org/Progress/pdf/D7.2.pdf>



- Rabin M and T O'Donoghue (2000) "The economics of immediate gratification", *Journal of Behavioral Decision Making* 13 pp 233–250.
- Rankin W and J Grube (1980) "A comparison of ranking and rating procedures for value system measurement", *European Journal of Social Psychology* 10(3) pp 233-246.
- Rass S, Fuchs S, Schaffer M and K Kyamakya (2008) "How to protect privacy in floating car data systems", *Proceedings of the fifth ACM international workshop on Vehicular Internetworking* pp 17-22.
- Reiman J (1995) "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy", *Santa Clara Computer & High Technology Law Journal* 11 pp 27.
- Research and Innovation Technology Administration (RITA) (2009) "Intelligent Transport Systems Applications Overview", [online] [Accessed 10th November 2010] Available from <http://www.itsoverview.its.dot.gov/>
- Ritchie S, Park S, Oh C, Jeng S and A Tok,(2005) "Anonymous vehicle tracking for real-time freeway and arterial street performance measurement", *California PATH Research Report, UCB-ITS-PRR-2005-9*.
- Roloff M E (1981) "Interpersonal communication: The social exchange approach" Beverly Hills, CA: Sage Publications.
- Rose J, Rehse O and B Röber (2012) "The Value of Our Digital Identity", Boston Consulting Group Report Commissioned by Liberty Global.
- Rosen J (2000) "The Unwanted Gaze: The destruction of privacy in American", Random House Digital Inc.
- SAFESPOT (No Date) "SAFESPOT Integrated Project", [online] [Accessed 11<sup>th</sup> January 2012] Available from <http://www.safespot-eu.org/>
- SatNav Forensics (No Date) "Satellite Navigation Forensics", [online] [Accessed 11<sup>th</sup> January 2012] Available from <http://www.satnavforensics.com/index.php>

Schäfer R, Thiessenhusen K and Wagner P (2002) “A traffic information system by means of real-time floating-car data”, ITS world congress Vol. 2.

Seraj S, Sidharthan R, Chandra B, Pendyala R and K Goulias (2012) “Parental Attitudes Towards Children Walking and Bicycling to School: A Multivariate Ordered Response Analysis”, Transportation Research Record: Journal of the Transportation Research Board 2323(1) pp 46-55.

Sevecom (No Date) “Secure Vehicle Communication”, [online] [Accessed 11<sup>th</sup> January 2012] Available from <http://www.sevecom.org/>

Simon H (1982) “Models of bounded rationality”, The MIT Press, Cambridge, MA.

Smith H, Milberg S and S Burke (1996) “Information privacy: Measuring individuals’ concerns about organizational practices”, MIS Quart. 20(2) pp 167-196.

Slovic P (2000) “What does it mean to know a cumulative risk? Adolescents’ perceptions of short-term and long-term consequences of smoking”, Journal of Behavioral Decision Making 13 pp 259–266.

Solove D (2002) “Conceptualizing Privacy”, California Law Review 90 pp 1087-1156.

Solove D (2006) “A Taxonomy of Privacy”, University of Pennsylvania Law Review 154(3) pp 477-564.

Spiekermann S, Grossklags J and B Berendt (2001) “Privacy in 2<sup>nd</sup> Generation E-Commerce: Privacy Preferences versus actual Behavior”, World Wide Web and Internet and Web Information Systems pp 38-47.

Stigler G J (1980) “An introduction to privacy in economics and politics”, Journal of Legal Studies 9 pp 623–644.

Sullivan S (2011) “Case Study in Real-time Ridesharing: SR 520 Carpooling Project, Seattle, WA”, ITSA.

Tavakol M and R Dennick (2011) “Making sense of Cronbach's alpha”, International journal of medical education 2 pp 53-55.

Techspan (2013) "Route Guidance and Information ... Informed Solutions", [online] [Accessed 11<sup>th</sup> January 2012] Available from <http://www.techspan.co.uk/index.php?page=vms-example-3>

Telegraph (2013) "Google Street View funny images", [online] [Accessed 11<sup>th</sup> January 2012] Available from <http://www.telegraph.co.uk/technology/google/5017329/Google-Street-View-funny-images.html?image=1>

Telegraph (2013) "Nigel Farage: I won't buy an Oyster card, I don't want them spying on me", [online] [Accessed 6th July 2014] Available from <http://www.telegraph.co.uk/news/politics/ukip/10155908/Nigel-Farage-I-wont-buy-an-Oyster-card-I-dont-want-them-spying-on-me.html>

Thaler R (1980) "Toward A Positive Theory of Consumer Choice", *Journal of Economic Behavior & Organization* 1(1) pp 39-60.

The Privacy Bulletin (1990) "Tracking people through their travels", Special Issue, August, Vol. 6 No. 2, Sydney Australia.

The Sun (2009) "Google Cheat View", [online] [Accessed 11<sup>th</sup> January 2012] Available from <http://www.thesun.co.uk/sol/homepage/news/2350771/Cheating-husband-caught-on-Google-Street-View.html>

The World Road Association (PIARC) (2004) "ITS Handbook: 2<sup>nd</sup> Edition edited by John C Miles and Kan Chen", Andrew Barriball.

Thomson J (1975) "The Right to Privacy", *Philosophy and Public Affairs* 4 (4) pp 295-314.

Ting-Toomey, S (1991) "Intimacy expressions in three cultures: France, Japan, and the United States.", *International Journal of Intercultural Relations* 15(1) pp29-46.

Toulminet G, Boussuge J and C Laugeau (2008) "Comparative synthesis of the 3 main European projects dealing with Cooperative Systems (CVIS, SAFESPOT and COOPERS) and description of COOPERS Demonstration Site 4", 11th International IEEE Conference Intelligent Transportation Systems pp 809-814.

- Traffic Radio (2011) “Traffic Radio Digital and Online – Frequently Asked Questions”, [online] [Accessed 11<sup>th</sup> January 2012] Available from <http://webarchive.nationalarchives.gov.uk/20110613092000/trafficradio.org.uk/faq/>
- Tranter P (2008) “How to save time and money: Using the walking school bus to increase your effective speed”, *World Transport Policy & Practice* 14 (1) pp 56-64.
- Tuan Seik F (2000) “An advanced demand management instrument in urban transport: electronic road pricing in Singapore”, *Cities* 17(1) pp 33-45.
- Turksma S (2000) “The various uses of floating car data”, *Tenth International Conference on Road Transport Information and Control* 472 pp 51-55.
- United Kingdom (1998) “Human Rights Act”, Article 8.
- USA Today (2007) “Google’s street-level maps raising privacy concerns”, [online] [Accessed 11<sup>th</sup> January 2012] Available from [http://usatoday30.usatoday.com/tech/news/internetprivacy/2007-06-01-google-maps-privacy\\_N.htm](http://usatoday30.usatoday.com/tech/news/internetprivacy/2007-06-01-google-maps-privacy_N.htm)
- US DOT (2006) “Traffic Detector Handbook”, [online] [Accessed 11<sup>th</sup> January 2012] Available from <http://www.fhwa.dot.gov/publications/research/operations/its/06108/02.cfm>
- United Nations (1948) “Universal Declaration on Human Rights”, Article 12.
- U.S. Department of Transportation (DOT) (2003) “Manual on Uniform Traffic Control Devices (MUTCD)”, [online] [Accessed 07<sup>th</sup> February 2012] Available from <http://mutcd.fhwa.dot.gov/HTM/2003r1/part4/part4f.htm>
- Vahidi A and A Eskandarian (2003) “Research advances in intelligent collision avoidance and adaptive cruise control”, *IEEE Transactions on Intelligent Transportation Systems* 4(3) pp 143-153.
- Van Eerde W and H Thierry (1996) “Vroom’s expectancy models and work-related criteria: A meta-analysis”, *Journal of Applied Psychology* 81 pp 575–586.
- Vance R and A Colella (1990) “Effects of two types of feedback on goal acceptance and personal goals”, *Journal of Applied Psychology* 75 pp 68-76.

- Varian H, Wallenberg F and G Woroch (2005) "The demographics of the do-not-call list", *IEEE Security and Privacy* 3(1) pp 34-39.
- VATS (1999) "The 1999 Victoria Travel and Activity Survey", Transport Research Centre, RMIT University, Melbourne.
- Von Sanden N D (2004) "Interviewer Effects in Household Surveys: Estimation and Design", PhD Thesis, University of Wollongong.
- Vroom V H (1964) "Work and motivation", New York, Wiley.
- Wallis Consulting Group (2007) "Community Attitudes to Privacy 2007", Office of the Privacy Commissioner, Australia.
- Wardman M (1988) "A Comparison of Revealed Preference and Stated Preference Models of Travel Behavior", *Journal of Transport Economics and Policy* January pp 71-91.
- Warren A and A Charlesworth (2012) "Privacy Impact Assessment in the UK", *Privacy Impact Assessment* pp. 205-224.
- Warren S and L Brandeis (1890) "The right to privacy", *Harvard Law Review* 4 pp 193-220.
- Weiland R and L Purser (2000) "Intelligent Transportation Systems". *Transportation in the New Millennium*.
- Weinstein N D (1989) "Optimistic biases about personal risks", *Science* 24 pp 1232–1233.
- Westin A F (1967) "Privacy and Freedom", Atheneum, New York.
- Westin A F (2003) "Social and Political Dimensions of Privacy", *Journal of Social Issues* 59(2) pp 1-37.
- Westin A F and the Staff of the Centre for Social & Legal Research (2003) "Bibliography of Surveys of the U.S. Public 1970-2003", Centre for Social & Legal Research.
- Whitman J (2003) "Two Western Cultures of Privacy: Dignity versus Liberty", *The Yale Law*

Journal 113 pp 1151-1221.

Winters N (2004) "Personal privacy and popular ubiquitous technology", Proceedings of Ubiconf 2004, April 19th, Gresham College, London.

Wood D (2002) "A Report on the Surveillance Society; 2<sup>nd</sup> Edition", Surveillance Studies Network, UK.

Wright T (1995) "Eyes on the road: Intelligent Transportation Systems and your Privacy", Information and Privacy Commissioner, Ontario.

Xu H, Teo H, Tan B and R Agarwal (2009) "The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services", Journal of Management Information Systems 26(3) pp 137-176.

Xu H, Parks R, Chu, C-H and X Zhang (2010) "Information Disclosure and Online Social Networks: From the Case of Facebook News Feed Controversy to a Theoretical Understanding", AMCIS 2010 Proceedings Paper 503.

Yang Y and E Markowitz (2012) "Integrating Parental Attitudes in Research on Children's Active School Commuting: Evidence from a Community School Travel Survey", 91st Annual Meeting of the Transportation Research Board.

Zhou T (2011) "The impact of privacy concern on user adoption of location-based services", Industrial Management & Data Systems 111(2) pp 212-226.

**Appendix A –Pilot Questionnaire**

**PART D - About You & Your Choices**

**D1. Your Choices and Experiences**

A) Do you use loyalty cards (Nectar Card, Tesco Club Card, Air Miles Card etc.)  YES  NO

B) Do you use a Hotmail/Gmail internet email account?  YES  NO

C) Do you regularly use internet search engines (Google, Yahoo etc.)?  YES  NO

D) Is your telephone number listed as being ex-directory?  YES  NO

E) Do you read a companies privacy policy before you use their service?  YES  NO

F) Have you ever checked the data, credit checking agencies (Experian etc) hold on you?  YES  NO

G) Do you fully understand what your legal rights with regards to privacy are?  YES  NO

H) Have you ever experienced an invasion of your privacy? If so please can you describe it below

YES  NO

\_\_\_\_\_

\_\_\_\_\_

I) Is there anything else that has influenced yours views on privacy?

\_\_\_\_\_

\_\_\_\_\_

**D2. Privacy Overview**

A) Are you concerned about threats to your personal privacy today?  YES  NO

B) Do you strongly agree that business organisations seek excessive amounts of personal information from consumers?  YES  NO

C) Do you strongly agree that federal governments invade citizens privacy?  YES  NO

D) Do you believe that you have lost all control over circulation of your personal data?  YES  NO

**D3. Information about**

These final questions are completely optional but would greatly assist our research. Please also remember that all of the answers you give us will be kept with complete confidentiality and analysis of your results will be done anonymously.

A) What is your employment status? Student  Employed  Retired  Unemployed  Other

B) What is your annual household income? £0-20K  £20-40K  £40-60K  £60-80K  £80K+

C) What is your ethnicity? (e.g. White British/Indian/Black Caribbean/Chinesse etc)

D) What sex are you? MALE  FEMALE  E) How old are you? \_\_\_\_\_

F) Do you have children? YES  NO  G) What is your martial status? \_\_\_\_\_

H) What is your highest level of education? None  GCSE/O Level  A Level  Undergraduate  Postgraduate


**D4. Further Information**

A) Would you like to be considered for a further interview for which you will be rewarded with a £20 gift voucher from either amazon or M&S? If so please can you provide us with either a contact number or email address below.

\_\_\_\_\_

**Thank you very much for your time please now return this survey in the freepost envelope provided**

Data Protection Act 1998. The information you provide will only be used to increase the understanding of people's views on privacy. All of your answers will be processed anonymously and with complete confidentiality.



**UNIVERSITY OF Southampton**  
School of Civil Engineering and the Environment

WEB ACCESS CODE: GB-0123

24th May 2010

Mr J Smith  
20 Random Street  
Lancaster  
Lancashire  
BA1 2DF

Dear Mr Smith

We are writing to ask for your participation in the International Privacy Survey. This is an important survey of citizens of the European Union and will help ensure that future technologies and policies will meet your privacy demands.

The University of Southampton has chosen you for this survey as part of a random sample of people selected from the edited electoral register. Your response is invaluable to the success of the investigation, as the more responses we gain, the more likely we will be to satisfy your privacy needs.

Please complete the enclosed survey and return it using the pre-paid envelope, also enclosed. Alternatively, you can complete the survey online at [www.privacy.soton.ac.uk](http://www.privacy.soton.ac.uk), by entering the access code at the top of this page.

Completing the questionnaire will take a maximum of 15 minutes. Please do take the time to respond; responding will seriously improve the accuracy of our results and will mean that your privacy preferences being represented in future technologies and policies.

For more information on our research and for answers to frequently asked questions, please visit our website at [www.internationalprivacysurvey.com](http://www.internationalprivacysurvey.com).

Thank you for your help. We look forward to hearing from you.

Yours sincerely,

Scott Cruickshanks  
School of Civil Engineering and the Environment  
University of Southampton  
Highfield  
Southampton  
SO17 1BJ



### PART A - Rewards, Consequences and Risks

**A1. Rewards**

For each of the following scenarios, please select which improvement you feel is the **BEST** and **WORST**. For example, from the following options - £1 million, No Reward, £100 and Status - I may reply: '£1 million is my BEST improvement and No Reward is my WORST improvement'.

Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5
£100	Spare Time	Enjoyment	Family Safety	Family Safety
Enjoyment	Status	No Reward	Status	£100
Reduced CO2	Family Safety	£100	Own Safety	Spare Time
Own Safety	No Reward	Spare Time	Reduced CO2	Status

Scenario 6	Scenario 7	Scenario 8	Scenario 9	Scenario 10
Own Safety	Spare Time	Status	No Reward	£100
Reduced CO2	No Reward	Enjoyment	Reduced CO2	No Reward
Family Safety	Enjoyment	Spare Time	Status	Own Safety
Enjoyment	Reduced CO2	Own Safety	£100	Family Safety

**A2. Consequences**

For each of the following scenarios, please select your **BEST** and **WORST** consequences

Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5
Death	Prison	Nothing	Inconvenience	Prison
£100 Fine	Bankruptcy	Death	Broken Leg	Bankruptcy
Inconvenience	Broken Leg	Prison	Bankruptcy	Death
Humiliation	Nothing	£100 Fine	Humiliation	Broken Leg

Scenario 6	Scenario 7	Scenario 8	Scenario 9	Scenario 10
£100 Fine	Inconvenience	Humiliation	Bankruptcy	Death
Humiliation	£100 Fine	Bankruptcy	Inconvenience	Nothing
Inconvenience	Broken Leg	Prison	Nothing	Broken Leg
Nothing	Prison	£100 Fine	Death	Humiliation

**A3. Risks**

How **SAFE** do you think your personal information is in the hands of the following groups?

5 - Very Safe, 4 - Safe, 3 - Average, 2 - Unsafe, 1 - Very Unsafe

Family		Journalist	
The Government		Stranger	
Medical Professional		Close Friend	
Criminal		Private Company	
Legal Professional		Work Colleague	

How **SAFE** do you think the following methods for exchanging private information are?

5 - Very Safe, 4 - Safe, 3 - Average, 2 - Unsafe, 1 - Very Unsafe

Correspondence via postal mail		Face to face conversation on busy train	
Conversation on mobile phone		Information sent by email	
Information sent by text message		Face to face conversation in a private place	
Using social networking sites		Conversation on landline telephone	

### PART B - Trade-offs

A) Would you give the details of everything that you purchase to a private company by postal mail in return for a financial gain?  YES  NO

B) Would you opt in to letting the government listen in on all of your private phone calls in return for an increase in the safety of you and your family?  YES  NO

C) Would you send your credit card details via email to book a room at a hotel to receive a discount?  YES  NO

D) Would you tell a legal professional working in a prison the location of a family member via his work landline telephone in return for a large amount of money?  YES  NO

E) Would you tell a journalist in a private meeting your embarrassing secrets in return for a rise in your social standing?  YES  NO

F) Would you tell the government by text message exactly where you plan to travel if it reduced your travel time?  YES  NO

G) Would you tell a stranger your travel plans via a social networking site if it improved the safety of you and your family during the journey?  YES  NO

H) Would you tell a work colleague your address on a busy train in order to reduce your carbon emissions?  YES  NO

I) Would you do something with a high risk of personal injury in return for enjoyment (eg. driving fast, sky diving, contact sports etc)?  YES  NO

J) Would you tell your dangerous secrets to a doctor via a mobile phone if you thought it would improve your health?  YES  NO

K) Would you tell a stranger your travel plans anonymously via a social networking site if it improved the safety of you and your family during the journey?  YES  NO

L) If your whereabouts was made public at all times would you stop travelling to certain places?  YES  NO

### PART C - Improvements

Which of the following improvements would you like implemented please tick a **MAXIMUM OF THREE** boxes

- Organisations making you more aware of exactly what your data will be used for and how it will be protected
- Organisations making it easier for you to change errors in the data they hold on you
- Better security to stop improper /external access to your stored personal data
- A better legal framework that punishes organisations that use your data for something that you have not authorised
- Organisations minimising the volume of personal data they collect
- Organisations giving you more control over exactly what your personal data is used for



**Appendix B – English Version of European Survey**

**PART D - About You & Your Choices**

**D1. Your Choices and Experiences**

A) Do you use loyalty cards (Nectar Card, Tesco Club Card, Air Miles Card etc.)  YES  NO

B) Have you ever purchased anything with a credit card on the internet?  YES  NO

C) Have you been through / Would you be willing to go through airport security?  YES  NO

D) Is your telephone number listed as being ex-directory?  YES  NO

E) Do you read a companies privacy policy before you use their service?  YES  NO

F) Have you ever checked the data, credit checking agencies (Experian etc.) hold on you?  YES  NO

G) Do you fully understand what your legal rights with regards to privacy are?  YES  NO

H) Have you ever experienced an invasion of your privacy? If so please can you describe it below  YES  NO

\_\_\_\_\_

\_\_\_\_\_

I) Is there anything else that has influenced yours views on privacy?

\_\_\_\_\_

\_\_\_\_\_

**D2. Information about**

These final questions are completely optional but would greatly assist our research. Please also remember that all of the answers you give us will be kept with complete confidentiality and analysis of your results will be done anonymously.

A) What is your employment status? Student  Employed  Retired  Unemployed  Other

B) What is your annual household income? £0-20K  £20-40K  £40-60K  £60-80K  £80K+

C) Do you hold a valid drivers license? YES  NO

D) What is your gender? MALE  FEMALE

E) Do you have any children? YES  NO

F) What is your highest level of education? None  GCSE/O Level  A Level  Undergraduate  Postgraduate

G) What is your ethnicity? (e.g. White British / Indian/ Black Caribbean / Chinese etc.) \_\_\_\_\_

H) How old are you? \_\_\_\_\_

G) What is your martial status? \_\_\_\_\_


**D3. Further Information**

A) Would you like to be considered for a further interview for which you will be rewarded with a £20 gift voucher from either amazon or M&S? If so please can you provide me with either a contact number of email address below.

\_\_\_\_\_

**Thank you very much for your time please now return  
this survey in the freepost envelope provided**

Data Protection Act 1998. The information you provide will only be used to increase the understanding of people's views on privacy. All of your answers will be processed anonymously and with complete confidentiality.



**UNIVERSITY OF  
Southampton**  
School of Civil Engineering  
and the Environment

«F2» «F3»  
«F4»  
«F5»  
«F6»  
«F7»  
«F8»

WEB ACCESS CODE: «F1»

14th March 2011

Dear «F2» «F3»

I am writing to ask for your assistance with some research that will form a major element of my postgraduate studies. My research is being funded by the EU Commission as part of the NEARCTIS project and will help ensure that future technologies and policies will meet your privacy demands. More information about my research is available at [www.internationalprivacysurvey.com](http://www.internationalprivacysurvey.com).

You have been chosen for this survey as part of a random sample of people that will represent the diverse views held across the European Union. Therefore your response is invaluable to the success of the investigation, as the more responses I gain, the more accurate the conclusions will be.

Please complete the enclosed survey and return it using the pre-paid envelope, also enclosed. Alternatively, you can complete the survey online at [www.internationalprivacysurvey.com](http://www.internationalprivacysurvey.com), by entering the access code at the top of this page.

Completing the questionnaire will take a maximum of 15 minutes. Please do take the time to respond.

Thank you for your help. I look forward to hearing from you.

Yours sincerely,

Scott Cruickshanks  
Postgraduate Student  
School of Civil Engineering and the Environment  
University of Southampton  
Highfield  
Southampton  
SO17 1BJ

**PART A - Rewards, Trust and Privacy**

**A1. Factors**  
When deciding on a mode of travel how **IMPORTANT** are the following factors?  
Please give a **SCORE OUT OF 10** where a **10 = Extremely Important** and **0 = Not Important At All**

Travel Time	<input type="checkbox"/>	Impact on the Environment	<input type="checkbox"/>
The Safety of You and Your Family	<input type="checkbox"/>	Enjoyment	<input type="checkbox"/>
Cost	<input type="checkbox"/>	Impact on your Image (What others will think)	<input type="checkbox"/>
Convenience	<input type="checkbox"/>	Reliability	<input type="checkbox"/>

**A2. Types of Information**  
How **PROTECTIVE** are you of the following types of information?  
Please give a **SCORE OUT OF 10** where a **10 = Extremely Protective** and **0 = Not Protective At All**

The Weather Conditions where you are	<input type="checkbox"/>	Your Driving Behaviour (Speed, Distance etc)	<input type="checkbox"/>
Your Current / Past Locations	<input type="checkbox"/>	Your Musical Preferences	<input type="checkbox"/>
Your Bank Details	<input type="checkbox"/>	Your Ethnicity	<input type="checkbox"/>
Your Income Level	<input type="checkbox"/>	Your Purchase History	<input type="checkbox"/>
Your Embarrassing Secrets	<input type="checkbox"/>	Your Medical Record	<input type="checkbox"/>

**A3. Trust – People**  
How **SAFE** do you think your personal information is in the hands of the following groups?  
Please give a **SCORE OUT OF 10** where a **10 = Extremely Safe** and **0 = Not Safe At All**

Family	<input type="checkbox"/>	Journalist	<input type="checkbox"/>
The Government	<input type="checkbox"/>	Stranger	<input type="checkbox"/>
Medical Professional	<input type="checkbox"/>	Close Friend	<input type="checkbox"/>
Criminal	<input type="checkbox"/>	Private Company	<input type="checkbox"/>
Legal Professional	<input type="checkbox"/>	Work Colleague	<input type="checkbox"/>

**A4. Trust – Technologies**  
How **SAFE** do you think your personal information is in the hands of the following groups?  
Please give a **SCORE OUT OF 10** where a **10 = Extremely Safe** and **0 = Not Safe At All**

Correspondence via postal mail	<input type="checkbox"/>	Face to face conversation on busy train	<input type="checkbox"/>
Conversation on mobile phone	<input type="checkbox"/>	Information sent by email	<input type="checkbox"/>
Information sent by text message	<input type="checkbox"/>	Face to face conversation in a private place	<input type="checkbox"/>
Using social networking sites	<input type="checkbox"/>	Conversation on landline telephone	<input type="checkbox"/>

**A5. Privacy Overview**  
Please give a **SCORE OUT OF 10** where a **10 = Fully Agree** and **0 = Do NOT Agree At All**

A) You are concerned about threats to your personal privacy.

B) Commercial organisations seek excessive amounts of information from consumers.

C) Federal governments invade on citizens privacy.

D) You have lost all control over circulation of your personal data.

**PART B - Trade-offs**

**B1. Scenarios**  
Please answer **YES** or **NO** to the following questions

A) Would you give the details of everything that you purchase to a private company by email in return for a financial gain?  YES  NO

B) During a car journey would you tell a company the road and weather conditions in your location via a wireless network if it would help to reduce your impact on the environment?  YES  NO

C) Would you send your credit card details over an internet connection to a private company to book a room at a hotel in order to receive a discount?  YES  NO

D) Would you tell a close friend your embarrassing secrets in a letter sent by postal mail if you thought it would bring you a lot of enjoyment?  YES  NO

E) Would you tell a journalist in a private meeting your musical preferences in return for a rise in your social standing?  YES  NO

F) Would you tell the government by text message exactly where you plan to travel if it reduced your travel time?  YES  NO

G) During a car journey would you tell a stranger your location over a wireless network if it improved the safety of you and your family during the journey?  YES  NO

H) Would you allow a security guard to search you and your luggage if it might improve your safety?  YES  NO

I) Would you let a private company know about your driving behaviour (speed at which you travel, how far you travel etc) if it reduced your insurance premiums?  YES  NO

J) Would you tell your medical conditions to a random doctor via a mobile phone if you thought it could improve your health?  YES  NO

K) During a car journey would you tell a stranger your location anonymously over a wireless network if it improved the safety of you and your family during the journey?  YES  NO

L) If your whereabouts was made public at all times would you stop travelling to certain places?  YES  NO

**PART C - Improvements**

**C1. Preferred Improvements**  
Which of the following improvements would you like implemented please tick a **MAXIMUM OF THREE** boxes

Organisations giving you more information about what your data will be used for and how it will be protected

Organisations making it easier for you to change errors in the data they hold on you

Better security to stop improper/external access to your stored personal data

A better legal framework that punishes organisations that use your data for something that you have not authorised

Organisations minimising the volume of personal data they collect

Organisations giving you more control over exactly what your personal data is used for



**Appendix C – Greek Version of European Survey**

**ΜΕΡΟΣ Δ - Σχετικά με εσάς και τις επιλογές σας**

**Δ1. Οι προσωπικές επιλογές και εμπειρίες σας**

A) Χρησιμοποιείτε κάρτες επιβράβευσης (π.χ. Κάρτα Carrefour-Μαρινόπουλος, Travelair Club Olympic Air);  ΝΑΙ  ΟΧΙ

B) Έχετε κάνει ποτέ κάποια αγορά με πιστωτική κάρτα μέσω διαδικτύου;  ΝΑΙ  ΟΧΙ

Γ) Έχετε περάσει/ Θα ήσασταν πρόθυμος να περάσετε μέσα από έλεγχο αεροδρομίου;  ΝΑΙ  ΟΧΙ

Δ) Έχετε επιλέξει ο τηλεφωνικός σας αριθμός να μη βρίσκεται στον τηλεφωνικό κατάλογο;  ΝΑΙ  ΟΧΙ

E) Διαβάζετε την πολιτική προστασίας προσωπικών δεδομένων των εταιρειών πριν χρησιμοποιήσετε τις υπηρεσίες τους;  ΝΑΙ  ΟΧΙ

ΣΤ) Έχετε ελέγξει ποτέ τα δεδομένα που διατηρούν οι φορείς πιστωτικού ελέγχου (Τειρεσίας κτλ) για εσάς;  ΝΑΙ  ΟΧΙ

Z) Έχετε πλήρη γνώση των νομικών σας δικαιωμάτων σχετικά με την προστασία των προσωπικών δεδομένων;  ΝΑΙ  ΟΧΙ

H) Έχουν ποτέ εισθάλει στα προσωπικά σας δεδομένα; Εάν ναι, παρακαλώ περιγράψτε την εμπειρία σας  ΝΑΙ  ΟΧΙ

\_\_\_\_\_

\_\_\_\_\_

Θ) Υπάρχει κάτι άλλο το οποίο έχει διαμορφώσει την άποψή σας για την ιδιωτικότητα;

\_\_\_\_\_

\_\_\_\_\_

**Δ2. Πληροφορίες**

Οι παρακάτω ερωτήσεις είναι προαιρετικές αλλά θα βοηθούσαν στην έρευνα. Σας διαβεβαιώνουμε ότι η ανάλυση θα γίνει ανώνυμα και θα τηρηθεί το απόρρητο των προσωπικών σας πληροφοριών.

A) Ποιά είναι η επαγγελματική σας κατάσταση; Μαθητής/Φοιτητής  Εργαζόμενος  Συνταξιούχος  Άνεργος  Άλλο

B) Ποιά είναι το ετήσιο οικογενειακό σας εισόδημα; 0-20.000€  20-40.000€  40-60.000€  60-80.000€  80000+€

Γ) Έχετε δίπλωμα οδήγησης; ΝΑΙ  ΟΧΙ

Δ) Ποιά είναι το φύλο σας; ΑΝΔΡΑΣ  ΓΥΝΑΙΚΑ

E) Έχετε παιδιά; ΝΑΙ  ΟΧΙ

ΣΤ) Το επίπεδο της εκπαίδευσής σας; Κανένα  Υποχρεωτική εκπαίδευση  Λύκειο  Προπτυχιακό  Μεταπτυχιακό

Z) Ποιά είναι η εθνικότητά σας; \_\_\_\_\_

H) Πόσο χρονών είστε; \_\_\_\_\_




Θ) Ποιά είναι η οικογενειακή σας κατάσταση; \_\_\_\_\_

**Δ3. Περισσότερες πληροφορίες**

A) Θα επιθυμούσατε να λάβετε μέρος σε μια συνέντευξη για την οποία θα ανταμειφθείτε με δωροεπιταγή 25 ευρώ από το amazon ή τα Marks&Spencer; Εάν το επιθυμείτε, παρακαλώ σημειώστε τον τηλεφωνικό σας αριθμό ή την ηλεκτρονική σας διεύθυνση.

\_\_\_\_\_

Ευχαριστώ πάρα πολύ για τον χρόνο σας, παρακαλώ ταχυδρομήστε το ερωτηματολόγιο μέσα στο φάκελο των προπληρωμένων τελών που παραλάβατε.

Αξιότιμε/η Κύριε/α

Σας γράφω για να ζητήσω τη βοήθεια σας σχετικά με μια έρευνα, η οποία αποτελεί σημαντικό τμήμα των μεταπτυχιακών μου σπουδών. Η έρευνά μου χρηματοδοτείται από την Ευρωπαϊκή Επιτροπή ως μέρος του προγράμματος NEARCTIS και θα διασφαλίσει ότι οι μελλοντικές τεχνολογίες και πολιτικές θα ανταποκρίνονται στις απαιτήσεις σας για την προστασία των προσωπικών σας δεδομένων. Περισσότερες πληροφορίες σχετικά με την έρευνα είναι διαθέσιμες στην ιστοσελίδα: [www.internationalprivacysurvey.com](http://www.internationalprivacysurvey.com).

Έχετε επιλεγεί για αυτήν την έρευνα από ένα τυχαίο δείγμα ατόμων, το οποίο θα αντιπροσωπεύσει τις διαφορετικές απόψεις που επικρατούν στην Ευρωπαϊκή Ένωση. Για αυτό το λόγο, η απάντησή σας είναι κρίσιμης σημασίας για την επιτυχία της έρευνας, καθώς όσες περισσότερες απαντήσεις συλλεχθούν, τόσο πιο ακριβή θα είναι τα τελικά αποτελέσματα.

Παρακαλώ συμπληρώστε το ερωτηματολόγιο και επιστρέψτε το χρησιμοποιώντας το φάκελο των προπληρωμένων τελών που εσωκλείεται. Εναλλακτικά, μπορείτε να συμπληρώσετε το ερωτηματολόγιο διαδικτυακά στην ηλεκτρονική διεύθυνση [www.internationalprivacysurvey.com](http://www.internationalprivacysurvey.com), εισάγοντας τον κωδικό πρόσβασης που θα βρείτε στο πάνω μέρος αυτής σελίδας.

Η συμπλήρωση του ερωτηματολογίου δεν θα διαρκέσει περισσότερο από 15 λεπτά. Θα σας παρακαλούσα να διαθέσετε αυτό το χρόνο για να το συμπληρώσετε.

Σας ευχαριστώ για τη βοήθεια σας και θα περιμένω την απάντησή σας.

Με τιμή,

Scott Cruickshanks  
Υποψήφιος διδάκτωρ  
Πολυτεχνείο Κρήτης  
Τμήμα Μηχανικών Παραγωγής και Διοίκησης  
Πολυτεχνειούπολη  
73100 Χανιά



## Μέρος Α - Επιβράβευση, Εμπιστοσύνη και Ιδιωτικότητα

## Α1. Επιβράβευση

Όταν αποφασίζετε τον τρόπο με τον οποίο θα ταξιδέψετε, πόσο ΣΗΜΑΝΤΙΚΟΙ είναι οι παρακάτω παράγοντες; Παρακαλώ βαθμολογήστε σε κλίμακα από 0 έως 10 όπου 10=Ιδιαίτερα σημαντικό και 0= Καθόλου σημαντικό

Χρόνος ταξιδιού	<input type="checkbox"/>	Οι επιπτώσεις στο περιβάλλον	<input type="checkbox"/>
Η δική σας ασφάλεια και της οικογένειά σας	<input type="checkbox"/>	Διασκέδαση	<input type="checkbox"/>
Το κόστος	<input type="checkbox"/>	Οι επιπτώσεις στη προσωπική σας εικόνα	<input type="checkbox"/>

## Α2. Τύποι πληροφοριών

Πόσο ΠΡΟΣΕΚΤΙΚΟΙ είστε όταν σας ζητούν τις παρακάτω πληροφορίες; Παρακαλώ βαθμολογήστε σε κλίμακα από 0 έως 10 όπου 10=Ιδιαίτερα προσεκτικός και 0= Καθόλου προσεκτικός

Τις καιρικές συνθήκες στη θέση που βρίσκεστε	<input type="checkbox"/>	Την οδική σας συμπεριφορά (ταχύτητα, απόσταση κτλ)	<input type="checkbox"/>
Τις ταινίες/ πραγματοποιημένες θέσεις σας	<input type="checkbox"/>	Τις μουσικές σας προτιμήσεις	<input type="checkbox"/>
Τα στοιχεία του τραπεζικού σας λογαριασμού	<input type="checkbox"/>	Την εθνικότητά σας	<input type="checkbox"/>
Το εισόδημά σας	<input type="checkbox"/>	Το ιστορικό των αγορών σας	<input type="checkbox"/>
Τα προσωπικά σας μυστικά	<input type="checkbox"/>	Το ιατρικό σας ιστορικό	<input type="checkbox"/>

## Α3. Εμπιστοσύνη-Άνθρωποι

Πόσο ΑΣΦΑΛΕΙΣ νομίζετε ότι είναι οι προσωπικές σας πληροφορίες στα χέρια των παρακάτω ομάδων; Παρακαλώ βαθμολογήστε σε κλίμακα από 0 έως 10 όπου 10=Απόλυτα ασφαλείς και 0= Καθόλου ασφαλείς

Οικογένεια	<input type="checkbox"/>	Δημοσιογράφος	<input type="checkbox"/>
Κυβέρνηση	<input type="checkbox"/>	Άγνωστος	<input type="checkbox"/>
Ιατρικό προσωπικό	<input type="checkbox"/>	Κοντινός φίλος	<input type="checkbox"/>
Εγκληματίας	<input type="checkbox"/>	Ιδιωτική εταιρεία	<input type="checkbox"/>
Νομικός	<input type="checkbox"/>	Συνάδελφος	<input type="checkbox"/>

## Α4. Εμπιστοσύνη-Τεχνολογία

Πόσο ΑΣΦΑΛΕΙΣ νομίζετε ότι είναι οι προσωπικές σας πληροφορίες στα χέρια των παρακάτω ομάδων; Παρακαλώ βαθμολογήστε σε κλίμακα από 0 έως 10 όπου 10=Απόλυτα ασφαλείς και 0= Καθόλου ασφαλείς

Αναπόκριση μέσω ταχυδρομείου	<input type="checkbox"/>	Συζήτηση σε γεμάτο τρέινο	<input type="checkbox"/>
Συζήτηση μέσω κινητού τηλεφώνου	<input type="checkbox"/>	Αποστολή ηλεκτρονικού ταχυδρομείου μέσω ενσύρματου δικτύου	<input type="checkbox"/>
Πληροφορίες που στέλνονται μέσω γραπτού μηνύματος	<input type="checkbox"/>	Συζήτηση σε ιδιωτική τοποθεσία	<input type="checkbox"/>
Αποστολή ηλεκτρονικού ταχυδρομείου μέσω ασύρματου δικτύου	<input type="checkbox"/>	Συζήτηση μέσω σταθερού τηλεφώνου	<input type="checkbox"/>

## Α5. Ιδιωτικότητα

Παρακαλώ βαθμολογήστε σε κλίμακα από 0 έως 10 όπου 10=Συμφωνών απόλυτα και 0= Δεν συμφωνώ καθόλου

- Α) Ανησυχώ για τις απειλές κατά της ιδιωτικής μου ζωής.
- Β) Οι εμπορικοί οργανισμοί αναζητούν υπερβολικά πολλές πληροφορίες από τους καταναλωτές.
- Γ) Η κυβέρνηση εισβάλλει στη ιδιωτική ζωή των πολιτών.
- Δ) Έχω χάσει τον έλεγχο της διαχείρισης των προσωπικών μου δεδομένων.

## ΜΕΡΟΣ Β - Ανταλλάγματα

## Β1. Σενάρια

Παρακαλώ απαντήστε ΝΑΙ ή ΟΧΙ στις παρακάτω ερωτήσεις.

- Α) Θα δίνετε πληροφορίες για τις αγορές σας έναντι οικονομικού οφέλους σε μια ιδιωτική εταιρεία μέσω ηλεκτρονικού ταχυδρομείου;  ΝΑΙ  ΟΧΙ
- Β) Κατά τη διάρκεια ενός οδικού ταξιδιού θα δίνετε πληροφορίες σε μια εταιρεία σχετικά με τον δρόμο και τις καιρικές συνθήκες στην τοποθεσία που βρίσκεστε μέσω ασύρματου δικτύου, εάν αυτό σας βοηθούσε να μειώσετε τις επιπτώσεις σας στο περιβάλλον;  ΝΑΙ  ΟΧΙ
- Γ) Θα δίνετε τα στοιχεία της πιστωτικής σας κάρτας σε μια ιδιωτική εταιρεία μέσω διαδικτύου για να κάνετε κράτηση δωματίου σε ξενοδοχείο με αντάλλαγμα έκπτωση στη τιμή;  ΝΑΙ  ΟΧΙ
- Δ) Θα αποκαλύπτατε τα προσωπικά σας μυστικά σε κάποιον καλό σας φίλο μέσω γραπτού ταχυδρομείου, εάν πιστεύατε ότι αυτό θα σας έκανε να νιώθετε καλύτερα;  ΝΑΙ  ΟΧΙ
- Ε) Θα αποκαλύπτατε σε μια ιδιωτική συναμία με δημοσιογράφο τις μουσικές σας προτιμήσεις, εάν αυτό βοηθούσε την καινική σας καταξίωση;  ΝΑΙ  ΟΧΙ
- ΣΤ) Θα ενημερώνατε μια κρατική υπηρεσία μέσω γραπτού μηνύματος που ακριβώς σκοπεύετε να ταξιδέψετε, εάν αυτό θα μείωνε το χρόνο ταξιδιού σας;  ΝΑΙ  ΟΧΙ
- Ζ) Κατά τη διάρκεια ενός οδικού ταξιδιού θα αποκαλύπτατε σε κάποιον άγνωστο τη θέση σας μέσω ασύρματου δικτύου, εάν αυτό βελτιώνει την ασφάλεια τη δική σας και της οικογένειά σας κατά τη διάρκεια του ταξιδιού;  ΝΑΙ  ΟΧΙ
- Η) Θα επιτρέπατε σε έναν φρουρό ασφαλείας να ψάξει εσάς και τις αποσκευές σας, εάν αυτό μπορούσε να βελτιώσει την προσωπική σας ασφάλεια;  ΝΑΙ  ΟΧΙ
- Θ) Θα επιτρέπατε σε μια ιδιωτική εταιρεία να γνωρίζει την οδική σας συμπεριφορά (ταχύτητα με την οποία ταξιδεύετε, πόσο μακριά ταξιδεύετε, κτλ), εάν αυτό μείωνε το κόστος των ασφαλιστρών σας;  ΝΑΙ  ΟΧΙ
- Ι) Θα λέγατε το ιατρικό σας ιστορικό σε οποιοδήποτε ιατρό μέσω κινητού τηλεφώνου, εάν θεωρούσατε ότι θα βοηθούσε την υγεία σας;  ΝΑΙ  ΟΧΙ
- ΙΑ) Κατά τη διάρκεια ενός οδικού ταξιδιού θα αποκαλύπτατε ανώνυμα σε κάποιον άγνωστο τη θέση σας μέσω ασύρματου δικτύου, εάν αυτό βελτιώνει την ασφάλεια τη δική σας και της οικογένειά σας κατά τη διάρκεια του ταξιδιού;  ΝΑΙ  ΟΧΙ
- ΙΒ) Εάν διαρκώς δημοσιεύονταν πληροφορίες για τις τοποθεσίες που βρίσκεστε, θα σας απέτρεπε από το να τις επισκέπτεστε;  ΝΑΙ  ΟΧΙ

## ΜΕΡΟΣ Γ - Βελτιώσεις

## Γ1. Επιθυμητές βελτιώσεις

Ποιές από τις ακόλουθες βελτιώσεις θα επιθυμούσατε να εφαρμοστούν; Παρακαλώ σημειώστε έως ΤΡΕΙΣ επιλογές.

- Οι οργανισμοί να σας παρέχουν περισσότερες πληροφορίες σχετικά με τη χρήση και τον τρόπο προστασίας των δεδομένων σας.
- Οι οργανισμοί να σας διευκολύνουν να διορθώσετε τυχόν λάθη στα στοιχεία, που διατηρούν σχετικά με εσάς.
- Μεγαλύτερη ασφάλεια στη διαφύλαξη των προσωπικών σας βάσεων δεδομένων από ανάρμοστη/εξωτερική πρόσβαση.
- Καλύτερο νομικό πλαίσιο που πμωρεί τη χρήση των στοιχείων σας από οργανισμούς χωρίς τη συγκατάθεσή σας.
- Οι οργανισμοί να μειώσουν τον όγκο των προσωπικών δεδομένων που συλλέγουν.
- Οι οργανισμοί να σας παρέχουν περισσότερο έλεγχο σχετικά με την ακριβή χρήση των προσωπικών δεδομένων σας.



**Appendix D – Dutch Version of European Survey**

## PART D - Over Uzelf &amp; Uw Keuzes

## D1. Uw Keuzes en Ervaringen

- A) Gebruikt u bepaalde klanten-/loyaliteitskaarten? (Albert Heijn Bonus Kaart, Air Miles, etc.)  JA  NEE
- B) Heeft u ooit iets online gekocht met een credit card?  JA  NEE
- C) Bent u/Zou u ooit door luchthaven security (ge)gaan?  JA  NEE
- D) Is uw telefoonnummer geregistreerd als een privénummer?  JA  NEE
- E) Leest u het privacybeleid van een bedrijf vooraleer u hun diensten gebruikt?  JA  NEE
- F) Heeft u ooit data opgevraagd die bedrijven gespecialiseerd in kredietwaardigheidschecks (Experian etc.) over u heeft?  JA  NEE
- G) Begrijpt u volledig wat uw juridische rechten zijn met betrekking tot uw privacy?  JA  NEE
- H) Heeft u ooit een inbreuk op uw privacy ervaren? Zo ja, geef hierover een korte beschrijving:  JA  NEE
- \_\_\_\_\_
- \_\_\_\_\_

- I) Is er nog iets anders dat uw kijk op privacy heeft beïnvloed?
- \_\_\_\_\_
- \_\_\_\_\_

## D2. Informatie over uzelf

Deze laatste vragen zijn volledig vrijblijvend, maar zouden een grote hulp zijn voor mijn onderzoek. Ik wil u eraan herinneren dat alle antwoorden die u geeft, volledig anoniem verwerkt en vertrouwelijk behandeld worden.

- A) Wat is uw arbeidssituatie? Student  Werkend  Met pensioen  Werkzoekend  Anders
- B) Wat is uw jaarlijks huishoudelijk inkomen? € 0-20K  € 20-40K  € 40-60K  € 60-80K  € 80K+
- C) Bent u in het bezit van een rijbewijs? JA  NEE
- D) Wat is uw geslacht? MAN  VROUW
- E) Heeft u kinderen? JA  NEE
- F) Wat is uw opleidingsniveau? Geen  VMBO  HAVO/VWO  Bachelor  Master / PhD / Post-doc
- G) Wat is uw etniciteit? (e.g. Blank / (Noord-)Afrikaans / Aziatisch / etc.) \_\_\_\_\_
- H) Wat is uw leeftijd? \_\_\_\_\_
- I) Wat is uw burgerlijke stand? \_\_\_\_\_

## D3. Verdere informatie

- A) Bent u beschikbaar voor een eventueel verder interview? Hiervoor zal u een kadobon ter waarde van €25 ontvangen van Amazon of M&S. Zo ja, vul dan hieronder uw telefoonnummer of e-mailadres in.
- \_\_\_\_\_

Ontzettend bedankt voor uw tijd! Gelieve deze enquête terug te sturen in de bijgesloten enveloppe. Een postzegel is niet vereist.



ONLINE TOEGANGSCODE: NL-001

7 maart 2012

Beste heer/mevrouw,

Ik schrijf u met de vraag om mee te doen aan een onderzoek dat deel uitmaakt van mijn promotieonderzoek. Mijn onderzoek is gefinancierd door de Europese Commissie als onderdeel van het NEARCTIS project en zal ertoe bijdragen dat toekomstig beleid en technologieën aan uw privacy eisen zullen voldoen. Meer informatie over mijn onderzoek kan u vinden op [www.internationalprivacysurvey.com](http://www.internationalprivacysurvey.com).

Door mee te doen aan deze enquête maakt u deel uit van een willekeurige steekproef van mensen, die de verschillende opvattingen in de Europese Unie vertegenwoordigen. Daarom zijn uw medewerking en uw antwoorden van onschatbare waarde voor het succes van dit onderzoek. Des te meer reacties ik kan verzamelen, des te nauwkeuriger de conclusies van dit onderzoek zullen zijn.

Vul de bijgevoegde enquête in en stuur deze terug in de bijgevoegde enveloppe. Een postzegel is niet vereist. Als alternatief kan u de enquête online invullen op [www.internationalprivacysurvey.com](http://www.internationalprivacysurvey.com) met behulp van de toegangscode die u bovenaan deze pagina vindt.

Het invullen van deze enquête zal maximaal 15 minuten duren. Neem alstublieft uw tijd om alle vragen te beantwoorden.

Bedankt voor uw hulp.

Met vriendelijke groet,

Scott Cruickshanks  
Postgraduate Student  
School of Civil Engineering and the Environment  
University of Southampton  
Highfield  
Southampton  
SO17 1BJ

## PART A - Beloning, Vertrouwen en Privacy

## A1. Factoren

Wanneer u kiest voor een vervoersmethode, hoe **BELANGRIJK** zijn de volgende factoren?

Geef een **SCORE OP 10** (10 = enorm belangrijk en 0 = totaal niet belangrijk)

Reistijd	<input type="checkbox"/>	Impact op het milieu	<input type="checkbox"/>
Veiligheid van u en uw familie	<input type="checkbox"/>	Plezier	<input type="checkbox"/>
Kosten	<input type="checkbox"/>	Impact op uw imago (Wat anderen zouden denken)	<input type="checkbox"/>

## A2. Types van Informatie

Hoe **BERSCHERMEND** bent u over de volgende types van informatie?

Geef een **SCORE OP 10** (10 = enorm beschermend en 0 = totaal niet beschermend)

De weersomstandigheden van uw huidige locatie	<input type="checkbox"/>	Uw rijgedrag (snelheid, afstanden, etc)	<input type="checkbox"/>
Uw huidige of vorige locaties	<input type="checkbox"/>	Uw muzikale voorkeur	<input type="checkbox"/>
Uw bankgegevens	<input type="checkbox"/>	Uw etniciteit	<input type="checkbox"/>
Uw inkomen	<input type="checkbox"/>	Uw aankoopgeschiedenis	<input type="checkbox"/>
Uw gênante geheimen	<input type="checkbox"/>	Uw medisch dossier	<input type="checkbox"/>

## A3. Vertrouwen – Mensen

Hoe **VEILIG** denkt u dat persoonlijke informatie is in de handen van de volgende groepen? Geef een **SCORE OP 10** (10 = enorm veilig en 0 = totaal niet veilig)

Familie	<input type="checkbox"/>	Journalist	<input type="checkbox"/>
De overheid	<input type="checkbox"/>	Onbekende	<input type="checkbox"/>
Medisch professional (vb. Dokter, verpleegster,...)	<input type="checkbox"/>	Goede vriend	<input type="checkbox"/>
Crimineel	<input type="checkbox"/>	Privébedrijf	<input type="checkbox"/>
Juridisch professional (vb. Advocaat, notaris,...)	<input type="checkbox"/>	Collega	<input type="checkbox"/>

## A4. Vertrouwen – Technologie

Hoe **VEILIG** denkt u dat persoonlijke informatie, verstuurd met de volgende communicatiemiddelen, is? Geef een **SCORE OP 10** (10 = enorm veilig en 0 = totaal niet veilig)

Correspondentie via brieven	<input type="checkbox"/>	Face-to-face conversatie op een druk bezette trein	<input type="checkbox"/>
Conversatie via een mobiele telefoon	<input type="checkbox"/>	Informatie verzonden via e-mail	<input type="checkbox"/>
Informatie verzonden met een SMS	<input type="checkbox"/>	Face-to-face conversatie op een private plaats	<input type="checkbox"/>
Gebruik van sociale netwerk sites	<input type="checkbox"/>	Conversatie via een vaste telefoonlijn	<input type="checkbox"/>

## A5. Privacy Overzicht

Geef een **SCORE OP 10** (10 = helemaal akkoord, 0 = helemaal niet akkoord)

- A) U bent bezorgd over uw persoonlijke privacy.
- B) Commerciële organisaties vergaren grote hoeveelheden informatie over consumenten.
- C) Federale overheden schenden de privacy van burgers.
- D) U bent alle controle verloren over de verspreiding van uw persoonlijke informatie.

## PART B - Scenarios

## B1. Scenarios

Antwoord met **JA** of **NEE** op de volgende vragen

- A) Zou u een privébedrijf details over al uw aankopen versturen via e-mail in ruil voor een financiële tegemoetkoming?  JA  NEE
- B) Zou u tijdens een autorit gegevens over de weg en weersomstandigheden op uw locatie versturen naar een bedrijf via een draadloos netwerk, als dat uw impact op het milieu zou verminderen?  JA  NEE
- C) Zou u de gegevens van uw credit card via internet naar een privébedrijf versturen om een hotelkamer te boeken als u daarmee korting krijgt?  JA  NEE
- D) Zou u een gênant geheim vertellen aan een goede vriend in een brief verzonden met de post als u denkt dat dat u plezier zou scheppen?  JA  NEE
- E) Zou u uw muzikale voorkeur vertellen aan een journalist tijdens een privéontmoeting als dat uw sociale status zou verhogen?  JA  NEE
- F) Zou u de overheid via SMS vertellen waar u exact naar toe wil reizen als dat de reistijd zou verminderen?  JA  NEE
- G) Zou u tijdens een autorit gegevens over uw locatie versturen naar een onbekende als dat de veiligheid van u en uw familie zou verbeteren tijdens de rit?  JA  NEE
- H) Zou u een beveiligingsbeambte toelaten u en uw bagage te doorzoeken als dat uw veiligheid zou verbeteren?  JA  NEE
- I) Zou u een privébedrijf toegang geven tot uw rijgedrag (snelheid, reisafstand, etc) als dat uw verzekeringspremie zou verminderen?  JA  NEE
- J) Zou u uw medische aandoeningen vertellen aan een willekeurige dokter via een mobiele telefoon als u denkt dat dat uw gezondheid zou verbeteren?  JA  NEE
- K) Zou u tijdens een autorit uw locatie anoniem versturen naar een onbekende via een draadloos netwerk als dat de veiligheid van u en uw familie zou verbeteren tijdens de rit?  JA  NEE
- L) Als uw verblijfplaats ten allen tijde publiek zou worden gemaakt, zou u dan stoppen met naar sommige plaatsen te reizen?  JA  NEE

## PART C - Verbeteringen

## C1. Verbeteringen

Welke van de volgende verbeteringen zou u graag geïmplementeerd zien? Kruis **MAXIMAAL DRIE** opties aan.

- Organisaties geven meer informatie over waarvoor ze uw gegevens gebruiken en hoe uw gegevens zullen worden beschermd.
- Organisaties maken het makkelijker om fouten in de gegevens die ze over u heeft te veranderen.
- Beter beveiliging om onbevoegde/externe toegang tot uw opgeslagen persoonlijke gegevens te verhinderen.
- Een beter juridisch kader om organisaties te straffen die uw gegevens gebruiken voor iets waarvoor u geen toestemming heeft gegeven.
- Organisaties minimaliseren het volume aan persoonlijke gegevens die ze verzamelen.
- Organisaties geven u meer controle over waarvoor uw gegevens exact worden gebruikt.



**Appendix E – Austrian Version of European Survey**

## Internationale Umfrage über Datenschutz

### Überblick

#### Ihr Code

Wenn Sie einen Code erhalten haben, geben Sie ihn bitte hier ein?

#### Ihre Nationalität

Was ist Ihre Nationalität?

#### TEIL A - Datenschutz Überblick

Bitte geben Sie eine Note von 0 bis 10 , wobei **10 = vollkommen einverstanden** und **0 = nicht einverstanden** entspricht

1) Sind Sie heutzutage um Ihre Privatsphäre besorgt?

 0  1  2  3  4  5  6  7  8  9  10

2) Suchen Organisationen übermäßige Informationen von den Konsumenten?

 0  1  2  3  4  5  6  7  8  9  10

3) Dringen Bundesregierungen in die Privatsphäre der Bürger ein?

 0  1  2  3  4  5  6  7  8  9  10

4) Haben Sie die gesamte Kontrolle über Weitergabe Ihrer persönlichen Daten verloren?

 0  1  2  3  4  5  6  7  8  9  10

Nächste

## Internationale Umfrage über Datenschutz

### Belohnungen und Konsequenzen

#### A1 Belohnungen

Bei der Entscheidung über eine Art des Reisens, wie **wichtig** sind die folgenden Faktoren?

Bitte geben Sie eine **Note von 0 bis 10**, wobei **10 = extrem wichtig** und **0 = überhaupt nicht wichtig** entspricht

Reisezeit

 0  1  2  3  4  5  6  7  8  9  10

Auswirkungen auf die Umwelt

 0  1  2  3  4  5  6  7  8  9  10

Die Sicherheit von Ihnen und Ihrer Familie

 0  1  2  3  4  5  6  7  8  9  10

Fahrspass

 0  1  2  3  4  5  6  7  8  9  10

Kosten

 0  1  2  3  4  5  6  7  8  9  10

Auswirkungen auf Ihr Ansehen (was denken andere über Sie)

 0  1  2  3  4  5  6  7  8  9  10



**A2 Arten von Informationen**

Wie **fürsorglich** gehen Sie mit den folgenden Arten von Informationen um?

Bitte geben Sie eine **Note von 0 bis 10**, wobei **10 = extrem fürsorglich** und **0 = überhaupt nicht fürsorglich** entspricht

Die Wetterbedingungen Ihres jetzigen Standortes

0  1  2  3  4  5  6  7  8  9  10

Ihr Fahrverhalten (Geschwindigkeit, Entfernung, etc.)

0  1  2  3  4  5  6  7  8  9  10

Ihr jetziger / voriger Standorte

0  1  2  3  4  5  6  7  8  9  10

Ihre Musikpräferenzen

0  1  2  3  4  5  6  7  8  9  10

Ihre Bank- / Kreditkarten Details

0  1  2  3  4  5  6  7  8  9  10

Ihre Abstammung

0  1  2  3  4  5  6  7  8  9  10

Höhe Ihres Einkommens

0  1  2  3  4  5  6  7  8  9  10

Ihre Einkaufsstatistik

0  1  2  3  4  5  6  7  8  9  10

Ihre peinlichen Geheimnisse

0  1  2  3  4  5  6  7  8  9  10

Ihre Krankenakte

0  1  2  3  4  5  6  7  8  9  10

Nächste

**Risiken****A3 Vertrauen - Leute**

Wie **sicher** betrachten Sie Ihre persönlichen Informationen in den Händen der folgenden Personengruppen?

Bitte geben Sie eine **Note von 0 bis 10**, wobei **10 = extrem sicher** und **0 = überhaupt nicht sicher** entspricht

Familie

0  1  2  3  4  5  6  7  8  9  10

Journalisten

0  1  2  3  4  5  6  7  8  9  10

Die Regierung

0  1  2  3  4  5  6  7  8  9  10

Fremde

0  1  2  3  4  5  6  7  8  9  10

Medizinische Fachkräfte

0  1  2  3  4  5  6  7  8  9  10

enge Freunde

0  1  2  3  4  5  6  7  8  9  10

Kriminelle

0  1  2  3  4  5  6  7  8  9  10

Privatgesellschaften

0  1  2  3  4  5  6  7  8  9  10

Juristische Fachkräfte

0  1  2  3  4  5  6  7  8  9  10

Arbeitskollegen

0  1  2  3  4  5  6  7  8  9  10

**A4 Vertrauen - Technologien**

Wie **sicher** werden Ihrer Auffassung nach Ihre persönlichen Informationen von den folgenden Technologien übertragen?

Bitte geben Sie eine **Note von 0 bis 10**, wobei **10 = extrem sicher** und **0 = überhaupt nicht sicher** entspricht

Korrespondenz per Post

0  1  2  3  4  5  6  7  8  9  10

Face to face-Gespräch in einem vollen Zug

0  1  2  3  4  5  6  7  8  9  10

Gespräch am Handy

0  1  2  3  4  5  6  7  8  9  10

E-Mail über eine Kabel-Internet-Verbindung gesendet

0  1  2  3  4  5  6  7  8  9  10

Informationen per SMS geschickt

0  1  2  3  4  5  6  7  8  9  10

Face to face-Gespräch an einem privaten Ort

0  1  2  3  4  5  6  7  8  9  10

E-Mail über eine WLAN-Verbindung gesendet

0  1  2  3  4  5  6  7  8  9  10

Gespräch am Festnetztelefon

0  1  2  3  4  5  6  7  8  9  10

Nächste

**Kompromisse****B1 - Szenarien**

Bitte beantworten Sie die folgenden Fragen mit **JA** oder **NEIN**

A) Würden Sie Details von allem was Sie kaufen, einem privaten Unternehmen per E-Mail als Gegenleistung für einen finanziellen Gewinn geben?

Ja  Nein

B) Würden Sie einem Unternehmen, während einer Autofahrt, über die Straßen- und Wetterbedingungen an Ihrem Standort über ein Funknetzwerk berichten, wenn es helfen würde, um Ihre Auswirkungen auf die Umwelt zu reduzieren?

Ja  Nein

C) Würden Sie die Daten Ihrer Kreditkarte über eine Internet-Verbindung an ein privates Unternehmen senden um ein Zimmer in einem Hotel zu buchen, um einen Rabatt zu erhalten?

Ja  Nein

D) Würden Sie einem engen Freund Ihre peinlichen Geheimnisse in einem per Post geschickten Brief mitteilen, wenn es es Ihnen viel Vergnügen machen würde?

Ja  Nein

E) Würden Sie einem Journalisten, in einem privaten Gespräch, Ihre Musikpräferenzen im Gegenzug für einen Anstieg in Ihrem sozialen Status sagen?

Ja  Nein

F) Würden Sie der Regierung per SMS mitteilen, wohin Sie reisen wollen, wenn es Ihre Fahrzeit reduzieren kann?

Ja  Nein

G) Würden Sie einem Fremden während einer Autofahrt Ihren Standort über ein Funknetz mitteilen, wenn es die Sicherheit von Ihnen und Ihrer Familie während der Fahrt verbessern kann?

Ja  Nein

H) Würden Sie einem Sicherheitsbeamten erlauben Ihr Gepäck zu durchsuchen, wenn dies Ihre Sicherheit verbessern könnte?

Ja  Nein

J) Würden Sie einem zufälligen Arzt Ihren Gesundheitszustand über das Handy mitteilen, wenn Sie denken würden, dass es Ihre Gesundheit verbessern könnte?

- Ja  Nein

K) Würden Sie einem Fremden während einer Autofahrt Ihren Standort über ein Funknetz **anonym** berichten, wenn es die Sicherheit von Ihnen und Ihrer Familie verbessern könnte?

- Ja  Nein

L) Würden Sie aufhören an bestimmte Orte zu reisen, wenn Ihr Aufenthaltsort zu jeder Zeit veröffentlicht würde?

- Ja  Nein

#### C1 - bevorzugte Verbesserungen

Welche der folgenden Verbesserungen würden Sie sich wünschen; kreuzen Sie bitte ein **Maximum von drei** Kästchen an

A) Organisationen die Ihnen mehr Informationen geben würden, wofür Ihre Daten verwendet werden und wie diese geschützt werden.

- Ja  Nein

B) Organisationen, die es für Sie einfacher machen, die Fehler in den Daten, die sie über Sie haben zu ändern.

- Ja  Nein

C) Mehr Sicherheit um den unsachgemäße / externe Zugang zu Ihren gespeicherten personenbezogenen Daten zu stoppen.

- Ja  Nein

D) Ein besserer rechtlicher Rahmen, der die Unternehmen, welche Ihre Daten für etwas, dass Sie nicht autorisiert haben, verwenden, bestraft.

- Ja  Nein

E) Organisationen, welche die Volumen von personenbezogenen Daten, die sie sammeln, minimieren

- Ja  Nein

F) Organisationen, die Ihnen mehr Kontrolle über die Verwendung Ihrer persönlichen Daten gibt.

- Ja  Nein

Nächste

## Über Sie & Ihre Wahlmöglichkeiten

### D1 - Ihre Entscheidungen und Erfahrungen

A) Benutzen Sie Kundenkarten (Billa/Merkur Card, BIPA Card, Miles & More etc)?

- Ja  Nein

B) Haben Sie sich jemals etwas mit einer Kreditkarte im Internet gekauft?

- Ja  Nein

C) Sind Sie schon einmal durch die Sicherheitskontrollen am Flughafen gegangen / Wären Sie bereit, hindurch zu gehen?

- Ja  Nein

D) Ist Ihre Telefonnummer als "nicht im Telefonbuch eingetragen" aufgelistet?

- Ja  Nein

E) Lesen Sie die Datenschutzbestimmungen eines Unternehmens, bevor Sie deren Service in Anspruch nehmen?

- Ja  Nein

F) Haben Sie jemals die Daten überprüft, die Kreditprüfungsagenturen über Sie festhalten?

- Ja  Nein

G) Verstehen Sie voll und ganz, was Ihre Rechte in Bezug auf die Privatsphäre sind?

- Ja  Nein

H) Haben Sie jemals eine Verletzung Ihrer Privatsphäre erlebt?

- Ja  Nein

**D2 - Persönliche Informationen**

Die Beantwortung der folgenden Fragen ist freiwillig, sie würde aber unsere Forschung sehr unterstützen. Bitte beachten Sie, dass alle Ihre Antworten absolut vertraulich behandelt werden und die Analyse Ihrer Ergebnisse anonym durchgeführt wird.

A) Wie ist Ihr Beschäftigungsstatus?

Student  Berufstätig  Rentner  Arbeitslos  Andere

B) Wie hoch ist Ihr jährliches Haushaltseinkommen?

€0-20.000  €20.000-40.000  €40.000-60.000  €60.000-80.000  €80.000+

C) Haben Sie einen gültigen Führerschein?  Ja  Nein

D) Was ist Ihr Geschlecht?  Mann  Frau

E) Haben Sie Kinder?  Ja  Nein

F) Was ist Ihr höchster Bildungsabschluss?

Keiner  Hauptschule  Matura  Bachelor  Master/Mag./DI

G) Was ist Ihre ethnische Herkunft? (z. B. österreichisch / türkisch / kroatisch / chinesisch etc)

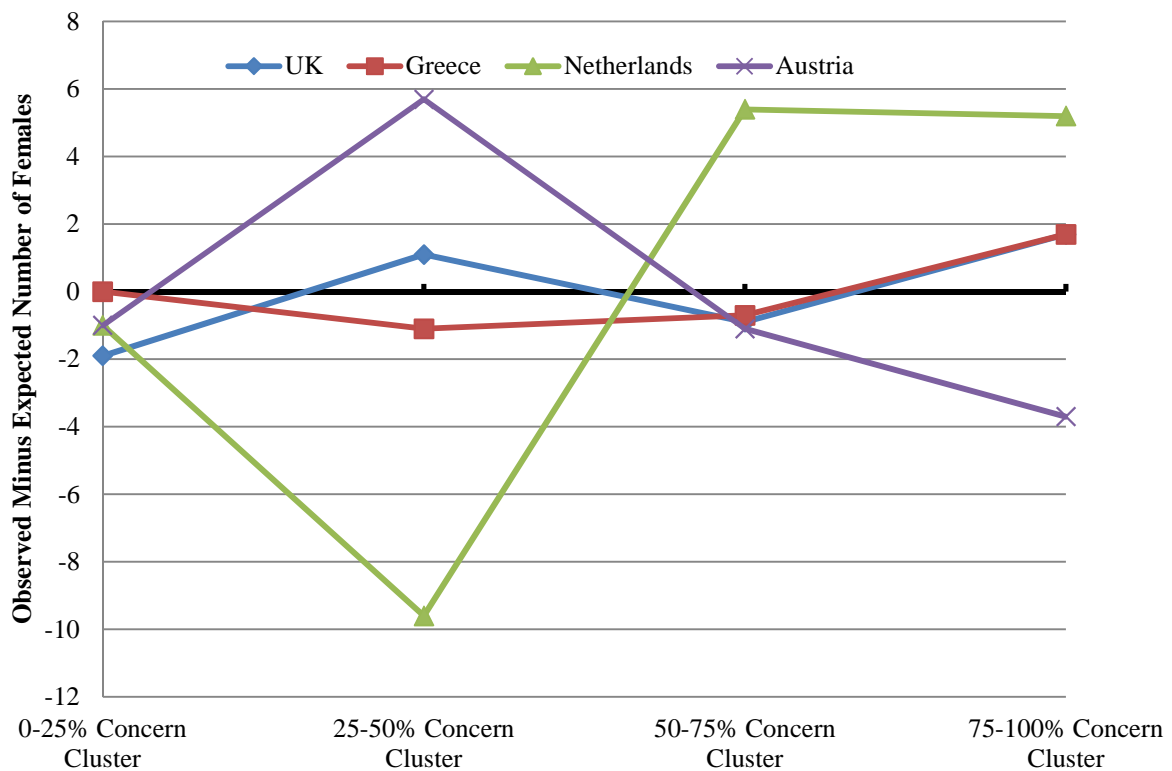
H) Wie alt sind Sie?

I) Wie ist Ihr Familienstand?

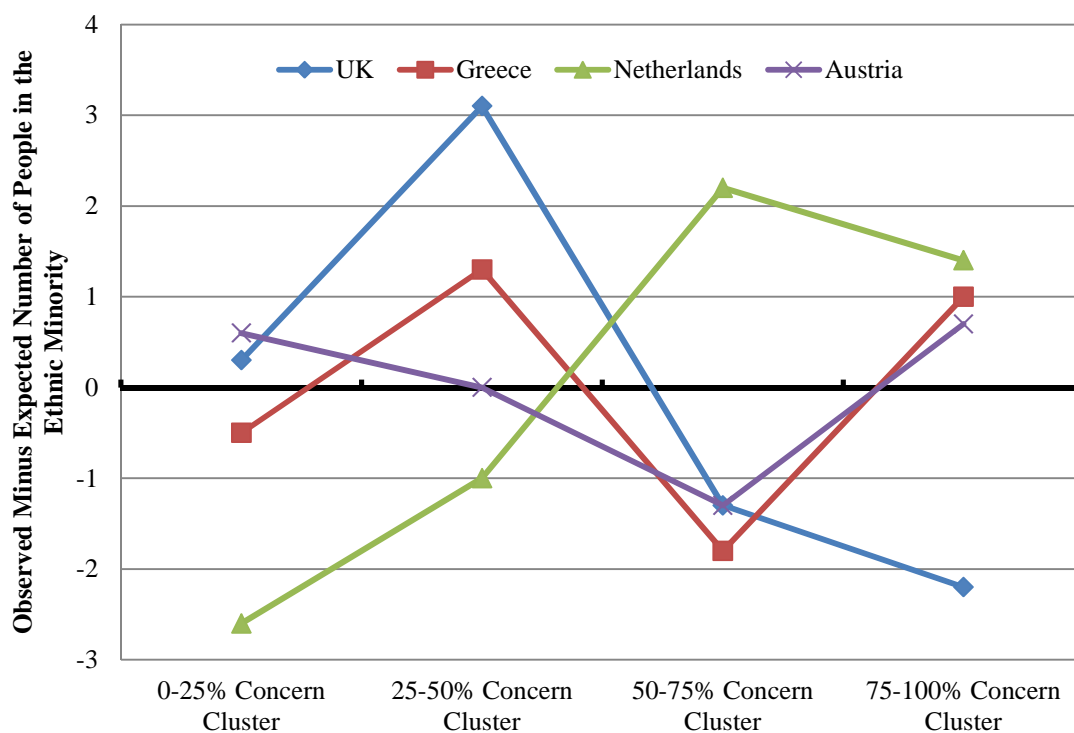
**Vielen Dank für Ihre Zeit!**

## Appendix F – Level of Concern Split by Country and Other Demographics

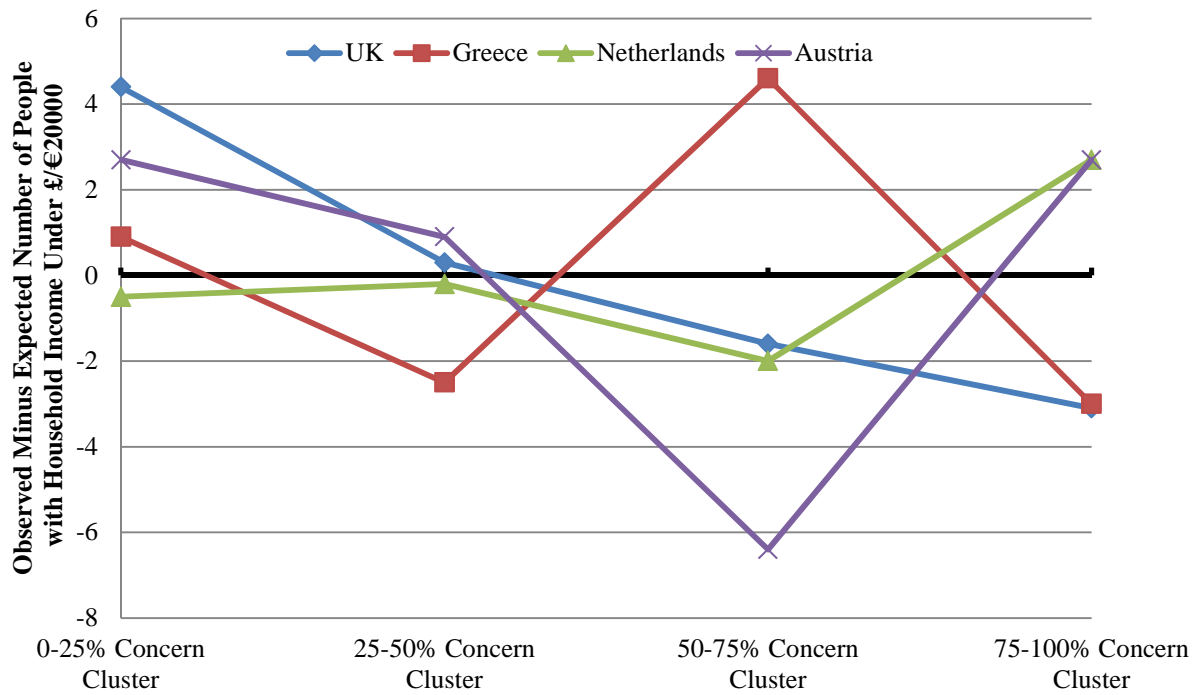
Observed Minus Expected Number of Females by Concern Cluster and Country



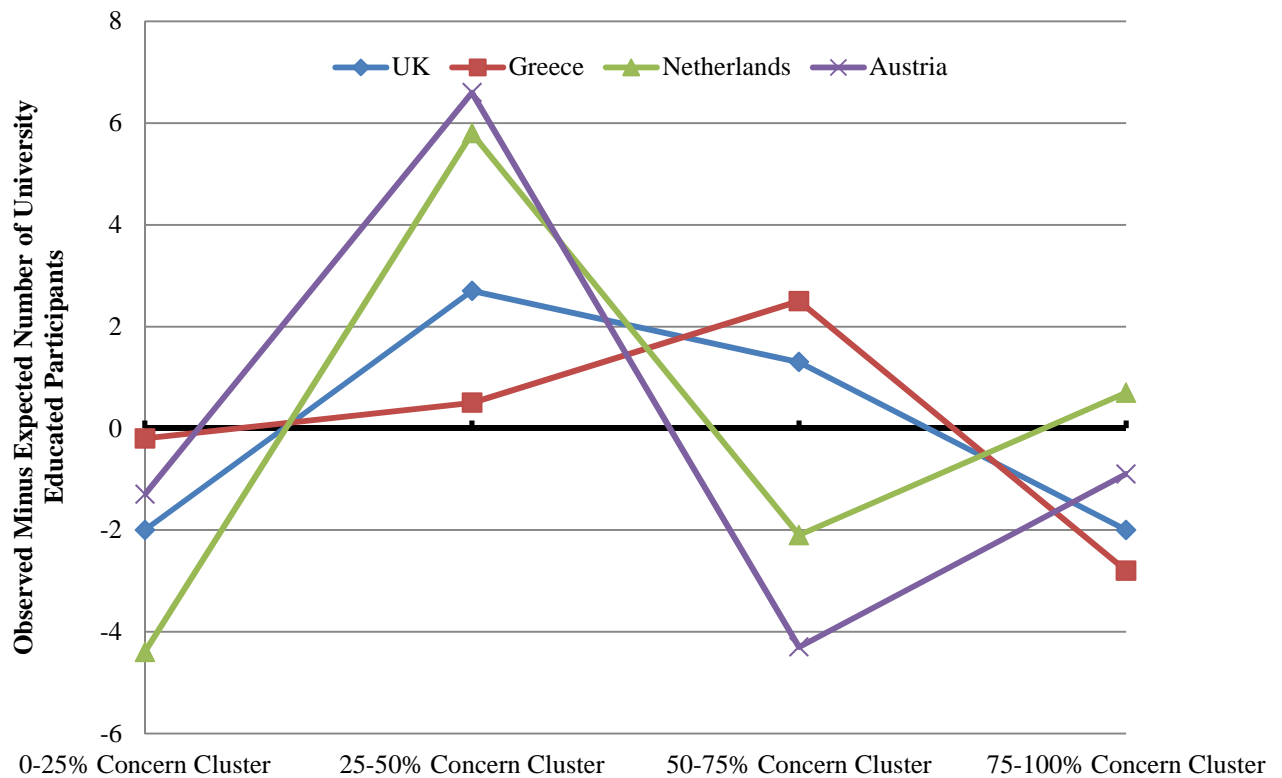
Observed Minus Expected Number of People in the Ethnic Minority by Concern Cluster and Country



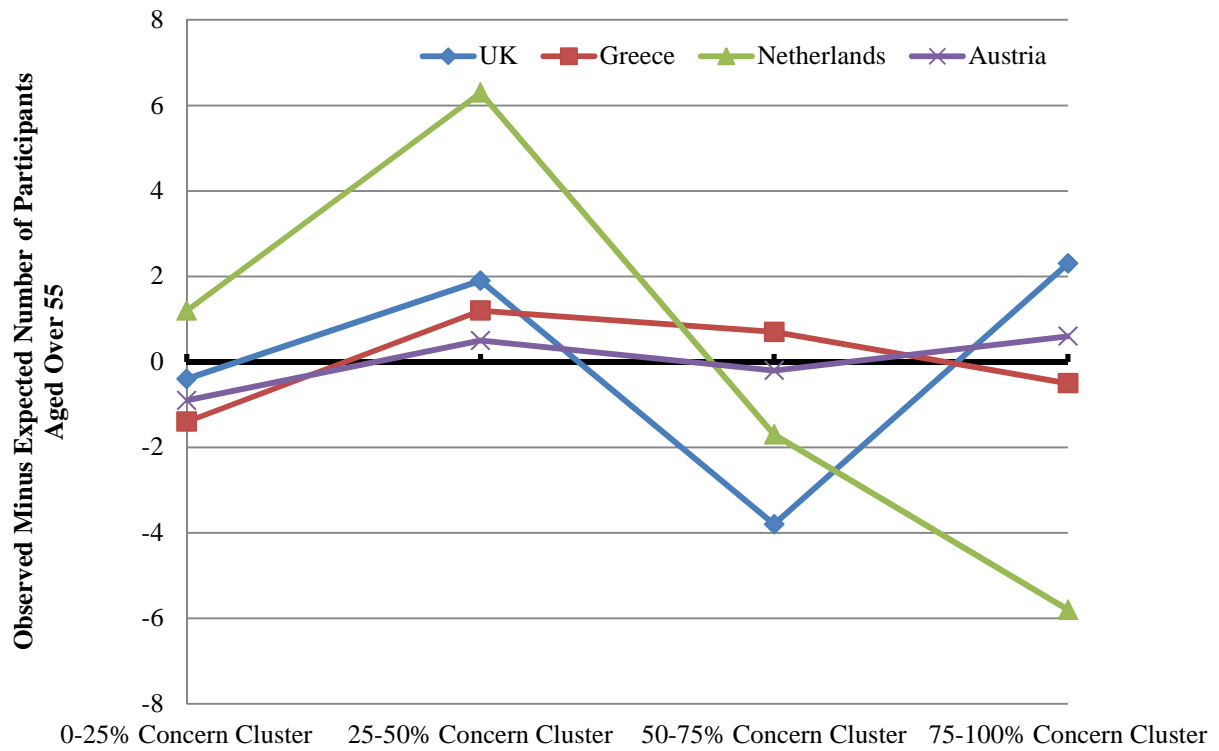
**Observed Minus Expected Number of People with Household Income Under £/€20000 by Concern Cluster and Country**



**Observed Minus Expected Number of University Educated Participants by Concern Cluster and Country**



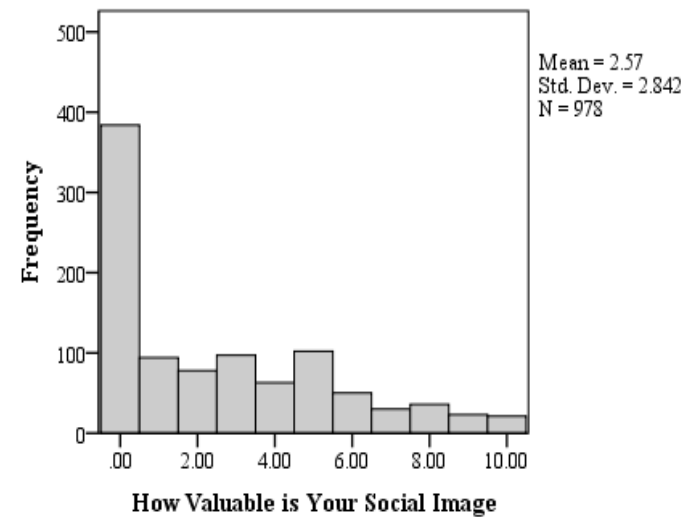
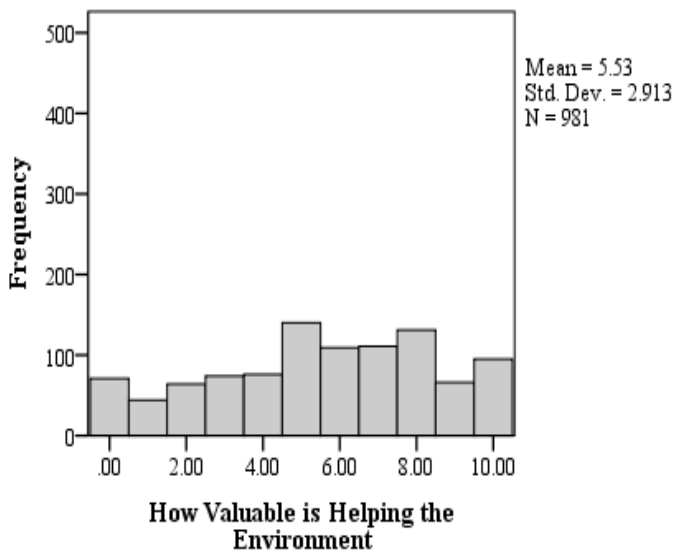
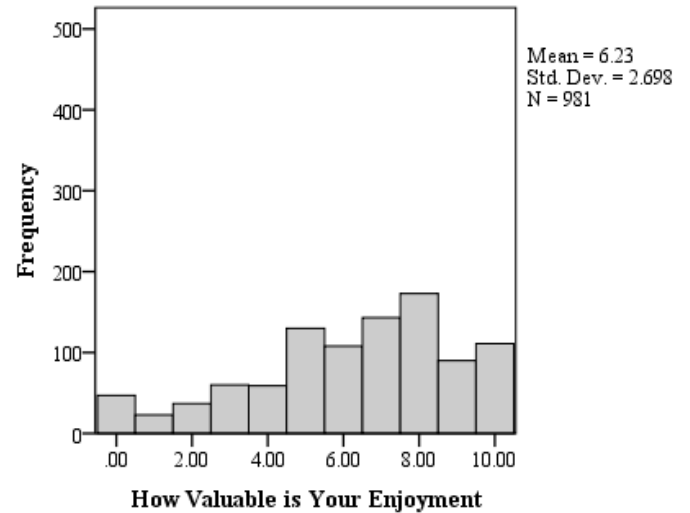
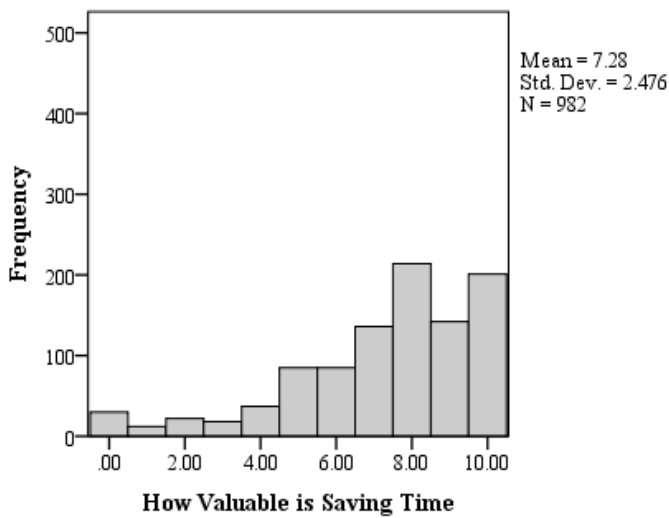
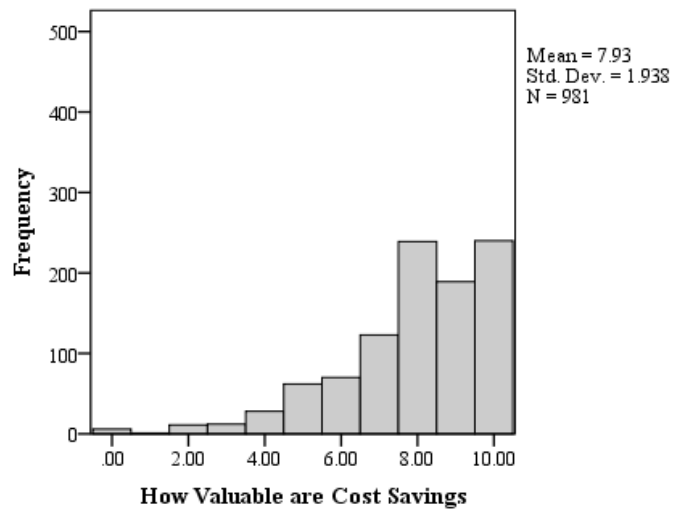
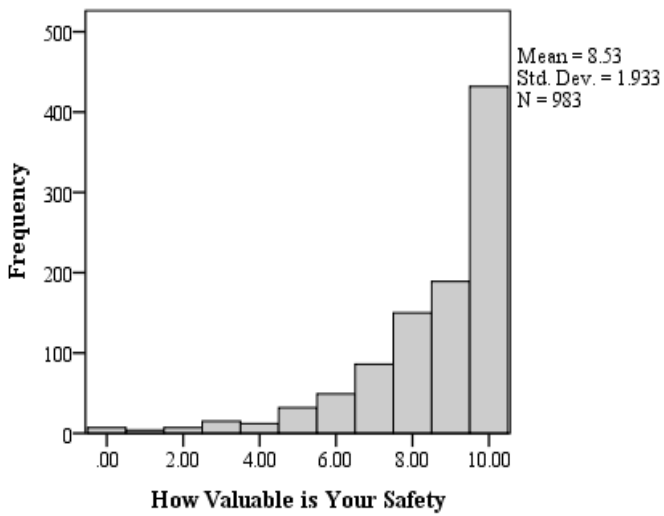
Observed Minus Expected Number of Participants Aged Over 55 by Concern Cluster and Country





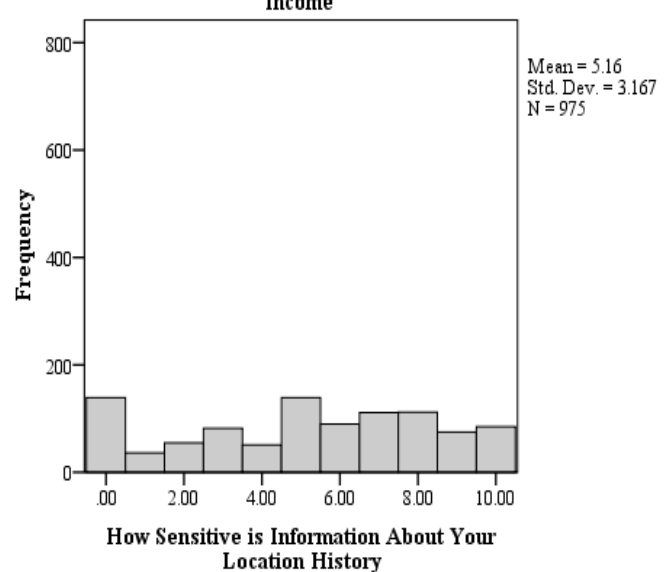
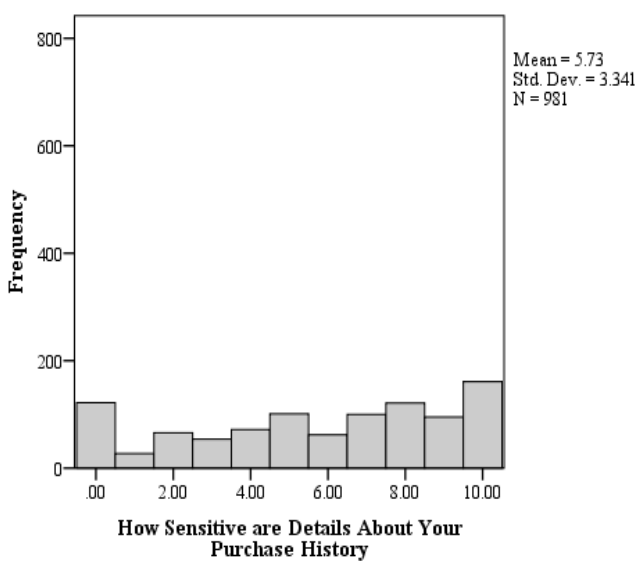
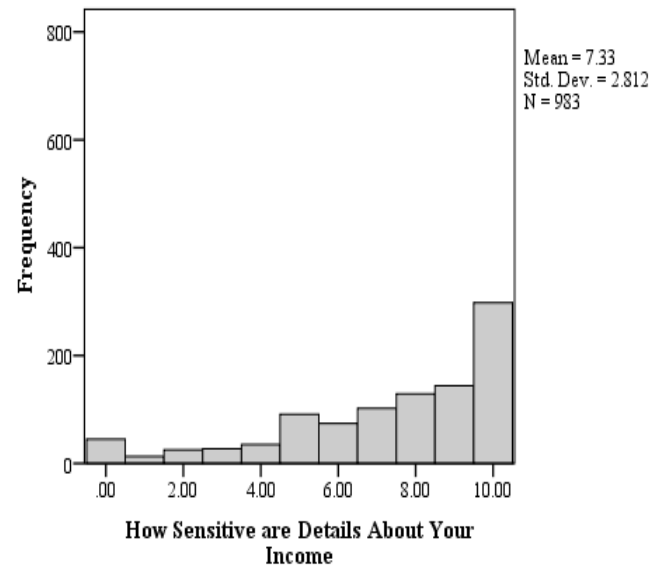
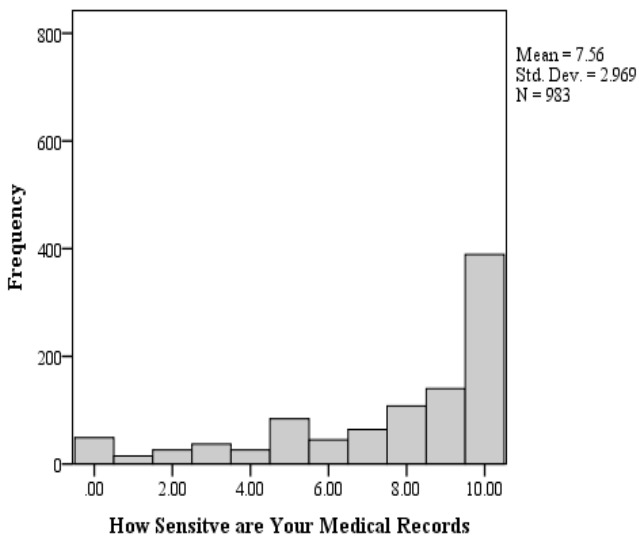
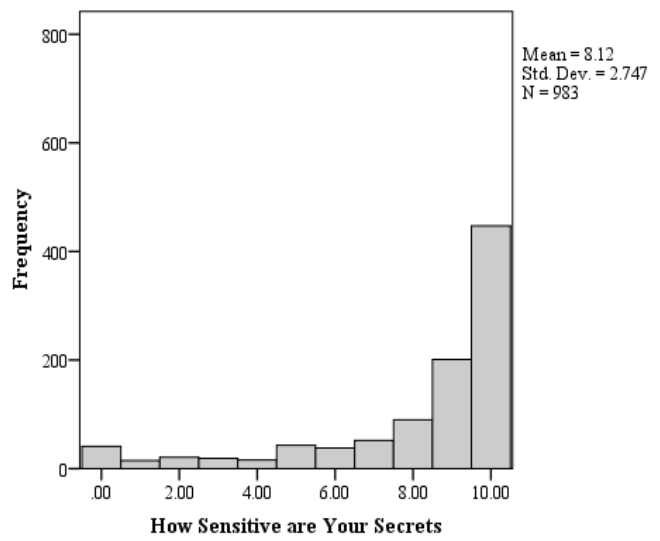
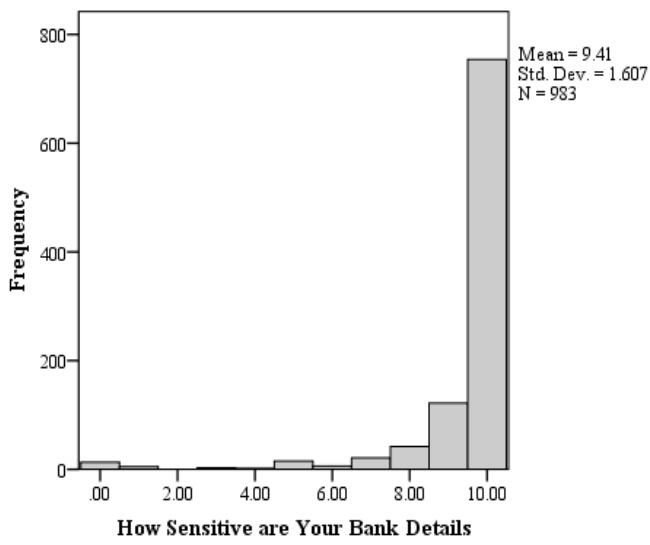


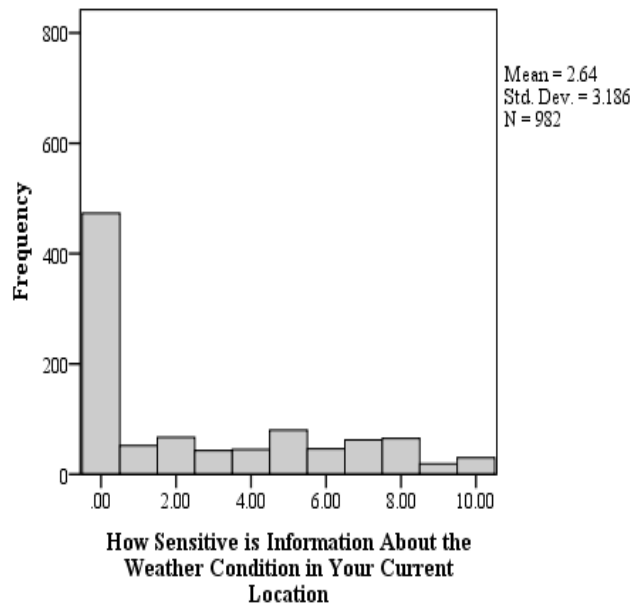
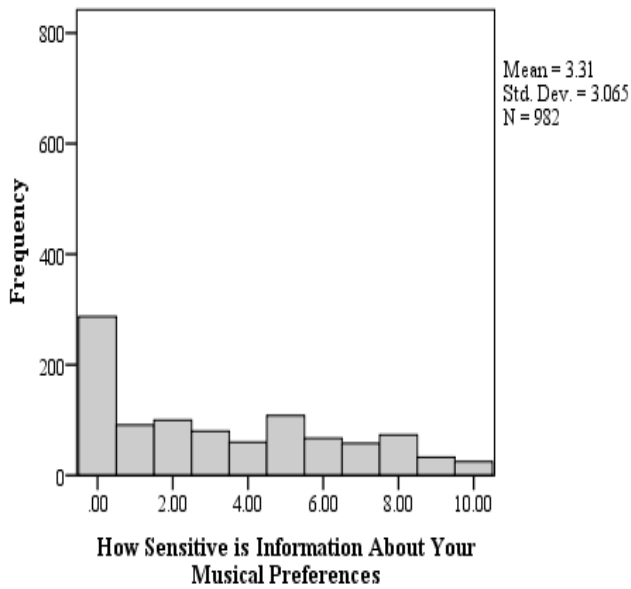
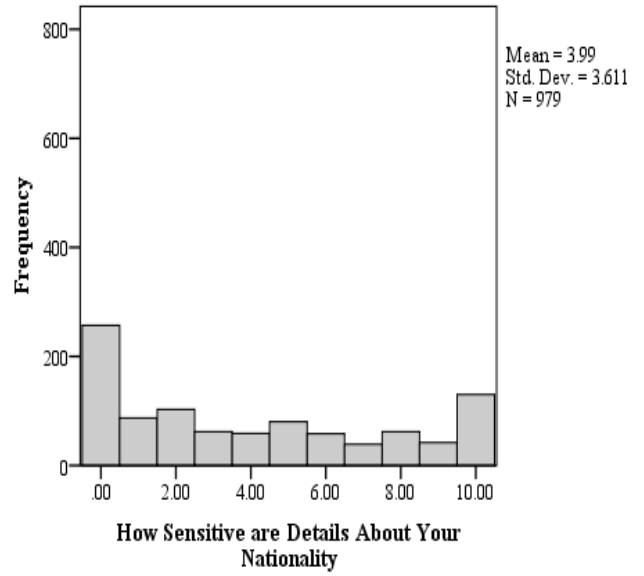
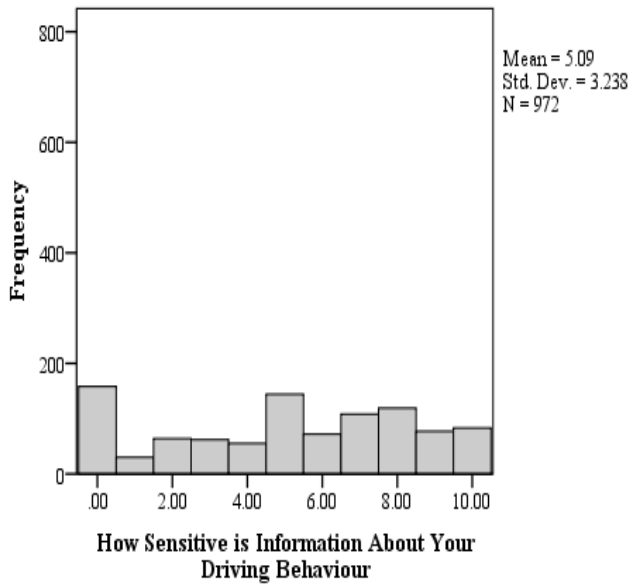
**Appendix G – Perception of Individual Rewards**



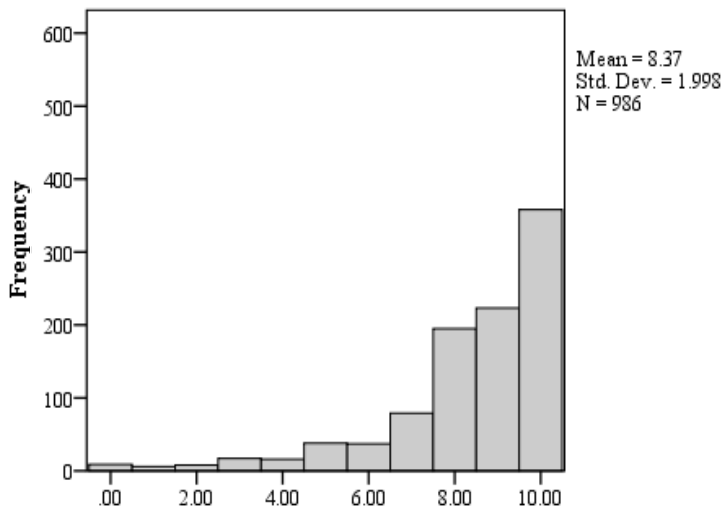


**Appendix H – Sensitivity of Individual Data Types**

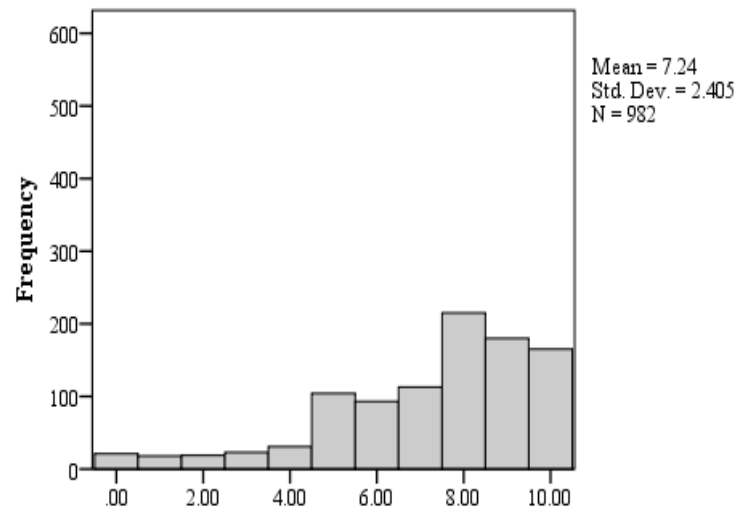




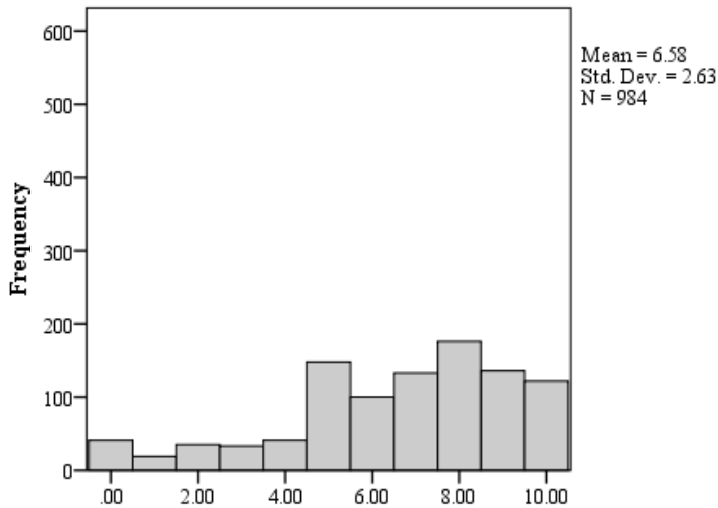
Appendix I – Trust in Individual Data Holders



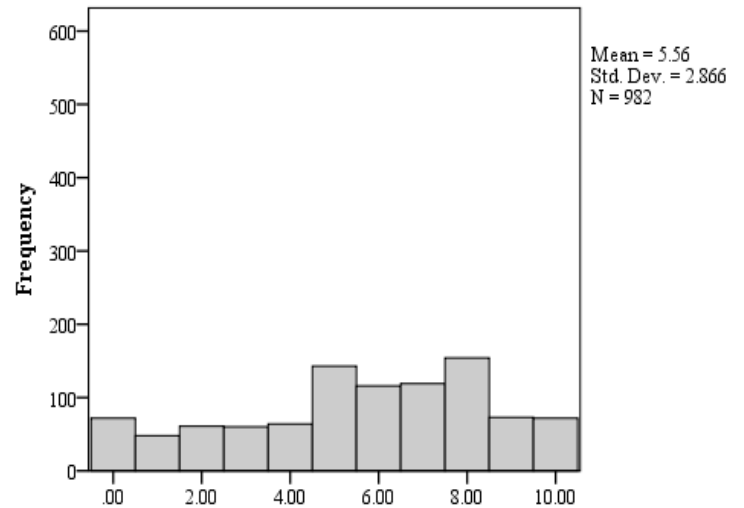
Level of Trust in Family Member



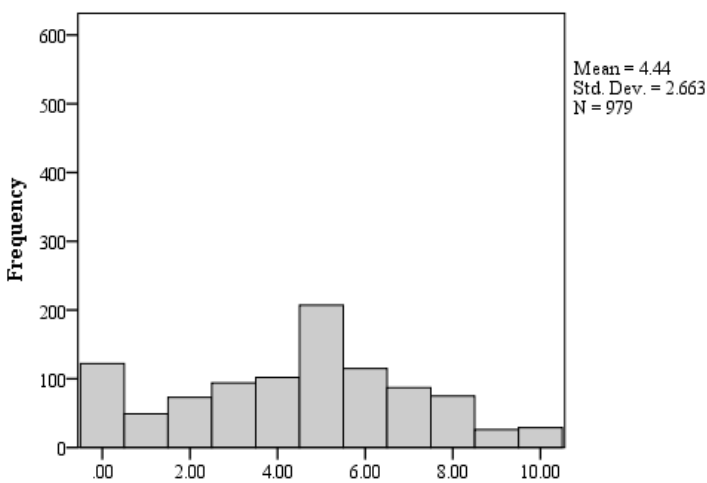
Level of Trust in a Close Friend



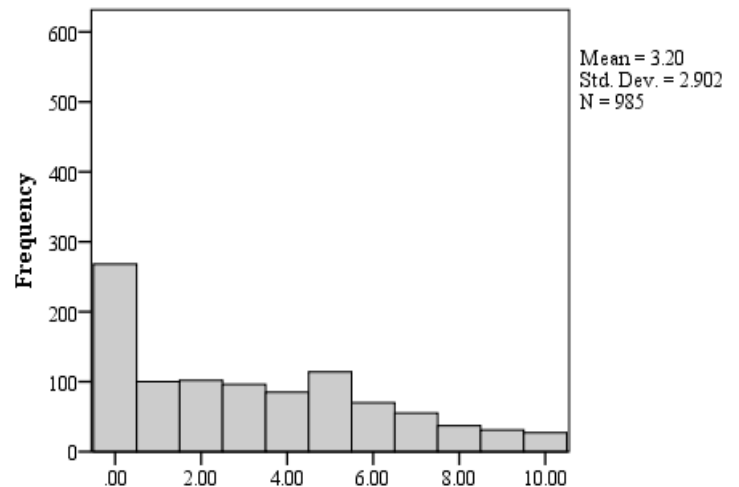
Level of Trust in a Medical Professional



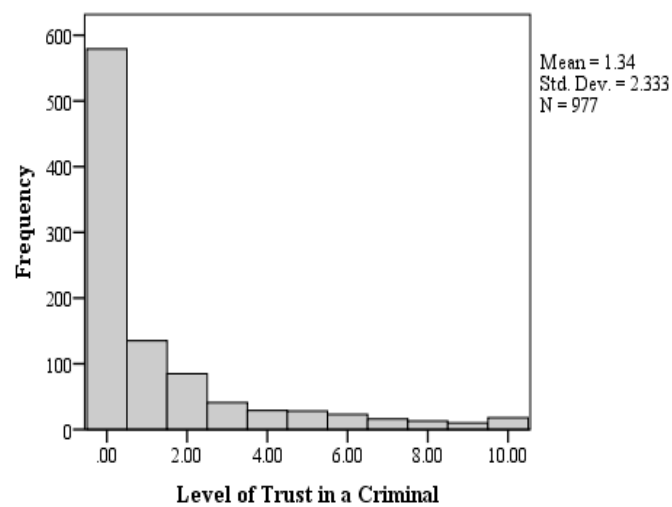
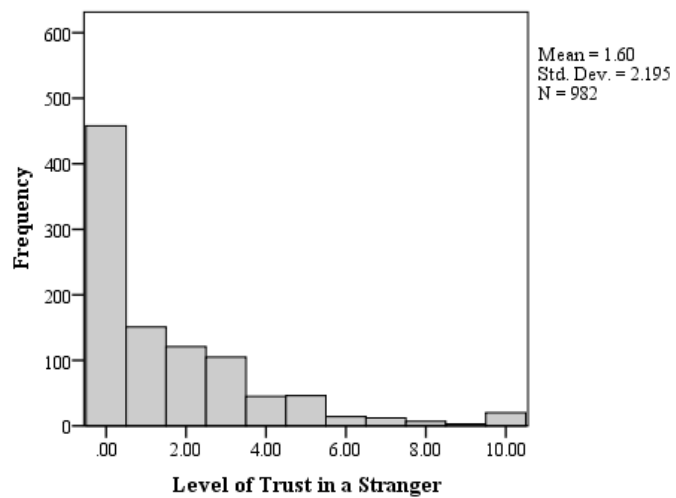
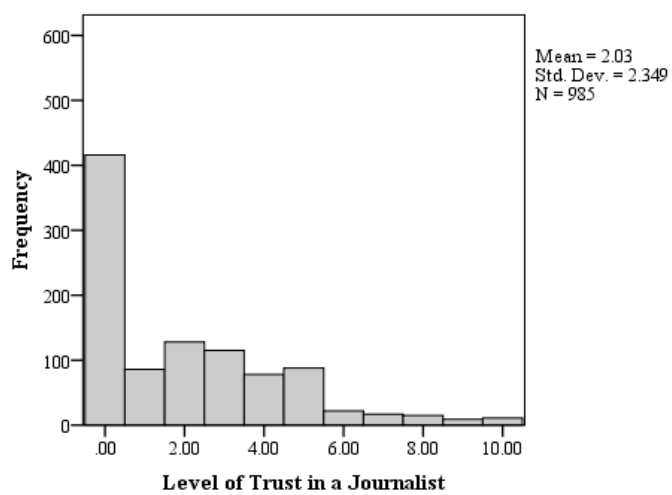
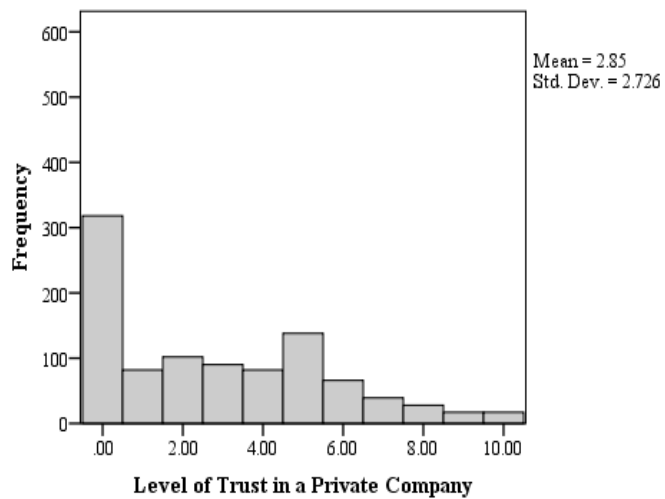
Level of Trust in a Legal Professional



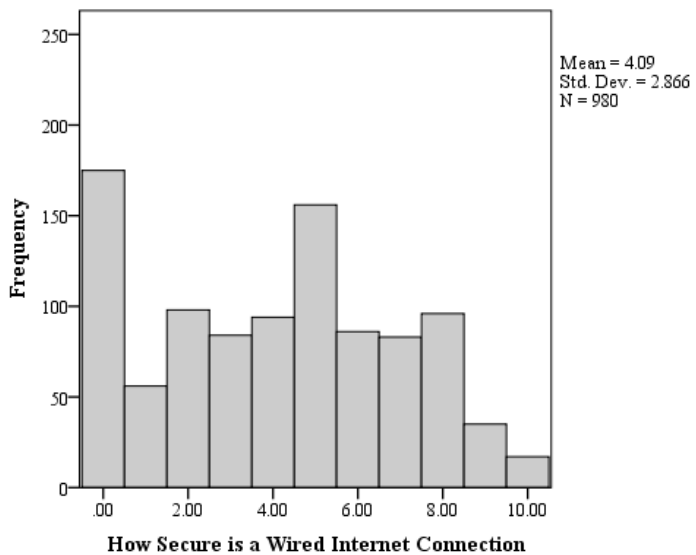
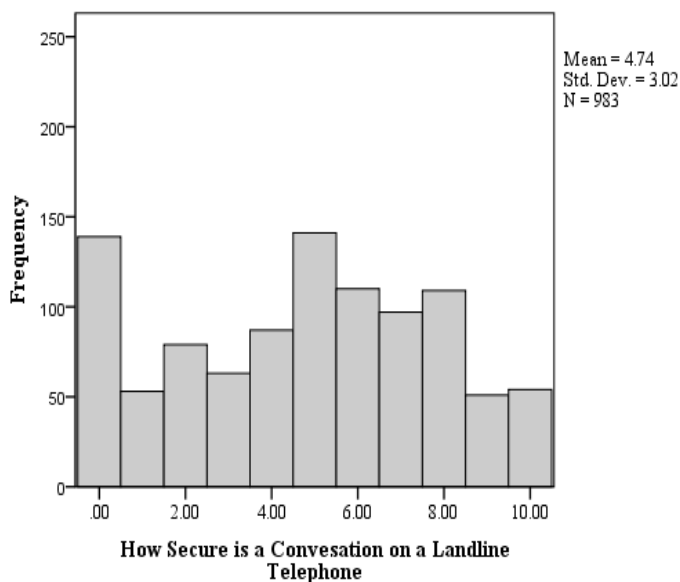
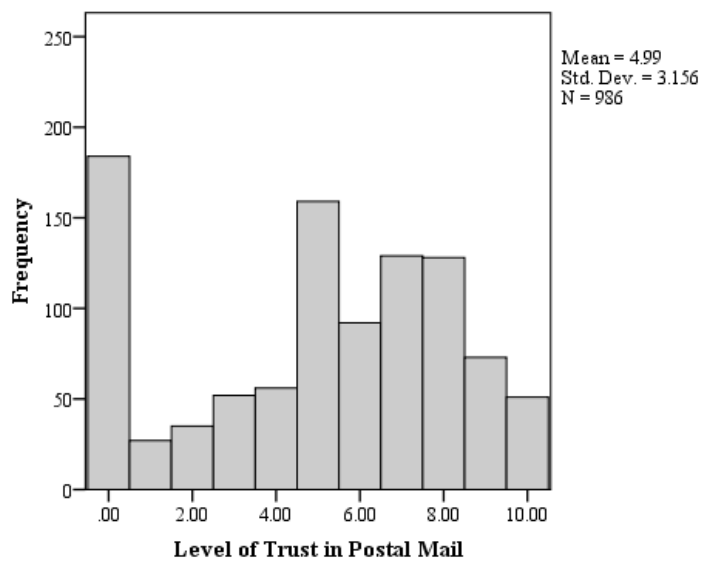
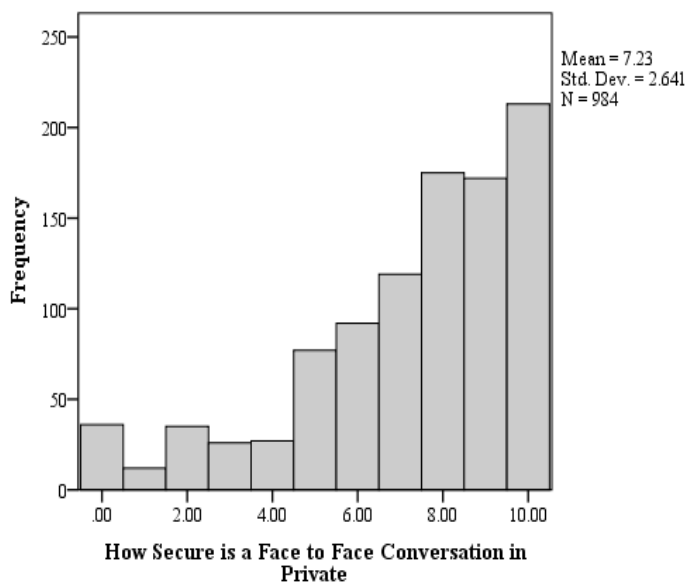
Level of Trust in a Work Colleague

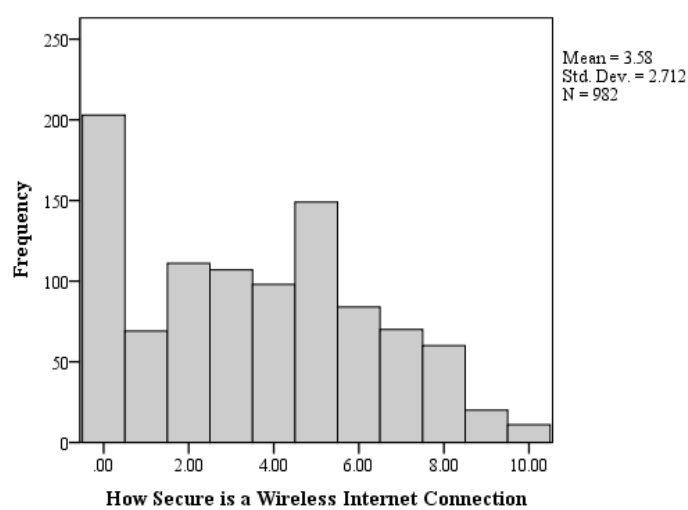
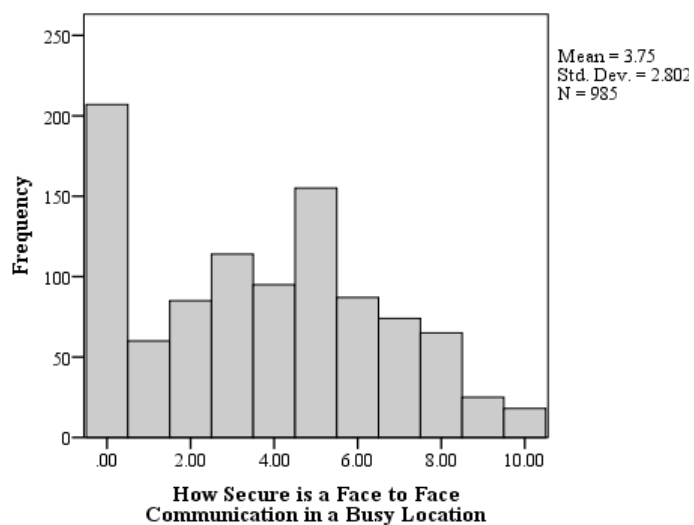
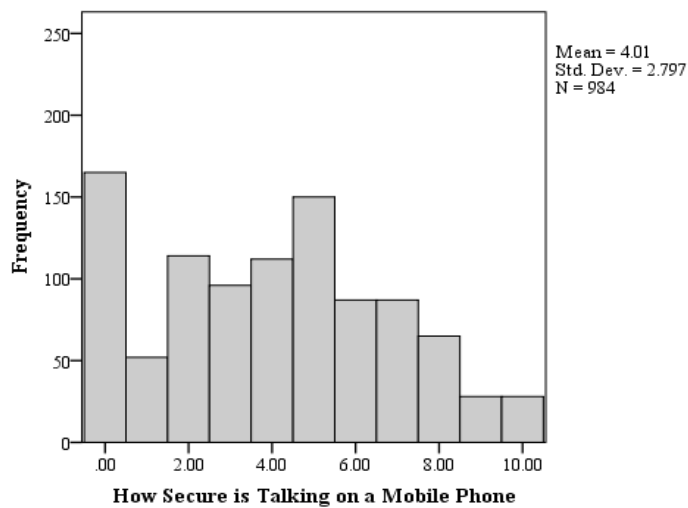
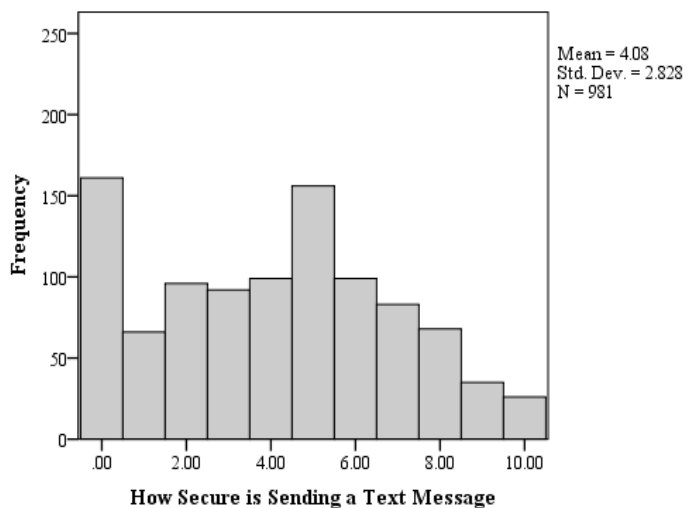


Level of Trust in the Government



**Appendix J – Trust in Individual Transfer Methods**







### Appendix K – Dendrogram of Number of Acceptable ITS Scenarios

