This product is part of the RAND Corporation technical report series. Reports may include research findings on a specific topic that is limited in scope; present discussions of the methodology employed in research; provide literature reviews, survey instruments, modeling exercises, guidelines for practitioners and research professionals, and supporting documentation; or deliver preliminary findings. All RAND reports undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

TECHNICAL
REPORT

Security, At What Cost?

Quantifying people's trade-offs across liberty, privacy and security

Neil Robinson, Dimitris Potoglou, Chong Woo Kim,
Peter Burge, Richard Warnes

Sponsored by the RAND Europe Board of Trustees

RAND EUROPE

The research described in this report was sponsored by the RAND Europe Board of Trustees.

Published 2010 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
Westbrook Centre, Milton Road, Cambridge CB4 1YG, United Kingdom
RAND URL: http://www.rand.org
RAND Europe URL: http://www.rand.org/randeurope
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Preface

The heightened security environment in the United Kingdom today is resplendent with examples of government policy that must strike a delicate balance between strengthening security without jeopardising public liberties and personal privacy. The introduction of national identity cards and biometric passports, the expansion of the national DNA database and cross-departmental sharing of personal data raise a number of privacy issues. Human rights may also be suspended by the exercise of stop-and-search powers by the police or detention of suspects prior to a trial. However, much of the current civil liberties versus security debate is adversarial and little robust research informs these arguments. This report outlines the results of a study that sought to understand objectively the real privacy, liberty and security trade-offs of individuals, so that policymakers can be better informed about individuals' true preferences in this area, and the true nature of the balance between privacy and civil liberties may be understood.

RAND Europe is an independent not-for-profit policy research organisation which aims to improve policy and decision-making in the public interest, through research and analysis. RAND Europe's clients include European governments, institutions, non-governmental organisations and firms with a need for rigorous, independent, multidisciplinary analysis. This study was conducted with internal investment from the RAND Corporation. This report has been peer reviewed in accordance with RAND's quality assurance standards.

For more information about RAND Europe or this document, please contact:

Neil Robinson
RAND Europe
Westbrook Centre
Milton Road
Cambridge CB4 1YG
United Kingdom
Tel. +44 1223 353329
Email: Neil_Robinson@rand.org

Dimitris Potoglou
RAND Europe
Westbrook Centre
Milton Road
Cambridge CB4 1YG
United Kingdom
Tel. +44 1223 353329
Email: Dimitris_Potoglou@rand.org

Contents

Table of figures

Table of tables

Summary

The right to life and right to privacy are established in a number of articles of the European Convention on Human Rights 1953, the UK Human Rights Act 2000 and the Data Protection Act 1998. Individual rights and freedoms include, for example, the right to a private life, the right to a fair trial and the right to freedom of assembly.

Policymakers and politicians present an urgent case for reconciliation of these rights in favour of security which has become specifically acute in recent times, given the markedly different nature of the terrorist threat now faced by the UK.

Civil libertarians often argue that consistently undermining these rights harms society, these measures are ineffectual and security objectives may be achieved via existing policy instruments.

There are numerous examples of where these two factors affect each other. These include the case of the monitoring of European citizens' financial transactions via the Society for Worldwide Interbank Financial Transfers (SWIFT) network; the mistaken shooting of Jean Charles de Menezes in London's Stockwell tube station in 2005, and the mistaken imprisonment of the Guildford Four in 1975.

Often, the interplay between these factors is characterised in terms of a balance between privacy or civil liberties and security.

Nonetheless, policymakers must weigh competing issues when deciding what and how to implement security policy, balancing these concerns in order to achieve certain broader security objectives without unnecessarily and disproportionately infringing human rights. They must take on board intelligence, information and data on threats and vulnerabilities in order to determine where, and to what extent, security investments should be made to offset the likelihood of these threats being realised against certain vulnerabilities. Such inputs may be in qualitative or quantitative terms, but most often are based on qualitative data from experience, professional judgement or historical precedent. In addition, identifying what constitutes the most effective security solution is challenging. Often, taking into consideration data on the implications of failure of security measures focuses only on such consequences in terms of impact on human life (fatalities or injuries) or direct economic impact. Very often the economic, social or behavioural consequences of security investments are not considered. While the consequences of the imposition (or not) of security measures on reducing predicted fatalities or injuries may be determined, this is not interpreted in a way that can be assimilated easily into decision-making by the security community. Such approaches are already common in health and social care policy settings.

However, economic appraisal of the value of fundamental rights such as liberty, privacy (or even a right to life) causes controversy amongst policymakers who traditionally have approached this from a legal perspective. Ultimately the challenges with current approaches revolve around the need to decide whether and how the views of the users of the security infrastructure may be accommodated in such decision-making, and to understand the long-term economic, social and behavioural consequences of the imposition of these security infrastructures upon individuals.

Existing attempts to provide an evidence base for understanding the preferences of users of security measures is largely based on opinion polls, surveys or qualitative research, each of which has its limitations because they only permit an absolute 'Yes/No' response to questions, and generally are not conductive to represent the instances in which an individual may be faced practically with a series of realistic choices which may have different effects on their privacy, liberty or security. Recent examples include the Westin-Harris Privacy surveys, a Gallup Organisation Flash Eurobarometer survey conducted for the European Commission; a British Social Attitudes Survey and tracking research conducted for the Home Office National Identity Scheme. However, these approaches suffer from three main challenges:

1 they are generally one-dimensional and thus unrealistic – they ask abstract, one-off questions that lead respondents to maximise but not satisfy their needs in terms of privacy, liberty or security, unrealistically indicating support for maximum security with minimum intrusion on privacy and liberty;
2 they do not quantify the extent to which people may be prepared to give up civil liberties or privacy. Surveys and opinion polls do not attempt to answer the question: 'By how much are people willing to give up their civil liberties to gain a potential security benefit?'
3 they cannot be integrated easily into an economic appraisal toolkit – it is difficult for the data gained from such surveys to be integrated easily into formal cost–benefit analysis.

The use of stated preference methods is one such avenue to address the deficiencies in such approaches. The use of stated preference methods to examine the trade-offs that people are prepared to make across liberty, privacy and security may allow a bottom-up and refined understanding of the importance that people place on these factors, which often are seen as competing or diametrically opposed. The objectives of this study are to answer the following types of question.

- Given that national security is a form of non-market public good, does the use of stated preference[1] techniques for gathering data on the trade-offs that people are willing to pay have merit?
- What drives choice when individuals decide to relinquish or surrender their liberty or privacy to obtain security benefits?

[1] Stated preference techniques aim to see how people respond to a range of choices and thus to establish collective willingness to pay for a particular benefit (or their willingness to accept payment in exchange for bearing a particular loss)

- Is it possible to monetise the trade-offs between security measures and liberty and privacy?

Methodology

Our research methodology focused on applying stated preference techniques to the challenge of trying to understand and quantify the trade-offs that people may make when confronted with choices about their privacy, security and liberty. We began by conducting a literature review on the topic. Following from this, we conducted three semi-structured interviews with proponents of all sides of the security–civil liberties debate. Finally, we devised a set of choice contexts in which we might present the experimental methodology, in order to circumvent the difficulties of dealing with abstract and difficult to define concepts with respondents. These were:

- applying for a passport;
- travelling on the national rail network;
- attendance at a major public event.

Case studies

Applying for a passport

Under current UK policy, the process of applying for a passport has become an event where concerns over privacy and civil liberties, set against the larger requirements of national security, have come to the fore. Citizens are expected to submit a significant quantity of personal data with their passport application on the current declared reason that doing so helps in the fight against a number of social 'bads', such as illegal immigration, terrorism and so forth. The conflict of privacy and liberty set against security is relatively abstract in this case, since it concerns aspects of what experts call 'informational self-determination' rather than any perceived immediate threat to the person. Our study has shown that in general, individuals are willing to submit their data for these purposes, except where this might be circulated more widely.

The data from this experiment indicated a universal degree of discomfort in the provision of advanced forms of biometric information, such as DNA, as part of the process of passport application. Respondents were only willing to accept (i.e. they derived negative utility from) the collection of DNA and photograph data at the point of application for a passport if there was a subsidy of £19 on the cost of a passport. A photograph and fingerprint was regarded commonly as preferable type of personal information to be provided, and respondents indicated a willingness to pay £7 for providing this data. This finding is relevant, given recent policy statements which indicate that fingerprint data will be collected as part of the application process (ZDNet, 2009). By contrast, as recent reports indicate, there is no requirement to submit further biometric information at present, since a facial biometric is compiled from the supplied photograph (Directgov, 2009a).

Rather more worryingly from a privacy perspective, there was universal discomfort identified with regard to the sharing of any personal data collected as part of the passport

application process with other organisations in the public or private sectors. As to the sharing of personal data, all else being equal, respondents preferred to see their personal data kept within the Identity and Passport Service, rather than sharing it either with other government departments, other European nations or the private sector. This has a number of important policy implications – most notably, whether the increasing desire to use such datasets by the public sector to achieve efficiencies or help in the fight against organised crime, illegal immigration and international terrorism matches with the preferences of the general public in this regard (Omand, 2009). Furthermore, there is the ongoing question over consent and choice and whether this may ever be construed as meaningful, given the extent of demand for passports.

The data illustrated that large incentives (e.g. a discount on the average price of a passport, perhaps as much as up to £30) would be required in order to reach a threshold where respondents would be comfortable in sharing their personal data with third parties. Respondents indicated that sharing information with the private sector was the least preferred alternative, and they would be willing to accept this only if the price of a passport was discounted by £30. For other European nations, a £23 subsidy would be required to elicit this being seen as an acceptable choice, and a subsidy of £16 to share this information with other parts of government.

Evidence from this case study appears clearly to contradict current government policy, particularly regarding the sharing of information contained in the National Identity Register (NIR), which may be collected as part of the passport application process, with other government departments as part of the 'identity assurance' policy agenda or the private sector. For example, it has been suggested that banks may wish to use the identity information in the NIR as a government-authenticated identity, removing the need for customers to present varying forms of credential when applying for a bank account (BBC, 2008a). Finally, in regard to sharing this information with other countries, the European Secure Identity Across Borders Linked (STORK) project (2009) between a number of EU Member States is evaluating methods to do just this, sharing identity information between Member States in order to deliver pan-European services such as the European Electronic Health Insurance Card (EHIC) (NETC@RDS Project, 2009). The existence of such compelling evidence regarding preferences suggests that policymakers ought to explore and consider the implications of this data and whether a subsidy is necessary, or at least the unintended consequences of the continued implementation of such policies that are contradictory to individual preferences.

Travel on the UK national rail network

Security mechanisms which may affect individuals privacy or civil liberties when travelling on the national rail network are viewed more enthusiastically by respondents. This may be due to familiarity: in contrast with sharing personal data in the passport case study, which is relatively abstract and distant, the security mechanisms present in this case, such as closed-circuit television (CCTV) and security arches, are much more physically present and perceptively 'closer' to the individual. This can be seen in the example of preferences regarding X-ray machines or a physical 'pat-down' and bag search; the latter being considered as more invasive, perhaps due to its physical intrusiveness. Despite this, the potential to exercise the right to privacy under this security measure may be less restricted

than when personal data is collected in passing through an X-ray arch, where data may be recorded, shared with others and stored for much longer, with little informational self-determination by the individual.

In relation to the second case study, individuals were comfortable with more intrusive types of security camera (with face-detection type technology) as they seemed to outweigh people's privacy and civil liberties concerns. Indeed, the extent to which this finding is representative of the oft-discussed 'surveillance society' is interesting, since it illustrates a degree of familiarity with privacy-invasive forms of technology such as CCTV cameras (Ball et al, 2006). However, there remains the question over the extent to which context plays a role, since people may have identified that in the precise and discrete environment of a railway station, being monitored by CCTV of any cause is an acceptable sacrifice to make to obtain security benefits. Similarly, the evidence may illustrate confusion about the perception that CCTV is a tool for detection of low-level street crime such as burglary, mugging or anti-social behaviour, rather than for dealing with more complex forms of criminal behaviour or international terrorism (Farrington and Welsh, 2007).

The findings regarding the degree of comfort attached to different types of security check were counter-intuitive. We anticipated that security checks which may have an obvious implication in terms of privacy would be less preferred than others with which individuals may be more familiar. However, the evidence illustrated that people were comfortable with the idea of passing through an X-ray arch or scanner, much more so than a pat-down or bag search. Understandably, these may be perceived as being more privacy-invasive due to the personal and physical nature of such searches, but by comparison, the data recorded in a metal detector or X-ray scanner in fact may adversely affect individuals' privacy in a broader fashion, being shared among more than one individual observing the images and potentially, recorded, stored and passed on. There is also the extent to which pat-downs and bag searches are more effective from a security perspective – historical evidence from the Israeli airline El-Al seems to indicate that alert, trained staff able to spot indicative signs of such behaviour may also prove to be an effective measure.

Finally, and somewhat unsurprisingly, there was a high degree of comfort expressed for more specialised security personnel, up to a point. Despite the perception in the security community that the deployment of armed police or the military creates a fearful atmosphere, in all cases the respondents were willing to pay for security personnel (there was no negative utility identified). Regarding the visible presence of uniformed military, as was seen for example at London Heathrow Airport in 2003 (The Times, 2003), most respondents were willing to pay for these measures (but less so than more 'low-key' forms of security personnel), and felt that their effectiveness was not correlated to the increasing levels of sophistication.

Attendance at a major public event

The public event scenario presents some similar characteristics regarding the security measures that may be implemented when travelling on the national rail network, but also aspects of what may be termed 'informational self-determination' regarding the use and control of personal data submitted upon entry that are similar to the passport scenario.

In the major public event case study, people preferred to have some form of identity check, but all else being equal, were less likely to pay for checks requiring biometric forms of personal data. Based on an expected ticket price of £40 for attendance at the opening ceremony of the Olympic Games, people would be prepared to pay £1.20 for a form of identity check of photographic ID and a check of the ticket. Forms of ticket check covering the use of biometric information (such as a fingerprint scan or iris scan) were less preferred, as individuals would be prepared to pay slightly more than £1 (£1.02) for these forms of identity check. This may be explained by the acceptance that it would be necessary to check the identity of the person presenting the ticket, in order to make sure that they were a legitimate ticketholder. The more interesting finding is that despite widespread media reported concern regarding the potential imposition into civil liberties that such technology might bring, individuals were still willing to pay for these intrusions into civil liberties to achieve security objectives. This is reinforced by the finding that respondents would be willing to pay less (£0.72) for a simple ticket check involving no check of identity information than for forms of ticket check involving some kind of personal or biometric information. This evidence is relevant, given continued discussions over what security technologies might be used to administer entry to Olympic events, with the Olympic Delivery Authority indicating that it would consider the use of 'facial and palm' biometrics for workers at the Olympics site (The Times, 2009).

In addition, the evidence from this part of the experiment indicated that people would be willing to pay more – between around £0.54 and £0.62 on the average likely price of a ticket (£40) (London Organising Committee of the Olympic Games, 2005) – for more specialised forms of security personnel, such as uniformed police or even armed police or military. Interestingly, the efficacy is perceived to be lower, compared to other security interventions. This evidence confirms the belief held by those in the security community, especially the police, that a visible police presence goes a long way to reassuring the public in crowed places. However, there is continued debate as to whether, from a security perspective, this is the most effective use of personnel for this specific context – indeed, the implementation of new 'behind-the-scenes' systems such as control rooms, aerial surveillance (e.g. via helicopter-based aerial support units) may represent better value for money in terms of achieving security objectives.

Conclusion

Our work has shown that it is possible to obtain and quantify the views and preferences of citizens as users of security infrastructure. In some cases we have demonstrated that it is also possible to monetise them, and that this would be valuable if conducted in a focused context.

This data may be used as another information source to support consideration of security investment decisions, when balancing the likely risk of an incident versus the costs and implications of the implementation of security infrastructure to mitigate this risk.

Our study can shed light on where policy and preferences differ, and thus can support policymakers and those deploying such security infrastructure to take informed, evidence-based decisions as to whether the cost of contravening or ignoring these preferences

outweighs the benefit that may be brought from implementing such measures. Similarly, it might be possible to identify where measures might be adjusted to take better account of preferences without undermining any security gains.

Finally, data such as the application of our methodology can provide can bring a degree of objectivity into a highly-charged and emotive debate, particularly when policy discussion turns to talk of 'finding the right balance' between civil liberties and security. Ultimately, this study has shown that use of the metaphor of balance is counterproductive without robust measurement of the weight of each factor to be balanced.

Acknowledgements

We would like to thank the RAND Corporation, as without their support this innovative study would not have been possible, and the RAND Europe Board of Trustees for selecting this study as their 2008 project. During the course of this project we interviewed a number of experts: Gareth Crossman and Jago Russell from Liberty, Gus Hosein from Privacy International, and Peter Clarke, the former coordinator of Counter-Terrorism Command for the Metropolitan Police. We would like to extend our gratitude to them for their candid responses to our questions.

In addition, we would like to extend our thanks to the participants of our internet panel and the staff of Research Now, most notably Andrew O'Connell and Christina Fox, for the administration of the experiment. Finally and most importantly, we would like to extend our thanks to a number of RAND Europe staff members, most notably Jonathan Grant, Hans Pung, Charlene Rohr, Lindsay Clutterbuck, Greg Hannah, Constantijn van Oranje, James Fox and Lorenzo Valeri, for their thoughtful and helpful comments during the conduct of this project and preparation of this report.

CHAPTER 1 Introduction

In the existing security climate in the United Kingdom, difficult public policy decisions often have to be made regarding the broader security of the public versus individual freedoms and liberties. This range of policies include the introduction of a national identity (ID) card programme, the growing use of technology which might adversely affect privacy (e.g. closed-circuit television, CCTV), and policies designed to provide for public security, for example, the UK Government's counter-terrorism strategy and associated pieces of legislation, such as section 44 of the Terrorism Act 2000, the Anti-Terrorism, Crime and Security Act 2001 and the Terrorism Act 2006. The public debate surrounding these decisions often characterises this process as finding "a balance between security and liberty" (e.g. The Guardian, 2006; The Daily Telegraph, 2007). This debate is highly polarised, with those from the civil liberties community strongly arguing against any infringement of privacy and liberty, and those from the security and policy community arguing that in many cases, the end justifies the means. Public policymakers have processes for security investment which is performed on the basis of internal decision-making using a comprehensive risk management framework. This includes consideration of the impact upon human life and cost to the economy. Despite these, there exists limited research into understanding the real privacy, liberty and security trade-offs that people make.

The aim of this project is to make a contribution to such a body of work using a robust evidence base, sparking a wider policy debate about whether government should take note of real privacy, liberty and security trade-offs in their policymaking.

1.1 Individual rights and freedoms

In the UK, the Human Rights Act 1998 gives further effects to those rights set down in the European Convention on Human Rights and Fundamental Freedoms 1953 (ECHR) and associated European Court of Human Rights case law. There are a number of rights set out in this Convention, but of most interest are the following (ETS 155, 1998):

- Article 2 – the right to life;
- Article 3 – prohibition of torture;
- Article 5 – the right to liberty and security;
- Article 6 – the right to a fair trial;
- Article 8 – the right to respect for private and family life.

In actuality, few of these rights are absolute. Specific allowance is made to abrogate temporarily or suspend these rights for a variety of recognised aims, including:

- national security;
- public safety;
- public health or morals;
- prevention of public disorder or crime;
- protection of the rights and freedoms of others.

These rights have been elaborated in various decisions from the European Court of Human Rights. Article 15 also provides for the derogation of certain rights in time of emergency, under a series of strict tests that any measures requiring the suspension of these rights must: be necessary in a democratic society, fulfil a pressing need; serve a recognised aim; be proportionate to the need; be prescribed by law and conform to democratic values of pluralism, tolerance and broad-mindedness (Klug et al, 1996).

1.1.1 The case for reconciliation of these rights in favour of security

The model of the compromise of these rights to obtain certain benefits is not new. The philosopher Thomas Hobbes argues in *Leviathan* that in order to gain security individuals enter into society, giving up in the process some of the freedoms inherent in a state of nature. Niccolò Machiavelli's *The Prince* introduces the idea that measures may be found necessary to preserve the state, even if this means severely curtailing the freedoms of individual citizens.

In the UK, recent official statements describe the ways in which these rights may be abrogated or suspended, either permanently or temporarily. Examples include various speeches by officials and ministers regarding the extension of the period of pre-trial detention, the benefits of the national identity register in addressing terrorism and illegal immigration, the utility of CCTV for identification of suspects, and so on (e.g. Brown, 2008).

Suspension of these fundamental rights is viewed as necessary, particularly in the current security context, due to the complexity of identification of terrorist and serious criminal activity. To illustrate this, it is possible to compare the response of the security and intelligence community to Irish republican terrorism in Great Britain in the 1970s and 1980s with the response to global jihadist terrorist activity in the late 1990s and early part of the 21st century. When dealing with Irish republican terrorism, its predictability and politically-driven nature meant that the security authorities could spend time collecting evidence and building a comprehensive case prior to the arrest of a suspect. However, with newer forms of terrorism such approaches are less viable. This is due to the following.

- The ideological, extremist and suicidal nature of international jihadist terrorism forces the security authorities to consider and prioritise the avoidance of mass casualties, meaning that suspects may be detained as a result of intelligence about an imminent attack, but then evidence and a robust trial case must be then built *ex post* – that is, after their detention.

- The global, networked and highly complex nature of international jihadist terrorist threats presents challenges to evidence collection and development of a case. The broad use of internet and communications technology by jihadist terrorists also complicates matters, meaning that developing enough evidence to secure conviction of a suspect may require considerable time and resources, more than normal procedures allow. In such cases a special warrant or court order is required. The exact length of time likely to be required (and the associated judicial oversight of procedures) formed the crux of discussions regarding arguments to extend the period of pre-trial detention from 28 to 42 days (Heyman, 2005).

The need to treat planning and counter-terrorism responses differently after 9/11 was recognised by the British police when it defined five types of challenges (Gregory, 2007):

1 a potentially catastrophic event defined partly by the scale of casualties caused by deliberate terrorist actions;

2 an attack without threat warning by suicide bombers using improved explosive devices;

3 a deadly and determined terrorist attack combining assault with automatic weapons, car or truck bombs and suicide or sacrifice bombers;

4 an attack against aviation targets using Man Portable Air Defence System weapons;

5 an attack using either a chemical biological, radiological or nuclear component added to an improved explosive device, or the direct use of a chemical biological, radiological or nuclear weapon.

1.1.2 The case against reconciliation of these rights in favour of security

The counter-claims are varied and arise from concern over what is seen as an ever-encroaching assault on civil liberties.

- Civil libertarians, commentators and others argue that these measures are unnecessary, as the same objectives can be achieved through existing means. In respect of the extension of the period of pre-trial detention to 42 days, for example, opponents of this have argued that if the authorities wanted to hold suspects for longer than the permitted 28 days, then this is already possible.

- Opponents question the efficacy of some measures in delivering required policy objectives. This has been particularly partisan in the case of ID cards and the National Identity Register (NIR), where the Government's stance that such cards will help to address terrorism and illegal immigration have been refuted by a number of parties, based on the evidence that terrorists involved in high-profile incidents made no attempt to hide their identity (London School of Economics, 2005). The evolving nature of the message as to the benefits from these cards (described variously as security benefits, efficiencies or even making life easier for the citizen) does little to refute such claims.

- Finally, and most importantly, they contend that a multitude of measures represent an insidious, piecemeal encroachment upon democratic rights and

freedoms. Clearly, the imposition of such measures may contribute to a growing atmosphere of mistrust of government, but opponents of these measures argue that piece by piece, democratic freedoms are being undermined in the name of security. For example, they argue that the wholesale imposition of data gathering, monitoring and surveillance, both via legislative means (such as the Regulation of Investigatory Powers Act 2000 and the Data Retention Directive 2006) and technological instruments (such as plans for a nationwide database of communications traffic), constitute a steady advance upon essential rights and liberties (e.g. see, Privacy International, 2006). Others argue that many recent legislative initiatives implemented in the name of national security constitute a broader restriction upon *habeas corpus*, and undermine many years of legal precedent (Liberty, 2009).

1.1.3 Examples where these factors affect each other

Although there have been notable historical instances where privacy, liberty and national security have come into play (for example the arrest and conviction of four innocent men (known as the Guildford Four) in 1975 where they were mistakenly imprisoned for their role in Irish republican terrorist activities (Coogan, 1987, p. 651; BBC, 1989) examples of contemporary events illustrative of this balance include the following:

- After 9/11, US intelligence agencies commenced the monitoring of financial data passing through the privately-owned Society for Worldwide Interbank Financial Transfers (SWIFT) network, ostensibly to identify suspicious financial activity. However, a Decision by the European Union's Article 29 Working Party ruled that this constituted a breach of European Data Protection regulations, since SWIFT, based in Belgium, had violated the provisions of the European Union (EU) Data Protection Directive 95/46/EC by permitting this data to be transferred to the USA (a jurisdiction deemed as inadequate by the European Article 29 Working Party on Data Protection in regard to its privacy regime) without prior authorisation (Article 29 Working Party of the EU Data Protection Directive, 2006).
- Following the imposition of increased border security measures in the USA, in 2003 the EU agreed to the transfer of various passenger name record data regarding European citizens travelling to the USA to the US Customs and Border Agency (later part of the US Department of Homeland Security). This was following the imposition of increased border security measures. Airlines were required to provide a variety of passengers' personal data, such as name, address, details of their trip, nationality and even what sort of in-flight meal they had requested.
- The use of National Security Letters by various US agencies, as revealed in the *Doe* v. *Ashcroft* case (American Civil Liberties Union, 2005). Under section 505 of the US Patriot Act of 2001, National Security Letters were used broadly by the US Federal Bureau of Investigation (FBI) to request various types of information on suspects. The Patriot Act permitted their use against US residents, visitors or US citizens who are not subject to any criminal investigation. In addition, National Security Letters were used by the US Department of Defense and the Central

Intelligence Agency (CIA). Also contained in these letters was a non-disclosure notice banning the recipient of the letter from disclosing its existence.

- The accidental fatal shooting of Jean Charles de Menezes at Stockwell tube station in London in July 2005 as part of Operation Kratos (the Metropolitan Police's policy of use of lethal force to counter deadly and determined suicide bombers in the immediate aftermath of the 7/7 attacks in London (BBC, 2008b). Following intensive surveillance of a block of flats in South London, security forces followed a man fitting the description of a suspect into the tube station, where he was shot dead. The subsequent investigation revealed the motivation of the security forces in that actions abrogating the rights of one individual (the right to life) were necessary and proportionate to prevent infringement of the same right of a far greater number of members of the public, since it was thought at the time that the individual was preparing to detonate a device.
- Operation Springbourne, the so-called 'Ricin Plot', was a wide-ranging investigation lasting from 2002–05 (Home Affairs - Fourth Report, 2006). The police investigated a network of Algerian extremists engaged in terrorist activity which also involved peripheral forms of fraud, for example, cheque and credit card fraud etc. The investigation ran into several months and spanned 26 other jurisdictions as well as the UK. Several of those arrested under terrorist offences were later charged with fraud and forgery crimes due to the impossibility of dealing with the evidence in the time available. Had more time been available to assemble evidence, then the opportunity for the prime conspirator to flee the country on bail may not have been present.
- As part of Operation Volga, in early June 2006 a house was raided in Forest Gate, East London, by the Metropolitan Police following intelligence that terrorist suspects were involved in the preparation of chemical weapons. Two men were arrested under the authority of the Terrorist Act. One was accidentally shot in the shoulder. Nearby roads were closed, but several days later the men were released without charge. The Metropolitan Police later apologised for the 'hurt' caused during this operation: a subsequent Independent Police Complaints Commission investigation (one of two) indicated that the police did not use excessive force, but that the response should have evolved as it became clear that the situation was under control and there was no imminent threat (Glass, 2007).
- Operation Overt in 2006 to prevent large-scale terrorist attacks using transatlantic airliners, which resulted in wide-scale security regime regarding liquids in UK airports. This operation involved a significant investment by the security services and a great deal of international cooperation between authorities in a number of different countries. Detective Superintendent Andy Heyman recounted how the operation involved coordination between the UK and US authorities as well as those in Pakistan (Hayman, 2009).

1.1.4 Security versus privacy and liberty: the metaphor of balance?

The use of the metaphor of balance between what are seen as competing concerns of privacy and liberty versus security is popular in the contemporary policy debate (Home Affairs Committee, 2008). A Home Office 2004 discussion paper places security and

liberty as two factors that must be reconciled (Home Office, 2004). A 2005 Democratic Audit scoping report for the Joseph Rowntree Reform Trust into the Government's counter-terrorism laws and strategy describes a "balance between security and liberty", but concedes that these should not be considered polar opposites, since Britain's human rights obligations under the ECHR are drawn up specifically to allow for emergencies such as a campaign of terror (Blick and Weir, 2005).

1.2 Policy challenges

Politicians, policymakers, and those in the security community must weigh up these differing viewpoints when considering the implementation of such measures. Currently, the framework under which this is undertaken is known as the Comprehensive Risk Management Approach, as part of the UK Government's overarching CONTEST counter-terrorism strategy (Home Office Security: Counter-Terrorism Strategy, 2009). The CONTEST strategy has four strands:

1 Prevent – addressing the underlying causes of terrorism;

2 Pursue – using intelligence effectively to disrupt and apprehend terrorists;

3 Protect – ensuring reasonable security precautions;

4 Prepare – making sure that the UK has the people and resources in place to respond effectively to the consequences of a terrorist attack (HM Government, 2006).

The strategy sets out the overall objectives of what should be achieved. Risk assessments are used to effectively and efficiently deliver the 'Protect' and 'Prepare' elements.

1.2.1 The process of assessing risk and balance of investment

Information, intelligence and threat assessments are used as inputs to a process of determining where and to what extent security investments should be made to offset the likelihood of these threats actually being realised against certain vulnerabilities. This is in common with risk assessments, which consider risk as a function of threat, vulnerability and consequence. As an illustration, an approach based on common practice in the insurance industry was applied recently to the sorts of intelligence challenges faced by the US Department of Homeland Security (Willis et al, 2007). In this approach, data was used to assess the following:

- threat – the likelihood of different types of attack on different targets;
- vulnerability – how threats differ from one target to the next, taking into account the attractiveness of each target and how easily or not a target may be damaged; and
- consequences – such as the characteristics of targets, density of population, human activity patterns and valuation of buildings and contents).

These inputs were used to arrive at an expected annual human and economic consequence from a particular form of terrorist risk.

These inputs may be described in qualitative or quantitative terms and may rely upon open source or classified data. As part of this process, investments also may be put in place to reduce the risk of an event occurring (either by actively dealing with the source of the problem, or by acting as deterrent), or deal with the consequences of the realisation of such risks. According to the UK's Centre for the Protection of the National Infrastructure, the utility of these investments are measured in terms of impact upon human life (numbers of lives saved), damage to the economy or impact upon essential services (Centre for the Protection of the National Infrastructure, 2008). Other organisations charged with protecting against national security threats also include 'damage to public good'. The necessity of taking these decisions based on a cost–benefit framework was identified in the 9/11 Commission report, which called on the US Government to "implement security measures that reflect assessment of costs and risks" (National Commission, 2004). Indeed, a wide range of policy guidance exists which includes the quantification of security risks as part of an overall decision support framework (NISTIR-7349, 2006). In more contemporary research this approach has been termed 'probabilistic terrorism risk assessment' (Willis et al, 2007).

Despite this, public reassurances regarding security investment tend to err on the side of caution, communicating that money is no object when it comes to security. For example, commenting on the security arrangements for the London 2012 Olympics, the head of the Olympic Delivery Authority reportedly said: "It will cost whatever it takes to ensure terrorism does not once again try to rob London of celebrating the 2012 Games" (Merrick, 2008). A further important element which is difficult to quantify is not only the cost but the benefit of certain security measures (Stewart and Mueller, 2009). For example, although evidence from interviews and debriefings of (failed or unactioned) terrorist conspiracies can highlight which security measure had the most impact in deterring the perpetrators, this is not always the case. Some literature exists that tries to understand and evaluate the efficacy of CCTV, and to what extent this is effective in addressing certain forms of crime (Hood, 2003; Gill and Spriggs, 2005). Nonetheless, the assessment and subsequent policy decision on what measure might be best applied is based largely on qualitative assessments, experience, judgement and the professional capabilities of those from the security community, rather than on elaborate analysis of quantitative data.

While data on threats may be garnered from expert opinion, intelligence analysis, historical events or covert intelligence collection or monitoring (which may provide actionable intelligence), and data on vulnerabilities may be gathered from understanding weaknesses in a building or infrastructure, estimating data on consequences is more controversial for a number of reasons. First is the sensitivity of discussing loss of life, injury or fatalities. Second, due to the indirect costs of many of these types of risk, estimating economic damage is complex (but not impossible as the insurance industry has been perfecting approaches in this domain for some time). Finally, there are complexities in translating one type of consequence (e.g. x number of fatalities, y number of injuries) into terms of use to the policymaker in a cost–benefit appraisal (mainly economic). Principally this holds for cost of human life but also other forms of impact, such as the change in behaviours as a result of fear of using infrastructures likely to be targeted, or the inconvenience caused by having to spend more time going through security infrastructures implemented as a consequence of heightened risk.

There is an increasing body of literature regarding the valuation of a number of hard to measure inputs into such risk assessments such as human life, security etc. Notable examples may be identified in the way in which Quality Adjusted Life Year (QALY) is used by the National Institute for Clinical Excellence (NICE) as an input metric when assessing the cost–benefit trade-offs of healthcare intervention. With regard to estimating the economic value of a human life – Value of Statistical Life (VSL) – a VSL of between US$1 and US$10 million is used by the US federal government to reflect the societal consideration, risk acceptability and willingness to pay to save a life (Viscusi, 2000). In 2008, in a report for the US Department for Homeland Security, a value of between US$6.3 million and US$12.6 million was proposed as a VSL relevant for homeland security regulatory purposes, taking into account the "involuntary, uncontrollable or dread" characteristics of forms of national security risks such as terrorism, rather than more familiar risks such as workplace or motor vehicle accidents (Robinson, 2008).

Away from conducting economic appraisals of the loss of human life (essentially putting an economic value on a statistical life), there is increasing interest in using economic methods to value other abstract rights that may be affected by security investment, such as privacy (see, Acquisti, 2009). This is subject to similar controversy, since the right to privacy is seen – at least in the European policy community – as inalienable and fundamental, and therefore not subject to economic appraisal. Research suggesting that this can be 'priced' or economically valued (Odlyzko, 2003) contrasts with the perspective taken by many privacy professionals, that privacy is an absolute right and can only be understood in a policy context via a legalistic approach.

1.2.2 Challenges to these approaches

In the context of appreciating and taking into account views of the users of a proposed security infrastructure, the challenges associated with these policy approaches are two-fold.

First, the measures for risk assessment described above only consider the impact of the realisation of the risks themselves in terms of loss of life or economic damage. The costs of imposing various forms of security measure also can be measured and quantified relatively easily. What is not rigorously considered is the impact of the imposition of these measures on the users of this infrastructure – namely, will such measures deter individuals from using the security infrastructure? These unintended consequences may be characterised according to three types:

1 economic – users of the security infrastructure may be deterred from participating in economic activity if this infrastructure is seen to be too onerous. This may be manifested in economic terms: for example, reduced revenue to various forms of businesses such as rail operating companies, transport companies, airport operators, retail facilities or event organisers;

2 social – measures implemented by government, if viewed as unnecessary and disproportionate, may result in increased mistrust on the part of citizens, leading to long-term social consequences such as changing patterns of travel and reluctance to participate in certain activities;

3 behavioural – perception of the politics of fear plays into understanding the behavioural consequences of these measures. The sight of armed police, for

example, may be viewed as justified in a heightened state of alert, or it might be viewed as unnecessary and counterproductive if the public perception of threat is low. The security authorities are aware of these dynamics, and consideration of the behavioural impact of overt security measures (in terms of raising concerns or increasing fear, anxiety or worry) does take place. This is particularly the case in consideration of risks in what are deemed 'crowded places', where there is a large concentration of the general public – for example at public events or transportation hubs such as major rail stations.

Second, there is a question that should be resolved about whether and how the views of users of the security infrastructure should be understood and accommodated in any efforts to mitigate these security risks. Currently, systematic discovery of the users' views is not conducted according to a standardised framework and is highly dependent on the size and extent of the mitigation measures being considered. For large-scale or high-profile investments there is likely to be consideration of the likely effect on the end-users of this infrastructure. Examples include the ongoing surveys and opinion polls conducted by the Identity and Passport Service as part of the roll-out of the Identity Cards Scheme, or the consideration of the impact of increased security measures which were imposed by airport operators at the request of the UK Government in summer 2006.

1.3 Existing literature on understanding behaviour, concerns and views in this field

A clear deficiency in this model of treating security, privacy and liberty as opposed to or at least in tension, is the challenge of information and evidence supporting either argument. Those in the security community argue that they have privileged information and that citizens must trust them to make the right decisions based on their access and analysis of this data. Meanwhile, on the civil libertarian side, many arguments are put forward from a 'absolutist' perspective, grounded more in a nuanced reading of legal texts rather than a practical understanding of the way that the user of a security infrastructure may adjust dynamically their preferences for any of these factors, depending on the environment and context.

Existing attempts to provide an evidence base for understanding the preferences of users of security measures is largely based on opinion polls, surveys or qualitative research, each of which has its limitations. Examples of such polls and opinion surveys include the following.

Westin-Harris series of privacy surveys. Various privacy related surveys have been carried out since the 1970s by Dr Alan Westin. More than 30 privacy-related surveys were conducted between 1978 and 2004 relating to general privacy, consumer privacy, medical privacy and other related areas. After many of these, privacy indexes were created to summarise the results and illustrate trends (Kumaraguru and Cranor, 2005). Usually, these indexes place people into one of three segmented categories, depending on their responses to privacy segmentation questions asking them to indicate their level of agreement with a series of statements from the 2003 Harris Poll (Taylor, 2003):

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

The General Privacy Concern Index from Westin's 1990 and 1991 Consumer Privacy Survey identified the following classifications.

- Privacy Fundamentalists – people who are generally distrustful of organisations asking for their personal information, and who are worried about the accuracy of computerised information. About 25% of the (US) public are privacy fundamentalists.
- Privacy Pragmatists – people who weigh the benefits of various consumer opportunities and services, protection of public safety or enforcement of personal morality against the degree of intrusiveness of personal information sought. Of the (US) population, 57% fits into this category.
- Privacy Unconcerned – people who are generally trustful of organisations collecting their personal information and are ready to forgo privacy claims to secure consumer service benefits or public order values. About 18% of the (US) population fits into this category.

While the explanatory description of some segments of respondents is imposed from the researchers, these surveys attempt to understand what is driving responses and the impact of falling into one of these categories in terms of willingness to surrender privacy to obtain commercial or public benefits. The use of these indexes has also become popular as benchmarks and means to classify respondents in other countries. Finally, in 1994 the same methodology was used to generate a Distrust Index, which classified respondents into 'low' (26%), 'medium' (38%), 'high' (31%) and 'no' (5%) distrust, according to their answers to a series of questions about levels of trust in government and the private sector (Westin et al, 1994).

British Social Attitudes Omnibus Survey. The British Social Attitudes Survey, conducted in 2006, asked a variety of poll questions regarding people's commitments to civil liberties. An overwhelming majority of people were prepared to give up various freedoms in order to help tackle the threat of terrorism. For example, 81% of respondents indicated that following people suspected of terrorism, tapping their phones and opening their mail is a price worth paying, and 80% agreed that restricting the freedom of movement of certain individuals suspected of terrorism is "a price worth paying" for greater security. Similarly, high levels of respondents (79%) felt that "allowing the police to detain people for more than a week or so without charge if the police suspect them of involvement in terrorism" is also a price worth paying to help tackle the threat of terrorism (Johnson and Gearty, 2006).

ICM poll conducted by the Joseph Rowntree Reform Trust. In February 2008 an ICM omnibus poll on ID cards and the Government's handling of personal information revealed that 52% of respondents were uncomfortable with "allowing personal information that is provided to one government department to be shared between all government departments that provide public services". The poll also showed that 50% were against the introduction of ID cards and 47% were in favour (Travis, 2008).

Home Office National Identity Scheme tracking research. Between February 2007 and February 2008 the Home Office conducted National Identity Scheme tracking research to monitor awareness and levels of support for the scheme. This was conducted in three waves: Wave One in February 2007, Wave Two in October 2007 and Wave Three in February 2008. Wave questions regarding the Government's National Identity Scheme and identity cards were added to the Taylor Nelson Sofres General Public Omnibus Survey. These included questions such as:

> Are you aware of the Government's plan to introduce a National Identity Scheme, including ID cards?
>
> … the extent to which you agree or disagree with the Government's plan to introduce a National Identity Scheme, including ID cards?

Responses to such schemes indicated that 35% of the UK population expressed strong agreement with the scheme. Those that expressed lack of support were asked a follow-up question to explore their motivation; 30% expressed the view that because the scheme represented a infringement of civil liberties they did not support it, while 17% indicated the same due to breach of human rights, and 2% indicated that their lack of support was due to "a breach of/intrusion on privacy" (Central Office of Information Research Unit, 2008).

Identity cards: an assessment of awareness and demand for the Identity Cards Scheme. In 2005 The Home Office conducted a quantitative study using conjoint analysis techniques[2] into awareness and demand for the NIR (Home Office, 2005). The purpose of this was to determine where both citizens and public and private sector organisations see most value from the Identity Cards Scheme, and to estimate potential demand for the ID card and verification services. Two waves of research were conducted, the first set of fieldwork in January to March 2005, and the second in August 2005. Despite a major terrorist attack occurring in London in July 2005, the before and after results did not change significantly. The conjoint analysis element of this research indicated that 75% of those respondents would be happy to pay £93 for a combined passport and ID card, or £50 just for the ID card. In addition, the attractiveness of the proposed card was varied, using price as the determining factor. To do this, two further options were presented: one highly attractive (e.g. free of charge), and one significantly less attractive (e.g. more

[2] Conjoint analysis is a statistical technique used in market research, environmental valuation and other disciplines to determine how people value different attributes that make up an individual product or service.

expensive than current passport charges). This generated 83% maximum demand and 63% minimum demand. A number of attributes were identified as factors likely to impact demand, including: price; method of payment; travel time to enrolment centre; opening hours of enrolment centre and turnaround time of an application. No attributes referred to the potential impact on privacy or civil liberties.

UK Department for Transport security screening trials. In 2006 the Security and Contingencies Directorate of the UK's Department for Transport conducted a number of trials of passenger security and screening equipment at national rail and Underground stations. These trials took place at Paddington, Canary Wharf, Greenford and in various places in London and Brighton (Harris, 2008). In-depth qualitative research techniques (interviews and group discussion) were used to understand what the public's attitude to security screening was, and what factors influence its acceptability. These occurred after small numbers of travellers had passed through various types of screening infrastructure, such as X-ray 'body scanners'. Furthermore, at the trial at Greenford station, quantitative research was conducted of 503 local residents regarding their willingness to participate in the trial: 6% of those who said that they would be unwilling to take part in a trial cited concern over privacy or civil liberties as the justification. However, 66% disagreed strongly with the statement when asked whether "screening was an unacceptable invasion of personal space" (Thornton and Goldstein, 2006).

Flash Eurobarometer No. 225: citizens' perceptions regarding data protection in the EU. A Flash Eurobarometer poll was conducted by the Gallup Organisation in February 2008 on behalf of the European Commission into citizens' perceptions regarding data protection in the European Union. The poll asked respondents to

> comment on whether, in the light of international terrorism, it should be possible to have different actions of people monitored, such as their telephone calls, credit card movements or personal details when they fly.

In addition, a set of conditions was presented including "Yes in all cases" or "Yes, but only people who are suspected of terrorist activities", in order to allow for a degree of granularity in response. The nature of opinion polls as a blunt instrument for nuanced understanding was illustrated again by high figures of between 69% and 82% of respondents indicating that conditionally or unconditionally, they would be willing to accept a restriction of their data protection rights when it benefited the fight against international terrorism (Gallup Organisation - Hungary, 2008).

This brief summary of some recent surveys presented above illustrates how current methods of collecting data on attitudes and concerns to the trade-offs that individuals make regarding their privacy, liberty and security may be seen as blunt instruments. The results variously show majority support or opposition to various privacy intrusive measures, and only offer further insight into what motivates responses via the use of simple follow-up questions.

More specifically, these surveys suffer from three main problems when it comes to acting as a means to provide the evidence to fulfil the requirements outlined previously. These weaknesses are as follows.

- They are generally one-dimensional and thus not realistic. The current generation of opinion polls and surveys in this domain ask abstract, one-off questions that do not reflect the reality of everyday situations where people may dynamically accept an intrusion of one sort in order to obtain certain benefits offered. Also, these preferences may change over time. The absence of a realistic hook or context leads respondents to answer in a predictable but unrealistic manner – specifically answering from the perspective that you can never have too much security. Because of the absence of a realistic contextual hook for the questions, they are particularly susceptible to the effects of recent events. Of course, following a terrorist incident, respondents to such an opinion poll are likely to be willing to accept intrusions into their civil liberties and privacy, since the memory of the event or media coverage may be at the forefront. A further aspect of this abstract nature is that they suffer from a bias regarding people's willingness to accept suspension of certain rights, provided there is a perception that it does not happen to them, or happens to everyone. When the question is posed at an individual level and respondents are forced to consider how intrusions might affect them specifically, then the responses might be different. Finally, they suffer from the usual question bias in terms of the use of certain phrases that may contribute to or frame likely responses.
- They do not quantify the extent to which people may be prepared to give up civil liberties or privacy. Surveys and opinion polls may support an understanding of the numbers of individuals who would be prepared to surrender civil liberties to obtain more security, for example, but they do not attempt to answer the question: 'By how much are people willing to give up their civil liberties?', or indeed whether this is different, depending on the type of security infrastructure under consideration.
- They cannot be integrated easily into other cost–benefit analysis. As these surveys do not make any attempt to measure how much liberty or privacy an individual may be prepared to give up to obtain more security, it is difficult for such judgements to be incorporated into formal cost–benefit analysis of the sort likely to be conducted prior to the widespread deployment of certain measures. Monetisation of these difficult to quantify trade-offs across privacy, liberty and security improvements (e.g. individuals' willingness to pay for installing X-ray scanners on the passenger rail network and give up some of their privacy) supports the economic evaluation of the costs and benefits regarding security infrastructure.

Joinson and Paine (2006) present a more nuanced approach to understanding preferences for people to trade off their privacy by matching Westin's Privacy Index against responses to different scenarios, roughly correlated with 2005 proposals from both the UK Home Office and London School of Economics. Generating data not affected by these issues would support greatly the processes described above in Section 1.6, and permit a more rigorous public policy debate based on sound evidence rather than rhetoric or simply statements of knowledge based on access to privileged information.

The use of discrete choice stated preference methods is one such avenue to address these gaps.

1.4 Use of stated preference methods

This study uses a discrete choice stated preference methods approach to examine the trade-offs that people are prepared to make across liberty, privacy and security.

The use of this approach may allow a bottom-up and refined understanding of the importance that people place on these factors, which are seen often as competing or diametrically opposed. The use of these methods has been popular in considering other non-market public goods such as healthcare, the environment and the value of time in transportation studies (Pearce and Ozdemiroglu, 2002). As national security and privacy may similarly be considered as examples of non-market public goods, there is some validity in the application of these techniques to this domain. Furthermore, the use of a methodology that permits identification of real choices and the trade-offs that people are prepared to make contrasts well with the 'top-down', risk-based approach in use by government, which matches vulnerability and threat against investment of resources. Finally, this methodology may help in the cost–benefit decision-making process regarding security measures, since it represents a way to determine robustly the economic threshold by which individuals would be deterred from participating in such infrastructures.

Ultimately the research questions that this study is trying to understand are as follows.

> Given that national security is a form of non-market public good, does the use of stated preference[3] techniques for gathering data on the trade-offs that people are willing to make have merit?
>
> If so, what drives choice when individuals decide to relinquish or surrender their liberty or privacy in order to obtain security benefits?
>
> Is it then possible to monetise the impacts of these security measures upon liberty and privacy?

[3] Stated preference techniques are aimed to examine how people trade-off among different levels of attributes presenting price, quality improvement in goods and services when they face different choice tasks. Analysis of the choices made can help to establish willingness to pay for different benefits (or willingness to accept payment in exchange for bearing a particular loss).

CHAPTER 2 Methodology

This chapter describes our research methodology for applying stated preference techniques to the challenge of trying to understand and quantify the trade-offs that people may make when confronted with choices about their privacy, security and liberty. We began by conducting a literature review on the topic. Following from this, we conducted semi-structured interviews with proponents of all sides of the security–civil liberties debate. We devised a set of choice contexts in which we might present the experimental methodology, in order to circumvent the difficulties of dealing with abstract and difficult-to-define concepts with respondents. Finally, we deployed this experimental methodology against an internet panel of UK residents, socio-economically consistent to the UK population.

2.1 Stated preference discrete choice experiments

Stated preference discrete choice experiments (SPDCE) provide a methodological toolkit for understanding and predicting how individuals make decisions between discrete (mutually exclusive) alternatives. The application of SPDCE is particularly useful when alternatives or certain characteristics of these alternatives are currently unavailable (e.g. new technologies, new policy interventions, environmental protection plans). In particular, SPDCE help to identify how people value the different attributes of services: for example, how people trade off between waiting time and cost when applying for a passport, or how much people are prepared to pay for improved security at rail stations or during public events. It is a technique which has been used extensively in the fields of marketing, health, environmental and transport economics (Louviere and Woodworth, 1983; Louviere, 1992; Louviere et al, 2000; Ryan et al, 2001).

Within the SPDCE framework it is possible to investigate the importance of specific drivers of individuals' choices. In combination with discrete choice analysis, SPDCE provide an empirically-derived evidence base for making informed decisions: for example, how important individuals feel that advanced CCTV cameras enabled with real-time, face recognition technology are. The technique is also data efficient, as more than one observation can be elicited from each respondent during one interview. However, its one drawback is that such data are based around what individuals state they would do in hypothetical situations, which may not exactly correspond to what they would do if faced with the same choice in real life. Well-designed and realistic experiments may help to

overcome this so-called hypothetical bias issue. Box 1 describes in more detail the theoretical underpinning and statistical modelling of a SPDCE.

Box 1: Theoretical background to modelling discrete choice data

Discrete choice models are used to gain insight into what drives the decisions that individuals make when faced with a number of alternatives. These models are constructed by specifying the range of alternatives that were available to the decision-maker, and describing each of these alternatives with a utility equation, which reflects the levels of each of the attributes that were present in the choice that they faced. Each term in the model is multiplied by a coefficient that reflects the size of its impact on the decision-making process ((Ben-Akiva and Lerman, 1985; Train, 2003).

It is the model coefficients that are estimated in the model estimation procedure. The model is based on the assumption that each respondent chooses the alternative that provides them with the highest utility. An error term is included on each utility function to reflect unobservable factors in the individual's utility. Therefore, the estimation can be conducted within the framework of random utility theory, i.e. accounting for the fact that the analyst has only imperfect insight into the utility functions of the respondents.

The most popular and widely-available estimation procedure is logit analysis, which assumes that the error terms on the utilities are independently, identically distributed. The estimation procedure produces estimates of the model coefficients, such that the choices made by the respondents are best represented. The standard statistical criterion of maximum likelihood is used to define the best fit. The model estimation provides both the values of the coefficients (in utility terms) and information on the statistical significance of the coefficients.

Additional terms and non-linear variations in the variables can be added to these utility functions, with testing of the appropriate forms for the utility functions being an important part of the model estimation process. By examining different functional forms we can investigate whether different groups of respondents place different values on the attributes in the choices; also we can test whether there are certain groups of respondents who are more likely to choose systematically one alternative

SPDCE offer respondents hypothetical – although realistic – choice scenarios where each alternative in the choice set is described by a set of attributes (e.g. type of security check, waiting time, processing time, price). Each of the attributes in the experiment is described by a number of levels: for example, the time to process a passport application attribute could have three levels: one day, three days and six days. The attribute levels are combined using principles of experimental design to define different choice scenarios. The respondents evaluate the alternatives and select one of the alternatives within a choice scenario, depending on the trade-offs between the levels offered and their personal

preferences. Of key interest for this study are the trade-offs that individuals are prepared to make when comparing different security measures with implications for their privacy, liberty as well as increases in waiting time or cost. When assessing the trade-offs that individuals are prepared to make when comparing changes of an attribute against price, then this ratio is an indirect measure of willingness-to-pay (WTP), which provides a quantification of individual benefits to feed into a cost–benefit analysis. Also, when trade-offs of attribute improvements are against time (instead of monetary cost), the measure is called 'value of time' (see, Hensher et al, 2005; Louviere et al, 2000).

2.2 Literature review

We began by reviewing the literature surrounding a number of policy interventions which may be regarded as having a beneficial or negative effect on security, civil liberties (as defined in Chapter 1) and privacy. In the literature review phase we were looking for a variety of features of each intervention, namely quantifiable attributes of each intervention including practical measures of their associated benefits and dis-benefits as well as their characteristics and costs.

2.2.1 Policy measures or interventions affecting liberty, privacy and security

The measures we *initially* considered are summarised below.

National DNA database. The national DNA database has been run by the Forensic Science Service on contract to the Home Office since 2005. In 2006, there were more than 4 million records on the database. It has proven its usefulness in tracking down serious offenders in a number of occasions – however, it is not without controversy (Cragg and Mahy, 2009). In 2006, Genewatch reported that the large number of unconvicted individuals on the database (in 2006 there were 124,347 people who were arrested but not subsequently charged or cautioned with an offence) were not beneficial in terms of its effectiveness (Genewatch UK, 2006). Recently, the Forensic Science Service has begun to use familial searching, which uses DNA found at crime scenes to see if there is a 'close match' on the database, raising further civil liberties concerns. Between April 1995 and March 2004, the database cost £182 million. It has come under some criticism for the storage of information for individuals who have not been convicted of any offence, leading to assertions that, given enough time, it will end up storing the DNA of various ethnic groups. Relevant attributes of this policy include:

- the quantity of DNA profiles in the database;
- the success rate of crimes solved as a result of records on the database;
- the numbers of records on the database for people who have not been convicted;
- the extent of sharing DNA profiles between various agencies.

National ID card programme. The Home Office indicates that the National ID card programme (including its back-end database, the NIR) will be useful in fighting terrorism and organised crime. There has been great debate about the validity of this statement and about the true costs of this programme, which has been the subject of public scrutiny, most notably by the London School of Economics. Data from the Home Office included

in its third biannual Cost Report, indicated that the cost of this scheme between October 2007 and October 2017 would be £5,612 million (Home Office, 2007).[4] Relevant attributes include:

- the numbers of successfully identified terrorists, criminals, etc.;
- the chance of cards being forged or used for fraud;
- the numbers of pieces of identity information that the card can replace (e.g. driving licence, passport, National Insurance card).

CCTV. The UK has 4 million CCTV systems and is one of the most well-covered countries in Europe. The cameras are meant to address a range of forms of behaviour including anti-social behaviour street crime as well as collecting evidence of other criminal behaviour. CCTV is known to be extremely useful in the conviction of criminals post-event as an evidential tool, but is less useful in an investigative context. Budgets for CCTV come out of local policing partnerships (Gerrard et al, 2007). However, Detective Chief Inspector Mick Neville, head of the Metropolitan Police's Visual Images, Identifications and Detections Office, has questioned publicly the efficacy and usefulness of CCTV evidence, claiming that it is "an utter fiasco" (BBC News, 2008a). Attributes of interest for CCTV include:

- successful convictions using CCTV footage for identification of suspects or vehicles;
- the number of pre-emptive security interventions as a result of CCTV;
- the perceived deterrent effect;
- the number of cameras;
- the number of times a person is captured on CCTV daily, on average;
- the number of CCTV cameras or warning signs seen daily, on average.

Counter-terrorism measures. These include the budgets of the security services charged with execution of the Government's counter-terrorism strategy, measures to counter violent radicalisation, and efforts to break down cultural barriers and misunderstanding. According to the Home Office 2007 Comprehensive Spending Review, £2.5 billion would be allocated to counter-terrorism and security spending in 2007–08 (HM Treasury, 2007). The attributes considered for this measure included:

- the number of police;
- the number of times people were stopped;
- the number of arrests for terrorism and serious and organised crime;
- the number of convictions for terrorism and serious and organised crime;
- the presence of police in major crowded places.

Public sector information-sharing. The UK has an ambitious programme of the delivery of many government services by electronic means known as 'transformational government'. This includes electronic storage of personal data and sharing personal information about citizens as a way to make government more effective. Examples include sharing data across

[4] This figure includes the provision of ID cards to UK and Irish citizens resident in the UK and foreign nationals applying to extend their leave between October 2007 and October 2017.

schools, Social Services, local authorities and the police in instances of behaviour towards children. The benefits of such sharing were reinforced further by the Varney Report (HM Treasury, 2006). As a user of personal data, the Government has a responsibility under the Data Protection Act 1998 to make sure that such personal data is managed in accordance with legal requirements. The relevant attributes of this measure include:

- the time and effort saved in governmental form-filling;
- a reduction in administrative burden;
- the number of privacy breaches;
- the number of individuals affected by data loss;
- the cost to the individual of rectification.

Transportation security measures. Transportation is widely regarded as one of the most 'at-risk' infrastructures in the UK, classified as 'crowded places'. Security in the transportation sector is highly regulated (the Directorate of Transport Security within the Department for Transport requires commercial transportation system operators to implement certain measures; (UK Dept. for Transport, 2008b). The costs of transportation security measures are extremely difficult to quantify: since they are implemented by the private sector, there is uncertainty about how much lost revenue and inefficiencies occur as a result of the security measures required by government. Typical attributes include:

- the number of security staff;
- the number of suspects identified and detained;
- the number of incidents prevented;
- the extent of delay and inconvenience;
- additional cost.

2.2.2 Semi-structured interviews

Following on from this initial list, we conducted a small number of interviews under the Chatham House Rule with representatives from the security or privacy and civil liberties debate. The interviewees were chosen on the basis of being experts in their respective fields. We interviewed Gareth Crossman and Jago Russell from Liberty, Gus Hosein from the London School of Economics and Privacy International, and Peter Clarke, retired Deputy Assistant Commissioner and former National Coordinator for Anti-Terrorist Investigations. These interviews were intended to clarify further our understanding from the desk research and confirm our view of the benefits and disbenefits of each policy measure. The interviews revealed the continuing gulf that makes the debate surrounding intrusions of liberty and privacy in the name of security so emotive.

2.2.3 Constructing the utility framework

Following the interviews, we considered how policy measures relevant to the achievement of security objectives at the expense of privacy or liberty could be incorporated into a SPDCE. In practice, this meant identifying and constructing the attributes which people might be expected to consider where the concepts of security, liberty, privacy may be in conflict. In addition, security benefits were identified and constructed, based on official

government policy statements on the expected benefits of such measures: for example, the use of ID cards in the fight against international terrorism.

Discussions initially focused on whether there were common attributes (factors) across a number of policy measures such as CCTV, ID cards or the national DNA database. For example, these attributes could include inconvenience, number of data breaches or number of arrests (as a result of the policy measure). However, it was felt that framing the attributes in this manner made the choices too abstract and consequently difficult for the respondent to understand. Moreover, this would lead to dominant alternatives which would not allow respondents to trade off. The use of the generic attributes across a number of different policy measures also meant weaknesses, as some attributes would not fit exactly with an individual's perceptions of the implications of each measure.

2.2.4 Devising choice contexts

The approach of devising choice contexts was identified as a potential avenue to overcome the challenges outlined above. Specifically, using real-world choice contexts would allow us to present instances where policy initiatives regarding security would manifest themselves to the respondent in common situations, and what the factors likely to influence individuals' decisions would be when privacy and liberty compete with security. This would overcome the difficulty of getting respondents to choose coherently and accurately from a number of attributes that were defined in abstract terms.

The rationale for using stated choice methods in this study was based on the absence of existing data (i.e. revealed preferences) that would enable the investigation of issues relevant to individuals' privacy, liberty and security, and in particular, individuals' willingness to trade off across these issues. Moreover, implementation of stated choice methods in this context enables the researcher to quantify trade-offs in monetary terms: for example, willingness to pay for a proposed security measure.

Rather than presenting the respondent with a variety of policy measures that may affect their privacy, security or liberty, we chose instead to try to present the respondent with practical real-world scenarios which most people would have experience of, where the three factors of privacy, security and liberty would come into play. Implementing this required some filtering of the initially identified policy measures described above in Section 2.1.1 and further discussion and consideration of what appropriate attributes to use that would be realistic, practicable and easy for a member of the general public to understand.

In particular, we decided to focus on three real-life situations, ranging from a case where individuals have to deal with a governmental agency such as the Identity and Passport Service when applying for passport, to a frequent routine exercise such as travelling on the UK national rail network, and finally, a situation under special circumstances, for example, attending a large-scale major event such as the opening ceremony of the 2012 London Olympics. These real-life situations incorporate security-related policies which may have an impact on individuals' privacy and liberty.

Applying for a passport. Following increased levels of concern relating to both national security and the theft of individual identity, there has been increasing debate and political pressure for the introduction of personal ID cards and/or the increasing use of biometric

passports with associated personal details stored on the NIR. While supporters have argued that as well as increased security benefits, such a system would benefit individuals through ease of identification, verification and speedier access to services, opponents have cited concerns over the amount of sensitive personal information being held in the central database, the risk of such information being misused or ending up in the public domain, and the additional costs that would be borne by the individual. A range of impacts may be relevant in this scenario, including:

- the amount of time that it takes to process the passport;
- the cost of the document itself;
- the extent of personal information to be shared with other organisations;
- the types of personal information that will be collected at the time of enrolment; and
- the security effectiveness of the system against its stated aims (e.g. disrupting terrorist conspiracies and identifying illegal immigrants).

Travel on the national rail network. Historically, national rail and underground transport networks have been particularly vulnerable to terrorism. The bomb attacks against the Paris Metro and TGV trains during 1995 and 1996, and more recently those on the Madrid Rail network in 2004 and the 7/7 suicide attacks in London in 2005, have served to highlight this concern. Such vulnerabilities are due in part to the very role of national rail systems, which are designed to be public mass transportation systems with the purpose of moving the largest number of people during a set period. Unlike aviation transport networks, the additional delays caused by individual screening of individuals and their baggage may prove counterproductive to any rail system, undermining its purpose and bringing it to a standstill. Consequently, the authorities have been faced with the dilemma of finding an effective balance between increasing security and maintaining the smooth operation of the railway system. As a result, deterrent and reactive measures have been employed regularly, such as high-visibility police patrols and the use of CCTV networks, while stop-and-searches and scanning have been more limited. Attacks such as 7/7 and the attempted 21/7 London tube bombings have led to calls for an increase in the use of such proactive and invasive security measures to ensure public safety. A range of attributes may be relevant in this context, including:

- the presence or absence of various types of security staff;
- the extent and types of monitoring system;
- the increase on the price of a ticket to cover the imposition of security measures;
- the time required to go through security measures; and
- the types of security check.

Finally, the efficacy of these measures also may be relevant in disrupting terrorist conspiracies or identifying illegal immigrants.

Attendance at a major public event. Ensuring the security of major public events such as sporting fixtures or political rallies always has proved a major security concern, as far back as the attack on athletes during the Munich Olympics in 1972 and before. While the buildings and locations themselves may not be considered to be high risk when unused, at the time of a major event the mass of public, key sporting and political figures and media coverage often combine to make the location particularly attractive to any would-be attackers. Consequently, the authorities have relied upon a variety of security measures ranging from basic questions to full searches and detailed questioning, depending on the nature and sensitivity of the event (The Job, 2008). While supporters of such measures argue that they provide increased levels of security for those individuals attending such an event, their detractors complain that many security measures are heavy-handed, excessively intrusive and cause excessive delays and frustration. Relevant manifestations of security measures in this scenario include:

- the delay to pass through security checks;
- the type of security and identity check;
- the type and location of security personnel;
- additional ticket costs to cover security measures; and
- the visibility of response to an incident.

2.2.5 Identifying Attributes and Levels

Attributes were identified through in-depth interviews with privacy and civil liberties experts (Hosein, 2008) and security officials (Clarke, 2007; Clarke, 2008), press articles (BBC, 2006) and literature review research. We studied a range of sources including the following:

- official government reports and policy – for example, UK Department for Transport research into security measures on local and national transportation networks, and Home Office policy statements on the national DNA database, NIR and passports;
- material from the law enforcement community – such as a feature dedicated to Olympic security in the May 2008 edition of *The Job* – the Metropolitan Police's internal newsletter;
- other official reports – such as the Gallup Flash Eurobarometer Survey of February 2009 into Data Protection in the European Union (data subjects' perceptions) and the UK House of Commons Justice Committee 2007 inquiry into the protection of private data;
- academic peer-reviewed articles – including those from the *Journal of Transportation Security*, *Terrorism and Political Violence*, *World Transport Policy and Practice* and the *Journal of Information Science*;
- literature published by independent organisations – including reports by Liberty (*Overlooked: A Review of Privacy*), the London School of Economics report into

the UK Identity Cards scheme, and a report for the Joseph Rowntree Reform Trust.

Once the attributes of each case study were identified and agreed, it was necessary to define the relative changes to the values of attributes associated with each case-study against a reference value (e.g. current price of a passport). Data from existing news reports, literature and the interviews were used to identify and develop the reference value for each attribute. We then hypothesised relative changes of the reference values within a realistic context, known as levels.

The reference values were derived from information available in the public domain. For example, for the numbers of terrorist suspects we reviewed open literature regarding estimates of these figures from experts in the field (The Daily Telegraph, 2006) and organisations in the intelligence community (BBC News, 2007). Similarly, for numbers of terrorist plots we reviewed open statements regarding estimates of these numbers (The Guardian, 2006). To develop the levels for the number of illegal immigrants we searched for official estimates of the numbers of illegal immigrants in the UK to use as the reference value (BBC News, 2005). For the processing time of passport application, we reviewed official Identity and Passport Service information on processing times (Directgov, 2009b). We also identified types of personal data currently collected at the point of passport application (Hall, 2006). Finally, we searched for the likely security measures expected to be implemented at the London 2012 Olympic Games (BBC News, 2008b) and reviewed security measures trialled at stations on the UK rail infrastructure (UK Dept. for Transport, 2008a).

2.3 Case study 1: Applying for a passport

Following increased levels of concern relating to both national security and the theft of individual identity, there has been increasing debate and political pressure for the introduction of ID cards, NIR and the use of biometric passports to collect identity related information. It is expected that this data will be shared amongst a variety of government organisations responsible for security, border management and immigration.

The design attributes introduced in this scenario were classified into three categories:

- *application-related characteristics* – such as total price and processing time of the application;
- *characteristics related to personal data* – such as personal information requirements to obtain a passport, the level of sharing personal data; and
- *potential personal and societal benefits* – such as convenience of using the passport for other purposes, the possibility of reducing illegal immigration and increasing the likelihood of identifying terrorists.

The attributes and their levels used in the choice experiment are shown in Table 1.

The security characteristics of biometric passports may affect privacy and liberty in different ways. For example, data collected for the purposes of law enforcement may be shared (either mistakenly or deliberately) with other organisations not associated with

achieving security objectives, perhaps resulting in discrimination or disenfranchisement of individuals based on the identity information stored. As more organisations are able to use this personal data, so the risk of abuse or mistakes increases.

Table 1: Attributes and levels in the passport application scenario

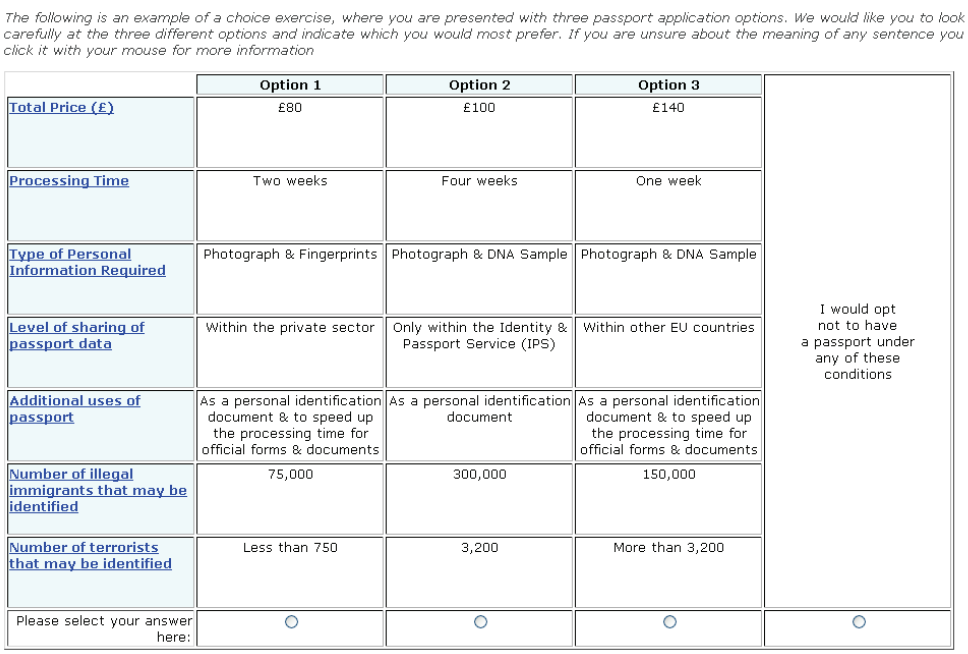
Attribute	Level
Total price (£)	(1) 59 (2) 65 (3) 72 (4) 80 (5) 90 (6) 100 (7) 120 (8) 140
Processing time	(1) Same day (2) Two to three business days (3) One week (4) Two weeks (5) Three weeks (6) Four weeks
Type of personal information required	(1) Photograph (2) Photograph and fingerprints (3) Photograph and iris scan (4) Photograph and DNA sample
Level of sharing of passport data	(1) Only within the Identity and Passport Service (2) Across government generally (3) Within the private sector (4) Within other EU countries
Additional uses of passport	(1) As a personal identification document (2) As a personal identification document and to speed up the processing time for official forms and documents
Number of illegal immigrants that may be identified	(1) 75,000 (2) 150,000 (3) 300,000 (4) 500,000 (5) 800,000 (6) 1,000,000
Number of terrorists that may be identified	(1) Less than 750 (2) 1,200 (3) 1,600 (4) 2,400 (5) 3,200 (6) More than 3,200

The choice experiment involved the choice between three varying situations when applying for a passport. Respondents were introduced to the choice exercise as follows:

> Imagine you are applying for a new style[5] passport for the first time or in order to renew your old passport. During the application process there are a number of factors associated with this, such as the price, processing time, type of personal information required and the way your personal data are stored and possibly shared with other organisations.

[5] A new style passport is one containing biometric information such as a facial biometrics and where the data is entered into the NIR.

A fourth option allowed respondents to reject all three proposed situations by stating "I would opt not to have a passport under any of these conditions" (see Figure 1).



The following is an example of a choice exercise, where you are presented with three passport application options. We would like you to look carefully at the three different options and indicate which you would most prefer. If you are unsure about the meaning of any sentence you can click it with your mouse for more information

	Option 1	Option 2	Option 3	
Total Price (£)	£80	£100	£140	
Processing Time	Two weeks	Four weeks	One week	
Type of Personal Information Required	Photograph & Fingerprints	Photograph & DNA Sample	Photograph & DNA Sample	
Level of sharing of passport data	Within the private sector	Only within the Identity & Passport Service (IPS)	Within other EU countries	I would opt not to have a passport under any of these conditions
Additional uses of passport	As a personal identification document & to speed up the processing time for official forms & documents	As a personal identification document	As a personal identification document & to speed up the processing time for official forms & documents	
Number of illegal immigrants that may be identified	75,000	300,000	150,000	
Number of terrorists that may be identified	Less than 750	3,200	More than 3,200	
Please select your answer here:	○	○	○	○

Figure 1: Example of a passport application choice scenario

The combination of all attributes and levels in Table 1 would result in a significantly large number of choice scenarios, which would be impractical to present as a whole to respondents. Therefore, we constructed an experimental design matrix consisting of 256 scenarios using the macros for discrete choice experiments of the statistical software SAS (Kuhfeld, 2005). The full combination of attributes (i.e. $2^3 * 4^6 * 6^9 * 8^3$) does not result into an orthogonal matrix, however, the 256 scenarios consist of a well-conditioned matrix which can explain main effects with reasonable statistical efficiency[6] (Bliemer and Rose, 2006; Louviere et al, 2000).

The final set of 27 scenarios in the design matrix was selected with several principles in mind. First, same-day passports cannot be cheaper than today's price of £72. Second, high-technology passports cannot be the cheapest options across the three options of a scenario. Within a particular option, personal information should be shared beyond the Identity and Passport Service in order to provide the benefit of speeding up processing times of filling in official forms. Overall, we attempted to control for other cases, so that none of the choice scenarios would seem unrealistic or dominant compared to the other two options. Each respondent was asked to complete eight choice exercises of the passport application scenario.

[6] D-efficiency was at 98.6% and maximum correlation between attributes at 0.18.

2.4 Case study 2: Travelling on the national rail network

The choice experiment in the travel on UK's national rail network scenario involved three categories of relevant attributes:

- *security improvements* – introduced as surveillance equipment, the presence of different types of security personnel and security checks;
- *potential benefits* – such as the likelihood that a terrorist plot may be disrupted and how things may be handled in case an incident occurs;
- *travel related characteristics* – such as waiting time to pass through security and additional costs to cover security improvements.

The complete list of attributes and levels used in the choice experiment is shown in Table 2.

There are a number of attributes that directly compete with privacy and liberty in this case study: most notably, the presence of security personnel may result in inadvertent detention. The presence of CCTV cameras has an impact upon privacy, as does different types of security checks, which many may regard as an invasion of their personal space (e.g. security personnel going through bags or personal effects).

Table 2: Attributes and levels in the rail scenario

Attribute	Level
Type of camera	(1) None (2) Standard CCTV cameras (3) Standard CCTV and new cameras that automatically identify individuals
Time required to pass through security	(1) 1 minute (2) 2–3 minutes (3) 4–7 minutes (4) 8–10 minutes (5) 11–15 minutes
Type of security check	(1) No checks (2) Pat-down and bag search for 1 in 1,000 travellers (3) Pat-down and bag search for 2 in 1,000 travellers (4) Pat-down and bag search for 10 in 1,000 travellers (5) Metal detector/X-ray for all
Presence of the following type of security personnel	(1) Rail staff (2) Rail staff and British Transport Police (3) Rail staff, British Transport Police and armed police (4) Rail staff, British Transport Police, armed police and uniformed military
Increase on price of ticket to cover security	(1) £0.75 (2) £1.00 (3) £1.50 (4) £3.00
Number of known terrorist plots disrupted	(1) 20 plots disrupted every 10 years (2) 10 plots disrupted every 10 years (3) 5 plots every disrupted 10 years (4) 2–3 plots disrupted every 10 years (5) 1–2 plots disrupted every 10 years (6) 1 plot disrupted every 10 years
Visibility of response to a security incident	(1) If an incident occurs, you are not aware of it (2) If an incident occurs, then you are aware of that when you get back home (3) If an incident occurs, things are handled with minimal disruption (4) If an incident occurs, there is some disruption and chaos (5) If an incident occurs, there is lots of disruption and chaos

The stated choice experiment in this case study was set in the context of choosing between three travel situations, each describing conditions that respondents may experience on arrival at the rail station. In particular, respondents were asked the following:

> Imagine that you are making a journey using public transport, such as on the national railway system. We would like you then to consider three ways in which you might make this journey. These are described by different levels of security or privacy.

As shown in Figure 2, an additional fourth option in the scenario allowed respondents to opt out from choosing one of the first three alternatives, stating, "I would choose not to use the rail system under any of these conditions." Each alternative differed in terms of security measures, potential benefits from improved security and travel-related characteristics.

We would like you to look carefully at the three different options and indicate which you would most prefer. If you are unsure about the meaning of any sentence you can click it with your mouse for more information

	Option 1	Option 2	Option 3	
Type of Camera	Standard CCTV & New cameras that automatically identify individuals	Standard CCTV & New cameras that automatically identify individuals	Standard CCTV cameras	
Time required to pass through security	1 Minute	11 to 15 Minutes	2 to 3 Minutes	
Type of security check	Pat down & bag search for 2 in 1,000 travellers	Pat down & bag search for 1 in 1,000 travellers	Pat down & bag search for 10 in 1,000 travellers	
Presence of the following type of security personnel:	Rail staff, British Transport Police & Armed Police	Rail staff and British Transport police	Rail staff, British Transport Police, Armed Police & Uniformed Military	I would choose not to use the rail system under any of these conditions
Increase on price of ticket to cover security	£1	£1.50	£3	
Number of known terrorist plots disrupted	5 plots disrupted every 10 years	5 plots disrupted every 10 years	10 plots disrupted every 10 years	
Visibility of response to a security incident	If an incident occurs there is some disruption and chaos	If an incident occurs there is some disruption and chaos	If an incident occurs things are handled with minimal disruption	
Please select your answer here:	○	◉	○	○

Figure 2: Example of a travelling on the national rail network choice scenario

Using the SAS macros for discrete choice experiments, the experimental design matrix in this case study included 120 scenarios (Kuhfeld, 2005). While the combination of attributes and attribute levels in Table 2 (i.e. 3^3 * 4^6 * 5^6 * 6^3) does not result into an absolutely orthogonal design matrix,[7] the 120 scenarios consist a well-conditioned matrix, which would explain main effects with reasonable statistical efficiency[8] (Bliemer and Rose, 2006; Louviere et al, 2000).

The final set of 71 scenarios in the design matrix was selected with several principles in mind. First, security checks could not be performed using 'Metal detector – X-ray' applied to all travellers if the waiting time within an alternative option was fewer than four minutes. Second, to allow for realistic representation of a choice scenario, when uniformed military was proposed, then other security improvements (i.e. advanced CCTV cameras capable of real-time face recognition) and tighter security checks (i.e. more than two checks in 1,000 travellers) should be in place. Each respondent was asked to complete eight choice exercises of the rail travel scenario.

[7] Orthogonal design is the most widely-used procedure for designing scenarios in SPDCE. The most important property of orthogonal designs is that attributes are not correlated with each other, and therefore true effects can be estimated. For more information on orthogonal designs, please see the references cited in the above text.

[8] The maximum correlation across attributes was 0.18 and the D-efficiency was at 98.6%.

2.5 Case study 3: Attending a major public event

The last case study introduced respondents into choice situations where they are about to attend a large-scale public event, such as the opening ceremony of the 2012 London Olympics. In particular, respondents were asked the following:

> Imagine you are attending the opening ceremony of the 2012 Olympics or any sort of large-scale public event such as a football match or music concert. Again, we would like you to consider carefully the different ways that the event is managed through the following eight scenarios. Again, each scenario involved three alternative options, which have different implications, e.g. on the cost of your ticket and amount of personal information you have to provide to enter the stadium or arena.

The relevant attributes in this choice experiment were divided into four categories:

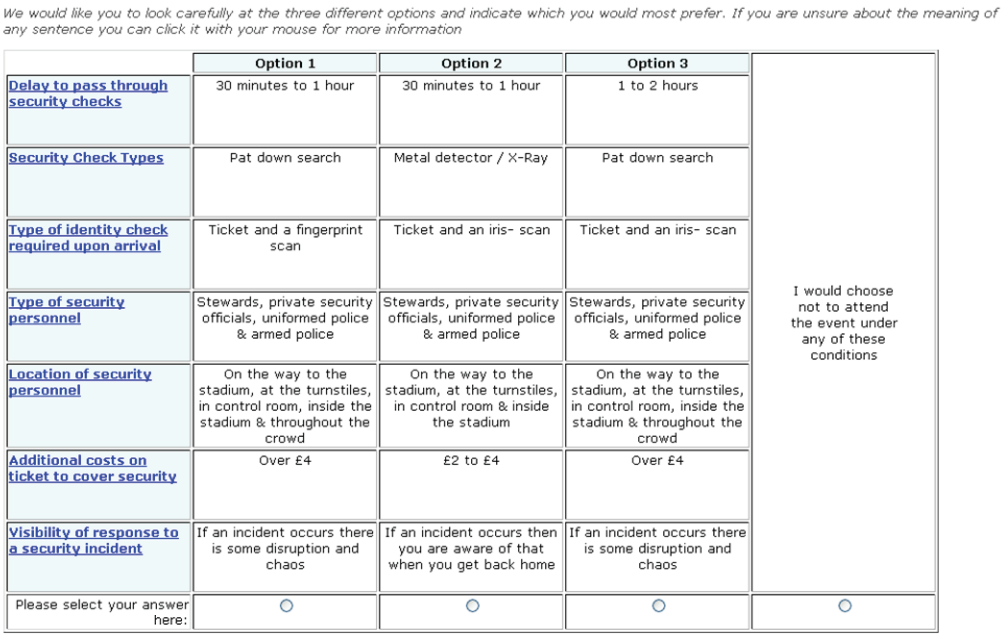
- *security personnel* – such as type and location;
- *burden due to security measures* – including time delays to pass through security, the additional cost to cover security;
- *requirements for individuals* – such as the type of identity and security checks required in order to enter the venue;
- *visibility of response to a security incident* – reflecting the degree of reassurance through the security measures introduced in the given situation.

The complete list of attributes and levels used in the choice experiment is shown in Table 3.

The measures implemented at a major public event to deal with security may affect liberty in a range of ways, including the impact on personal privacy resulting from the collection of personal data upon entry to the event, various forms of personal data being used to verify the identity of the ticketholder and the possibility of detention by the security authorities.

Table 3: Attributes and levels in the public event scenario

Attribute	Level
Delay to pass through security checks	(1) 15 mins or less (2) 15 to 30 mins (3) 30 mins to 1 hour (4) 1–2 hours (5) 2–3 hours
Security check types	(1) Bag search and questioning (2) Pat-down (3) Metal detector/X-ray
Type of identity check required upon arrival	(1) Check of ticket (2) Check of the ticket and pass or badge issued (3) Ticket and photographic ID (4) Ticket and fingerprint scan (5) Ticket and iris scan
Type of security personnel	(1) Stewards and private security officials (2) Stewards, private security officials and uniformed police (including public order police) (3) Stewards, private security officials, uniformed police (including public order police) and armed police or military personnel
Location of security personnel	(1) In control room (2) At the turnstile and in control room (3) On the way to the stadium, at the turnstiles and in control room (4) On the way to the stadium, at the turnstiles, in control room and inside the stadium (5) On the way to the stadium, at the turnstiles, in control room, inside the stadium and throughout the crowd
Additional costs on ticket to cover security	(1) £0 (2) Under £0.50 (3) £0.50 to £1 (4) £1–£2 (5) £2–£4 (6) More than £4
Visibility of response to a security incident	(1) If an incident occurs, you are not aware of it (2) If an incident occurs, then you are aware of that when you get back home (3) If an incident occurs, things are handled with minimal disruption (4) If an incident occurs, there is some disruption and chaos (5) If an incident occurs, there is lots of disruption and chaos



We would like you to look carefully at the three different options and indicate which you would most prefer. If you are unsure about the meaning of any sentence you can click it with your mouse for more information

	Option 1	Option 2	Option 3	
Delay to pass through security checks	30 minutes to 1 hour	30 minutes to 1 hour	1 to 2 hours	
Security Check Types	Pat down search	Metal detector / X-Ray	Pat down search	
Type of identity check required upon arrival	Ticket and a fingerprint scan	Ticket and an iris- scan	Ticket and an iris- scan	
Type of security personnel	Stewards, private security officials, uniformed police & armed police	Stewards, private security officials, uniformed police & armed police	Stewards, private security officials, uniformed police & armed police	I would choose not to attend the event under any of these conditions
Location of security personnel	On the way to the stadium, at the turnstiles, in control room, inside the stadium & throughout the crowd	On the way to the stadium, at the turnstiles, in control room & inside the stadium	On the way to the stadium, at the turnstiles, in control room, inside the stadium & throughout the crowd	
Additional costs on ticket to cover security	Over £4	£2 to £4	Over £4	
Visibility of response to a security incident	If an incident occurs there is some disruption and chaos	If an incident occurs then you are aware of that when you get back home	If an incident occurs there is some disruption and chaos	
Please select your answer here:	○	○	○	○

Figure 3: Example of attending a major public event choice scenario

The scenario matrix of the major event attendance scenario included a total of 90 scenarios, which resulted from the execution of the SAS macro for experimental design using a combination of 3^6*5^12*6^3 attributes and levels.[9] The final set of 54 scenarios was selected after implementing a number of constraints. For example, time delays longer than two hours are justified only when type of identity check involves advanced checking such as fingerprints or iris scans. Also, advanced checks including fingerprinting and iris scans could not be proposed in scenarios where the security staff are located at control rooms. Finally, the additional cost of tickets to cover security took the value of zero only in scenarios where simple identity checks were required (e.g. ticket, badge or photographic ID) and security checks included only bag search and questioning. Each respondent was asked to complete eight choice exercises of the major public event attendance scenario.

2.6 Background questions

In addition to the stated choice scenarios, the survey collected data on the respondents' socio-economic characteristics (e.g. age, gender, employment status, income, frequency of travel by rail, etc) and media preferences, including newspapers and news channels. Also, the respondents were asked general questions about their attitudes towards security, liberty and privacy, known as the Distrust Index (Kumaraguru and Cranor, 2005; Louis Harris et al, 1994). Finally, the survey included a number of cognitive questions concerning the stated choice scenarios. The cognitive questions were designed to ensure that respondents understood and attributed meanings to the choice scenarios that were consistent with both the intent of the survey and the interpretations of the other survey respondents.

[9] The D-efficiency of the matrix was 91.7%.

CHAPTER 3 Descriptive analysis

3.1 Implementation of the survey and distribution of the sample

The stated choice experiments were conducted through the internet between 17 and 19 September 2008.[10] The 2,058 participants were recruited from a nationwide panel of internet users who were registered with Research Now (2007), a marketing research company with the largest panel of internet users in the UK. Originally, the email invitation to participate in the survey was sent to 15,214 individuals, yielding a response rate of approximately 24%, after excluding the number of individuals who did not meet the eligibility criteria (e.g. age <18 years, 0.8%), provided incomplete information (7.9%) or the sample quotas had been collected already (4.5%).

As shown in Table 4, the sample represents well the general population in terms of gender and age. However, as expected with internet surveys, the proportion of individuals with a high level of education in the sample is remarkably higher than the proportions in 2001 UK census (www.statistics.gov.uk/census2001). In comparison to the 2001 UK census, retired individuals (28% vs. 13.4%) are overrepresented and students are underrepresented (see Table 4). Because of the use of the internet as the data collection mode and differences in the socio-economic profiles of our sample compared to the 2001 UK census, there could be no claim that the collected sample is a statistically representative of the UK population. However, one may argue that it is representative of an active segment of the population in the UK which does match with the demographic profiles (i.e. age and gender) of the UK census.

With regard to attitudes towards privacy, liberty and security, as shown in Table 2, 95.8% of the respondents indicated the statement "protecting the privacy of my personal information" as important or very important. Also, 96.3% agreed that "taking action against important security risks" was important or very important. Interestingly, a remarkably lower percentage (85.7%) of respondents – compared to the previous statements – agreed that "defending current liberties and human rights" was important or very important. The responses of participants to the Distrust Index (Kumaraguru and Cranor, 2005; Louis Harris et al, 1994, see also Appendix A) questions showed that 33.8% of respondents were highly distrusting, whereas only 4.8% were not distrusting at all.

[10] The survey was pre-tested and modified in accordance with post-survey cognitive questions by 260 individuals between 27 and 29 June 2008.

Finally, based on newspaper preferences, the respondents were classified into conservative (55.8%) and non-conservative (44.2%).

Table 4: Descriptive statistics of the sample

Variable	Sample (%)	2001 UK census (%)
Gender (females)	52	52
Age group		
18–24	7	16
25–34	13	16
35–44	19	19
45–54	18	16
55–64	21	14
65 and over	22	20
Education level		
None	11	29.1
O level/GCSE	32	35.9
A level/CSE	26	8.3
First degree or higher	32	19.8
Other	-	6.9
Occupational status		
Working full time	42	59.6
Working part-time	16	
Student	4	7.2
Retired	28	13.4
Seeking work	3	4.5
Other	7	15.3
Income		
Less than £30,000	58	
£30,000–£69,999	26	
£70,000 or higher	2	
Not reported	14	
Rail user (*at least twice a year*)	80.1	–
Attitudes to privacy, liberty and security		
Privacy concerned	95.8	–
Liberty concerned	85.7	–
Security concerned	96.3	–
Distrust Index		
High	33.8	–
Medium	37.9	–
Low	23.5	–
Not distrusting	4.8	–

3.2 Trading behaviour in stated preference choices

The first set of tests prior to development of discrete choice models for all three choice experiments focus on the trading behaviour of respondents between the proposed situations (options) within the experiments. These tests provide an indication of whether the respondents engaged with the experiments, or just consistently chose the same option regardless of the cost and level of the other attributes offered. As mentioned in the previous sections, each respondent completed a total of 24 different scenarios (choice exercises): that is, eight scenarios per case study. Therefore, there is always the risk of respondents' non-trading behaviour – that is, respondents always choosing the same option, which can have significant impact on model results (Hess et al, 2008).

Across the three choices experiments (i.e. passport application, rail travel and major public event attendance) approximately 0.1%–0.25% of respondents consistently chose Option 1, 0.25%–0.47% always chose Option 2 and 0.04%–0.29% chose Option 3 (see Table 5). The choice modelling was conducted after excluding 31 unique respondents (1.4% of the sample) who consistently chose the same option across all three experiments. In the context of the case studies, a consistent choice of an option does not have a particular behavioural implication, and therefore respondents who consistently chose the same option across the eight scenarios of across all case studies were excluded from the analysis of all three case studies. This analysis also indicates that more than 98% of respondents did not consistently choose the same alternative in the choice experiments of the case studies, and appear to have taken into account the different costs and levels of the rest of the attributes offered when making their choices.

Table 5: Trading behaviour of respondents across experiments[11]

	Scenario		
Trading	Passport application	Rail travel	Major event attendance
Always Option 1	2	5	5
Always Option 2	10	10	5
Always Option 3	1	5	6
Always 'Opt-out'	82	153	164
Trading between alternatives	1,963	1,885	1,878
Total	**2,058**	**2,058**	**2,058**

3.3 Checking understanding of choices

The data obtained from the diagnostic questions following the choice exercises of each case study were used to investigate whether the respondents understood the SPDCE. These data showed that 87 out of 2,058 respondents in the passport application scenario, 66 out of 2,058 respondents in the rail travel scenario and 48 out of 2,058 respondents in the major public event attendance scenario did not feel able to make comparisons in the choice scenarios offered to them (see Figure 4). Previous research suggests that these respondents should be excluded from further analysis (Rouwendal and De Blaeij, 2004), and therefore a decision was taken to exclude these responses from the model development on the basis that they would be unable to make coherent trade-offs within the experiments. Following the exclusions mentioned in the current and the previous sections, the data available to model individual choices include 1,940 responses in the passport application, 1,961 in the rail travel and 1,979 in the major public event attendance scenarios.

[11] This table includes all instances examined separately in each choice experiment, rather than the 31 unique respondents who consistently chose the same option in any of the three experiments.

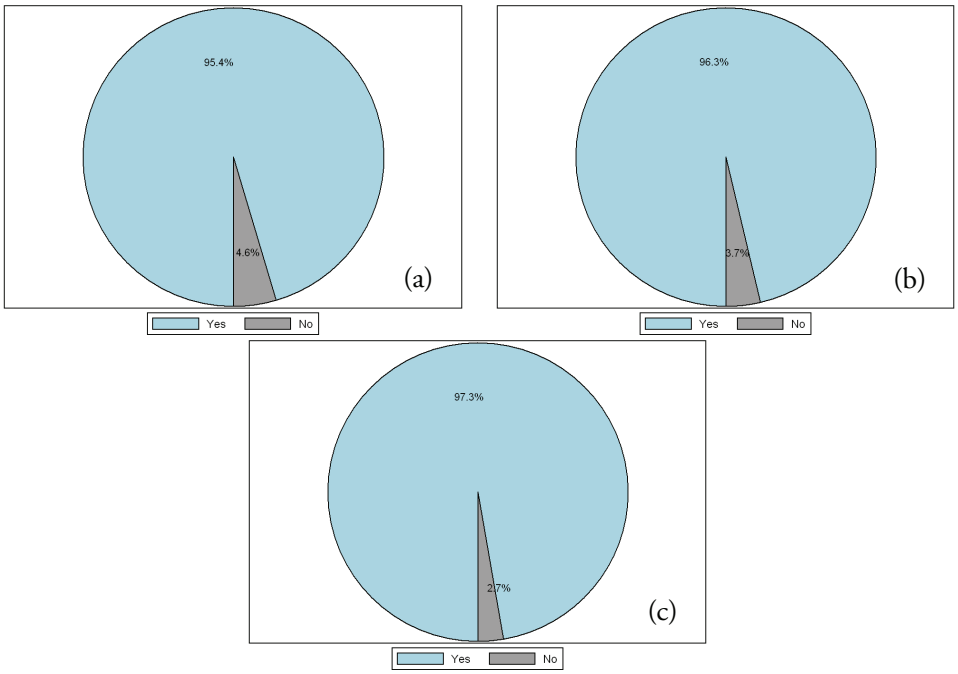


Figure 4: Respondents able to make comparisons in: (a) passport application; (b) rail travel; and (c) major public event case studies

CHAPTER 4 Modelling of the stated preference data

4.1 Introduction

A total of three discrete choice models were developed from the stated preference data, one for each case study. A total of 24 scenarios, eight per case study, were presented to the respondents. Within a given scenario, the respondents made a choice between three alternative situations and an 'opt-out' option. As a result, the choice model contained four utility functions, one for each of the alternatives. The variables in the utility functions of the first three options (i.e. Options 1, 2 and 3) reflect the levels of each of the alternative situations that were present in the choice scenario that they faced. Each variable in the model is multiplied by a coefficient (β_k), which reflects the size of its impact on the decision-making process. The utility of the 'opt-out' option is only a function of respondents' characteristics, as all attribute levels are coded with zero values.

For example, a simple utility function for Option 1 and the 'opt-out' option of the passport application scenario may be expressed as follows:

$$
\begin{aligned}
&U(\text{Option 1}) = \text{Constant\_Option1} \\
&+ \beta_{price} * \text{level of passport price} \\
&\quad + \beta_{processing\_time} * \text{level of processing time} \\
&\quad + \beta_{personal\_info} * \text{level of personal information} \\
&\quad + \beta_{data\_sharing} * \text{level of data-sharing} \\
&\quad + \beta_{add\_use\_of\_passport} * \text{level of additional uses of passport} \\
&\quad + \beta_{ill\_immigrants} * \text{level of number of illegal immigrants} \\
&\quad + \beta_{terrorists} * \text{level of number of terrorists that may be identified} \\
&\quad + \varepsilon_{\text{Option 1}}
\end{aligned}
$$

$$
\begin{aligned}
&U(\text{Opt-out}) = \beta_{gender} * (1, \text{if respondent is female; 0, otherwise}) \\
&\quad + \beta_{age} * (1, \text{if respondent is between 18 and 24; 0 otherwise}) \\
&\quad + \beta_{education} * (1, \text{if individual holds a university degree; 0 otherwise}) \\
&\quad + \beta_{distrust} * (1 \text{ if individual is highly distrustful, 0 otherwise}) \\
&\quad + \varepsilon_{\text{Opt-out}}
\end{aligned}
$$

Figure 5: Examples of utility functions

The model coefficients β_k are estimated in the model estimation procedure, whereas ε is the error term for capturing the observed heterogeneity in the model (Ben-Akiva and Lerman, 1985). Also, a constant is placed on each of the three options to capture the mean of the unobserved effects and control for different biases in the choice experiment (Hensher et al, 2005). The models developed in this study are based on the assumption that each respondent chooses the alternative option that provides them with the highest utility. Therefore, the estimation can be conducted within the framework of random utility theory: that is, accounting for the fact that the analyst has only imperfect insight in the utility functions of the respondents (McFadden, 1973). The functional form of the models estimated is the multinomial logit. All the models in this report were estimated using the ALOGIT software package, a widely-used package for developing models within the logit model family (ALOGIT, 2005).

4.2 Model development

A number of statistical specification tests were undertaken during the model estimation procedures. Following an initial model that used only the attribute levels of the experiments, alternative model specifications included the characteristics of the respondents and their attitudes in order to test whether different groups of respondents placed different valuations on any of the attributes. Possible differences were identified by examining cross tables that summarised the in-sample predictive ability of the model. This approach allowed us to address key differences in the choices made by individuals within the sample.

The tests conducted included a comprehensive list of background variables, including the respondents':

- age, gender, education level, income, socio-economic group, annual income, employment status, place of residence;
- frequency of travelling abroad, travelling by rail and attending major public events;
- Distrust Index, attitudes towards privacy, liberty and security; and
- newspaper preferences as a proxy for ideological or political views (conservative, non-conservative)

Similarly, tests were undertaken to explore whether there was variation in the sample in the terms of the 'value' placed on the cost attributes across the three discrete choice experiments. In all three experiments, there is a plausible trend across the income bands, with individuals with higher income demonstrating less sensitivity to increases in the cost attributes.

Model development tests also focused on the functional representation of the attributes in order to determine whether categorical, linear or piece-wise linear specifications were the most appropriate. In the initial models, each of the attributes were coded as a series of

categorical (dummy) variables, each corresponding to an attribute level.[12] Then the coefficients of these models were plotted against the attribute levels to provide a graphical representation of the extent to which the value placed on attribute levels (coefficient) may or may not be linear. This guided a series of model tests that determined statistically whether those attributes which appeared to be valued linearly in fact could be represented adequately in linear terms applied to the attribute level changes in question (e.g. number of illegal immigrants stopped, number of plots that may be identified, etc.). Those attributes that could not be represented with linear terms (i.e. that experienced a statistically, significant loss of model fit) were specified as piece-wise linear terms that contained one or two points of inflection at one of the levels, informed by the graphical plots. In some cases, the gradient of one of these changes was equal to zero, i.e. the second and/or third level were not valued any more than the first level. The following sections discuss the findings of each case study in more detail.

The final step in model development was to correct for the interdependence of stated preference observations. While SPDCE offer an important advantage in allowing for several responses to be collected from each individual, which reduces substantially the cost of data collection, the collection of multiple responses means that each respondent's basic preferences apply to a series of responses that they have given: those are therefore independent. Naïve analysis methods that assume the independence of stated preference observations provided by the same participant are, in principle, invalid. While a number of methods can used to correct for the interdependence of stated preference observations, experience has shown that a good practical method is to use the 'jack-knife' procedure (Bissell and Ferguson, 1975; Miller, 1974). This is a standard statistical method for testing and correcting misspecifications. RAND Europe has pioneered its use in connection with stated preference data and has found it to be effective and reliable in this context (Cirillo et al, 1998). (The jack-knife procedure is described in more detail in Appendix D.) This procedure was applied to all models, in order to provide corrected estimates of the coefficients and their standard errors.

4.3 Interpreting model results

In reporting the model, we present a number of model fit statistics, as described in Table 6. In interpreting the coefficient values the following points should be considered.

- **A positive coefficient** means that the variable level or constant has a positive impact on utility, and so reflects a higher probability of choosing the alternatives to which it is applied.
- **A negative coefficient** means that the variable level or constant has a negative impact on utility, and so reflects a lower probability of choosing the alternative to which it is applied.
- **Some coefficients are multiplied by continuous or piece-wise linear variables,** and therefore reflect the disutility per unit of the variable.

[12] It should be noted that when attributes are represented as a series of discrete levels, one of these levels needs to be constrained to a value of zero to act as the base from which the other levels are measured.

- **Attribute coefficients applied to categorical variables** reflect the total utility increase or decrease for that variable, relative to a base situation – for example, the increase or decrease in utility as a result of moving from a situation where no cameras exist, to one where standard CCTV cameras are in place at rail stations.

The value shown in parenthesis after each coefficient estimate is the t-ratio. This defines the (statistical) significance of the coefficient estimate: regardless of the sign, the larger the t-ratio, the more significant the estimate. A coefficient with a t-ratio greater than +/-1.960 is estimated to be significantly different from zero at the 95% confidence level. A t-ratio of +/-1.645 is significantly different from zero at the 90% confidence interval.

The model results before and after the jack-knife procedure are presented in the following tables, with the latter having corrected estimates of the standard errors on the coefficients, and hence corrected t-ratios.

Table 6: Model fit statistics

Statistic	Definition
Observations	The number of observations included in the model estimation.
Final log (L)	This indicates the value of the log-likelihood at convergence. The log-likelihood is defined as the sum of the log of the probabilities of the chosen alternatives, and is the function that is maximised in model estimation. The value of log-likelihood for a single model has no obvious meaning; however, comparing the log-likelihood of two models estimated on the same data allows the statistical significance of new model coefficients to be assessed properly through the Likelihood Ratio test.
D.O.F.	Degrees of freedom – i.e. the number of coefficients estimated in this model. Note that if a coefficient is fixed to zero, then it is not a degree of freedom.
$Rho^2(0)$	The rho-squared measure compares the log-likelihood (LL(final)) to the log-likelihood of a model with all coefficients restricted to zero (LL(0)): $Rho^2(0) = 1 – LL(final)/LL(0)$ A higher value indicates a better fitting model.
$Rho^2(c)$	If we compare the log-likelihood (LL(final)) value obtained with the log-likelihood of a model with only constants (LL(c)) we get: $Rho^2(c)$: 1 – LL(final)/LL(c) Again, a higher value indicates a better fitting model.

4.4 Discrete choice modelling results of the case studies

4.4.1 Case study 1: Applying for a passport

First, the stated preference data were checked for accuracy: 87 records were discarded, as these were respondents who felt that they did not understand the survey (see Rouwendal and De Blaeij, 2004). Also, as mentioned in Section 3.2, there is a risk of non-trading behaviour: that is, respondents always choosing the same option, which can have a significant impact on model results (Hess et al, 2008). To alleviate these issues, the 31 respondents who consistently chose the same option across the eight scenarios of all experiments were excluded from the analysis. Thus, the analysis of the stated preference data concerning the rail travel scenario was conducted using 1,940 observations.

Initially, the attribute levels in the passport application choice experiment were dummy coded to the levels of the attributes (Hensher et al, 2005). In addition, the *number of illegal immigrants that may be identified* and *the number of terrorists that be may identified* attributes were tested using liner-cardinal variables. In addition, for the purposes of

dummy coding the aforementioned attributes, these were coded as 75,000, 150,000, 300,000, 500,000, 800,000, 1,000,000 illegal immigrants that may be identified, and as 500, 1,200, 1,600, 2,400, 3,200, 4,000 terrorists that may be stopped. Also, the *processing time* attribute was coded as 1, 2.5, 7, 14, 21 and 28 days.[13] The choice experiment attributes in the "I would opt not to obtain to have a passport under any of these conditions" option were coded with zero values for each of the attributes.

The stated choices experiment was designed with the assumption that the observable utility function would follow a strictly additive form. The model was specified so that the probability of selecting a particular option (i.e. Option 1, 2 or 3) was a function of the seven attributes presented to respondents. Similarly, the probability of selecting the fourth (i.e. 'opt-out') option would be a function of the respondents' characteristics. Using (ALOGIT, 2005) and the 15,520 choices elicited from 1,940 respondents, the highest value of the log-likelihood function was found for the specification shown in the first column of Table 7.[14]

The overall fit of the model, as measured by McFadden's ρ^2, indicates a moderate fit, and the coefficients are statistically significant and intuitively correct. All the potential data requirements that may compete with privacy and liberty are significant factors in the choice of a particular scenario of passport application in the UK. *Ceteris paribus*, attributes related to increased data requirements, including the type of personal information required and the level of sharing passport data, have a significant impact in the probability of respondents selecting or rejection a particular option.

Following an initial model development that used generic coefficients for all respondents in the sample, we tested whether different groups of respondents placed different valuations on any of the attributes in the choice experiment. To identify possible differences, we examined cross-tables that summarised the in-the-sample predictive ability of the model. These tests were conducted on a comprehensive list of respondents' attitudes (e.g. the Distrust Index) and background variables, including age group, gender, socio-economic group, income band and education level.

The negative sign of the *price* of the passport coefficient demonstrates that respondents made rational choices and would prefer passport application procedures. However, the processing time of the passport application presents some interesting results. While the security-unconcerned respondents would prefer options where the processing time of the passport application takes the shortest time, the security-concerned individuals would be in favour of options where processing time takes up to seven days of processing. Our prior expectation about processing time was that all respondents would prefer shorter processing times; however, our finding coincides with evidence from the diagnostic questions

[13] The estimated coefficients were plotted against the step sizes of variables to provide graphical representation of the extent to which the value placed on the attribute levels may or may not be linear. This guided a series of model specifications that tested whether attributes could be specified using a single linear term, or bi-linear terms that contained a point of inflection at one or more of the levels.

[14] The model has been corrected for the interdependence of stated preference observations (i.e. multiple responses per individuals) using the jack-knife procedure.

following the choice experiment and several comments made by respondents at the end of the survey. In particular, processing time was ranked as the *last* most important characteristic when the respondents made a choice across all different options. Only fewer than 10% of the respondents indicated that processing time was the most important characteristic, whereas a handful of respondents indicated that waiting time was not an issue for them when applying for a passport.

The *type of personal information* required and *level of sharing of passport data* were the two attributes where privacy and liberty may compete with the prospect of improving security. On the one hand, individuals may be obliged to provide personal information which may consequently be released to third parties (e.g. the international police) and indirectly, may enhance security and safety through better information control at the borders and across security agencies. On the other hand, one can claim that there is a clear threat to the privacy of individuals and liberty, as fundamentally these data are released to an agency, may be lost or stolen, and ultimately be used against individuals in order to be detained or refused to travel abroad, and so on.

The model findings show that first, individuals would be willing to provide up to a certain level of personal information. All else being equal and comparing to the base case, where an alternative option would require individuals to provide only their photograph, with an option that would ask individuals for a photograph and fingerprints, respondents would be more likely to choose the option that requires their photograph and fingerprints. However, individuals were insensitive to a scheme that would require their photograph and iris scan. Second, the respondents were less likely to choose an option that would require their photograph and DNA sample. In addition, the respondents' preferences for the photograph and DNA-sample level present sensitivity by social status and educations. In particular, white-collar individuals with a university degree form the most sensitive group of respondents who are against photograph and DNA samples as a data requirement to issue a passport. Blue-collar workers and white-collar workers without a university degree are equally sensitive and against providing a DNA sample to obtain a passport.

With regard to personal data-sharing, all the respondents were against any scheme that would release their personal identification data beyond the Identity and Passport Service such as governmental agencies, the private sector or other EU countries. All else being equal, the respondents associated the lower disutility under the option of sharing their personal data across government, and the highest disutility under a scenario where their personal data would be shared within the private sector. In the latter case, there is also a difference in the sensitivity of responses by the individual's education level. As shown from the size of the estimated coefficients in Table 7, the respondents with a university degree associated the highest disutility against sharing their data within the private sector, compared to the respondents without a university degree.

The *additional uses of passport, number of illegal immigrants and number of terrorists that may be identified* attributes were introduced as proxies for potential personal and societal benefits to the respondents when releasing personal data. In fact, these attributes were considered as the basis for trade-offs between sacrificing individuals' privacy and liberty through releasing their personal data, and allowing these to be shared across third parties and achieving improved security and safety. Only those respondents who were identified as

being unconcerned with privacy issues associated a positive utility value with the prospect of using their passports as both as a personal identification document and to speed up the processing time for official forms and documents. Also, the respondents associated positive utility with the *number of illegal immigrants* and *number of terrorists that may be identified*, however, the utility values increase at lower rates when a hypothetical option proposed that more than 2,400 terrorists may be identified.

Finally, the estimation results provided an indication of the profiles of respondents who were more or less likely to opt out and choose none of the first three options offered to them. As shown in Table 7, liberty-concerned individuals were more likely to reject all three options. On the other hand, individuals with scores on the Distrust Index, those between 18 and 24 years of age and security-concerned, were more likely to choose one of the first three options and actually trade off across privacy, liberty and security.

Table 7: Estimation results in the passport application scenario

Variable	Coefficient (t-ratio)
Total price	
x (1, if income less than £50,000; 0, otherwise)	-0.212 (-28.3)
x (1, if income greater than or equal to £50,000 ; 0, otherwise)	-0.018 (-10.0)
x (1, if income unknown; 0 otherwise)	-0.026 (-21.0)
Processing time[15]	
x (1, if security concerned, 0 otherwise)	0.034 (6.3)
x (1, security concerned and processing time >7 days; 0 otherwise)	-0.057 (-8.9)
x (1, security unconcerned, 0 otherwise)	-0.015 (-2.4)
Type of personal information required	
Photograph	Base (N/A)
Photograph and fingerprints	0.152 (3.0)
Photograph and iris scan	0.000 (0.0)
Photograph and DNA sample	
x (1, if holds university degree and is white-collar worker; 0 otherwise)	-0.688 (-7.8)
x (1, if does not hold university degree and is white-collar worker; 0 otherwise)	-0.312 (-7.8)
x (1, if blue-collar worker; 0 otherwise)	-0.312 (-7.8)
Level of sharing passport data	
Only within the Identity and Passport Service	Base (N/A)
Across government generally	0.349(-10.0)
Within the private sector	
x (1, if does not hold a university degree; 0 otherwise)	-0.554 (-10.5)
x (1, if holds a university degree; 0 otherwise)	-0.846 (-12.0)
Within other EU countries	-0.496 (-13.4)
Additional uses of passport	
As a personal identification document	Base (N/A)
As a personal identification document and to speed up the processing time for official forms and documents	
x (1, if privacy unconcerned; 0 otherwise)	0.528 (5.1)
Number of illegal immigrants that may be identified (in thousands)	
x (1, if educational level is up to O-level; 0, otherwise)	0.0009 (15.9)
x (1, if educational level is A-level or higher; 0, otherwise)	0.0006 (9.5)

[15] First two terms under processing time are additive.

Number of terrorists that may be identified[16]	
x (1)	0.00039
x (1, if number of terrorists that may be identified > 2,400; 0 otherwise)	(17.7)
	-0.00036 (-9.5)
Variables in the "I would opt not to obtain to have a passport under any of these conditions" option	
Individual's Distrust Index is high (1,if yes; 0 otherwise)	-0.320 (-3.1)
Individual's age is between 18 and 24 years (1,if yes; 0 otherwise	-0.732 (-3.9)
Individual already holds a passport (1, if yes; 0 otherwise)	-0.472 (-2.6)
Individual is security-concerned (1,if yes; 0 otherwise)	-1.045 (-4.6)
Individual is liberty-concerned (1,if yes; 0 otherwise)	0.465 (3.0)
Constant, Option 1	0.956
Constant, Option 2	(3.0)
Constant, Option 3	1.050
	(3.3)
	0.806
	(2.5)
No. of observations (1,940 x 8)	15,520
Log-likelihood function, L(β) (*d.f.)*	-18,369.5
$\rho^2(C)=1-[L(\beta)/L(C)]$	(26)
$\rho^2(0)=1-[L(\beta)/L(0)]$	0.146
	0.114

4.4.2 Case study 2: Travelling on the national rail network

In addition to the 31 respondents who consistently chose the same option across the eight scenarios of all experiments and who were excluded from the analysis, 66 records were discarded, as these were respondents who felt that they did not understand the survey (Rouwendal and De Blaeij, 2004). Therefore, the analysis of the stated preference data concerning the rail travel scenario was conducted using 1,961 observations. Prior to the analysis, the stated choice data were dummy coded according to the levels of the attributes (Hensher et al, 2005). In addition, the *time required to pass through security*, *increase on price of ticket to cover security* and the *number of known terrorist plots disrupted* attributes were tested as linear-cardinal variables in the model specification. Consequently, the *time required to pass though security* took the levels 1, 2.5, 5.5, 9 and 13 minutes. Similarly, the *number of known terrorist plots disrupted* was coded as 1, 1.5, 2.5, 5, 10, and 20.[17] The choice experiment attributes in the "I would choose not to use the rail system under any of these conditions" option were coded with zero values for each of the attributes. Using ALOGIT (2005) and the 15,688 choices elicited from 1,961 respondents, the highest

[16] The following two terms are additive.

[17] The estimated coefficients were plotted against the step sizes of variables to provide a graphical representation of the extent to which the value placed on the attribute levels may or may not be linear. This guided a series of model specifications that tested whether attributes could be specified using a single linear term, or bi-linear terms that contained a point of inflection at one or more of the levels.

value of the log-likelihood function was found for the specification shown in the first column of Table 8.[18]

The overall fit of the model, as measured by McFadden's ρ^2, indicates a moderate fit, and the coefficients are statistically significant and intuitively correct. All the potential security attributes that may compete with privacy and liberty are significant factors in the choice of a particular scenario of travel on the national rail network in the UK. *Ceteris paribus*, attributes related to improved security measures, including type of camera, security checks and the presence of specialised security personnel, increase the probability that a particular travel situation (option) is selected.

The negative signs on the *price* and *time required to pass through security* coefficients indicate that respondents made rational choices and prefer alternatives that are less costly and require shorter times to pass through security checks. Also, valuation of the increase of ticket price was different across income bands. As expected, the respondents in the lowest income band (<£20,000 per year) placed a higher value on the potential extra cost of the ticket to cover security than the respondents in the higher income band (>£20,000 per year). Interestingly, the respondents who refused to report their income placed an even higher value on the cost of the ticket. General trends regarding the acceptability of related fare increases and time delays are in line with previous opinion surveys of the UK Department for Transport (2005; 2006; 2008a).

Overall, the respondents would prefer travel situations that offer some type of monitoring system, being either standard CCTV cameras or advanced CCTV cameras that enable real-time face recognition. Also, the value placed on improving CCTV cameras to advanced CCTV cameras differed if respondents were identified as liberty-concerned and according to the respondents' education level. In particular, respondents with higher education level placed a lower value on the presence of advanced CCTV cameras compared to individuals with a lower education level (i.e. A-level or lower). These results agree with previous opinion surveys and focus-group research findings. For example, respondents in the Crime Concern/Transport and Travel Research report (1997) felt that a broad range of measures including more staff, improved levels of lighting, CCTV and help points might enhance security and perceptions of personal security for a wide variety of public transport settings. Also, the UK Department of Transport (2006) opinion poll found that in general, respondents were comfortable with the presence of CCTV cameras at rail stations.

With regard to the *type of security check*, respondents generally would prefer travel situations that involve some type of security check. This finding agrees with findings from the UK Department for Transport (2005) study, where the majority (71%) of respondents supported the use of body searches at least twice a week or more. However, it is worth noting that our study findings indicate that on average, respondents would prefer less intrusive security checks (i.e. X-ray imaging) than hand searching. Moreover, different segments of respondents in the sample (white-collar versus blue-collar workers) placed different values on *pat-down and bag search for 10 in 1,000 travellers*, whereas preferences for *metal detector and X-rays for all* were different across gender and males' education level.

[18] The model has been corrected for the interdependence of stated preference observations (i.e. multiple responses per individuals) using the jack-knife procedure.

Concerning the different levels of *security personnel*, the estimation results highlight that respondents would prefer travel situations where more specialised security personnel – other than rail stuff only – are present at rail stations. Evidence from previous research has shown that more uniformed staff has been found to enhance security awareness (Collins, 1993; quoted from Cozens et al, 2002). As shown in Table 8, blue-collar and conservative white-collar workers placed higher value on the presence of more specialised personnel, even for the presence of uniformed military. In contrast, non-conservative white-collar workers were less likely to choose a situation where uniformed military was present over situations with rail staff only.

The *number of known terrorist plots disrupted* attribute was considered to be a potential benefit of improved security measures. In line with *a priori* expectations, the estimated coefficients showed that the respondents would prefer situations where more terrorist plots are disrupted. The estimated coefficients are the result of piecewise-linear specification with two points of inflection at 2.5 and 10 plots every 10 years. Also, the respondents were insensitive to any improvement at the first two levels to the *visibility of response to a security incident* attribute. However, they were less likely to choose options where an incident would cause some disruption or lots of disruption and chaos.

Finally, the estimation results provided an indication of the respondents who were more or less likely to opt out and choose the fourth option offered. As shown in Table 8, males, respondents who scored high values of the Distrust Index and those living in the southern parts of Great Britain were more likely to opt out. In contrast, individuals aged between 18 and 24 years, the security-concerned, frequent rail travellers and people who attend public events were more likely to choose one of the first three options.

Table 8: Estimation results in the 'travelling on the national rail network' scenario

Variable	Coefficient (t-ratio)
Type of camera	
None	Base (N/A)
Standard CCTV cameras	0.552 (16.2)
Standard CCTV and new cameras that automatically indentify individuals	
x (1, if liberty-unconcerned and holds a university degree; 0 otherwise)	1.117 (10.6)
x (1, if liberty-concerned and holds a university degree; 0 otherwise)	0.636 (10.6)
x (1, if liberty-concerned and does not hold university degree; 0 otherwise)	0.886 (18.5)
Time required to pass through security	-0.073 (-25.6)
Type of security check	
No checks	Base (N/A)
Pat-down and bag search for 1 in 1,000 travellers	0.234 (6.5)
Pat-down and bag search for 2 in 1,000 travellers	0.234 (6.5)
Pat-down and bag search for 10 in 1,000 travellers	
x (1, if white-collar worker; 0 otherwise)	0.234 (6.5)
x (1, if blue-collar worker; 0 otherwise)	0.445 (8.9)
Metal detector/X-ray for all	
x (1, if female; 0 otherwise)	0.830 (11.2)
x (1, if male and education level is O-level or lower; 0 otherwise)	0.830 (11.2)
x (1, if male and education level is A-level or higher; 0 otherwise)	0.2341 (6.5)
Presence of the following type of security personnel	
Rail staff	Base (N/A)
Rail staff and British Transport Police	0.197 (8.1)
Rail staff, British Transport Police, and armed police	

x (1, if conservative and white-collar worker or blue-collar worker)	0.197 (8.1)
Rail staff, British Transport Police, armed police and uniformed military	
x (1, if blue-collar worker; 0 otherwise)	0.197 (8.1)
x (1, if conservative and white-collar worker; 0 otherwise)	0.164 (2.8)
x (1, if non-conservative and white-collar worker; 0 otherwise)	-0.199 (-3.7)
Increase of price ticket to cover security	
x (1, if income is less than £20,000; 0 otherwise)	-0.332 (-12.6)
x (1, if income is greater than or equal to £20,000; 0 otherwise)	-0.225 (-9.0)
x (1, if income is unknown; 0 otherwise)	-0.459 (-8.7)
Number of known terrorist plots disrupted	
x (1)	0.296 (13.0)
x (1, if plots greater than 2.5; 0 otherwise)	-0.229 (-9.0)
x (1, if plots greater than 10; 0 otherwise)	-0.043 (-5.7)
Visibility of response to a security incident	
If an incident occurs, you are not aware of it	Base (N/A)
If an incident occurs, then you are aware of that when you get back home	0.000 (0.0)
If an incident occurs, then things are handled with minimal disruption	0.000 (0.0)
If an incident occurs, then there is some disruption and chaos	-0.356 (-13.6)
If an incident occurs, then there is some disruption and chaos	-0.650 (-13.5)
Variables in the "I would choose not to use the rail system under any of these conditions" option	
Male	0.313 (3.3)
Individual's Distrust Index is high (1, if Distrust Index = high; 0 otherwise)	-0.231 (-2.3)
Individual lives in southern UK (1, if yes; 0 otherwise)	0.414 (3.5)
Individual's age is between 18 and 24 years (1, if yes; 0 otherwise)	-0.714 (-3.2)
Individual is security-concerned (1, if yes; 0 otherwise)	-1.234(-4.9)
Individual travels by rail at least twice per year (1, if yes; 0 otherwise)	-0.348 (-2.9)
Individuals attends public events at least once a year (1 if yes; 0 otherwise)	-0.269 (-2.6)
Constant, Option 1	-1.577 (-6.2)
Constant, Option 2	-1.556 (-6.1)
Constant, Option 3	-1.769 (-6.8)
No. of observations (1,961 x 8)	15,688
Log-likelihood function, L(β) (*d.f.*)	-19,150.0
$\rho^2(C)=1-[L(\beta)/L(C)]$	0.119
$\rho^2(0)=1-[L(\beta)/L(0)]$	0.105

4.4.3 Case study 3: Attending a major public event

The last case study involved analysis of respondents' trade-offs for privacy, liberty and security in the context of attending a major public event. The stated preference data available for discrete choice analysis included responses from 1,979 participants. As in the previous two case studies, 31 respondents were excluded from the analysis as they were consistently choosing the same option across all three case studies. Moreover, 48 observations also were excluded from the analysis of the event attendance data as these were respondents who felt that they did not understand the survey (Rouwendal and De Blaeij, 2004).

Each attribute level in the stated preference data was coded as dummy variable. Also, the *additional cost of ticket to cover security* and the *delay to pass through security* attributes were tested as cardinal-linear variables in the model specification. Therefore, the *additional cost of ticket to cover security* took the levels £0, £0.25, £0.75, £1.5, £3 and £4. Similarly, the *delay to pass through security* attribute was coded as 7.5, 22.5, 45, 90 and 150 minutes. The

choice experiment attributes in the "I would choose not to attend the event under any of these conditions" option were coded with zero values for each of the attributes. Using ALOGIT (2005) and the 15,832 choices elicited from 1,979 respondents, the highest value of the log-likelihood function was found for the specification shown in the first column of Table 9.[19]

The negative coefficients of the *delay to pass through security checks* and *additional costs on ticket to cover security* demonstrate that the respondents made rational choices and would prefer options offering shorter delays and less cost to cover security. Following the trends in the data and after testing a model with linear specification that resulted in a statistically significant drop in the fit of the model, the final specification of the *delay to pass through security* attribute included a piece-wise linear specification with a point of inflection at 45 minutes. Also, as shown in Table 9, the valuation on the additional cost to cover security was different across income bands. As expected, the more affluent respondents (i.e. income greater than £40,000) placed the lowest value on the increased ticket cost to cover security, whereas the respondents who did not report their income placed the highest value on the increase of ticket cost.

With regard to the *type of security checks*, the respondents would be more likely to choose options involving checks with a metal detector and X-ray than having to go through bag searches and questioning. The value placed on the metal detector and X-ray options differed by gender: females placed a higher value on this than men. The majority of respondents were insensitive between a pat-down search option and the base level of bag search and questioning. However, individuals of 55 years of age and older were less likely to choose an option involving pat down search as compared to the base level of bag search and questioning. Indeed, the older respondents repeatedly commented that it would have been embarrassing for them to go through pat-down checks. As in the previous case study, the estimation results showed that respondents felt that metal detectors and X-rays resulted in a higher security or privacy and liberty trade-off. Finally, it appears that, especially for the older segments in the sample, there is discrimination of checks between those involving physical and non-physical contact.

The model findings showed that respondents would prefer a more enhanced identity check compared to the base situation of a simple ticket check. Liberty-unconcerned respondents placed the highest utility on ticket and iris-scan checks, whereas liberty-concerned respondents, which consist of the majority of the sample (85.7%), placed a significantly lower value on biometric checks (i.e. fingerprint and iris scan). As shown from the size of the estimated coefficients, on average and compared to the base level of a simple ticket check, the most preferred option would be ticket and photographic ID.

Concerning the different levels of specialisation of the *security personnel* present at the venue, the estimation results highlight that compared to the base level situation (i.e. stewards and privacy security officials), only a segment in the sample would prefer situations that involve the presence of more specialised security personnel. As shown in Table 9, females born in the UK were the only group that would prefer situations where

[19] The model has been corrected for the interdependence of stated preference observations (i.e. multiple responses per individuals) using the jack-knife procedure.

uniformed police and even armed police and military are present at the venue. However, the other hand, males who were not born in the UK placed the highest disutility against any options that involved the presence of armed police or military personnel.

With regard to the *location of security personnel*, the respondents would prefer security personnel to be located throughout and on the way to the venue, and not in control rooms. Valuations varied by gender and ideological orientation. In particular, females and conservative males would be more likely to choose options where security personnel would be located, among other places proposed at lower levels, inside the stadium and throughout the crowd. Non-conservative males also would prefer options where security personnel are placed across other areas, including inside the stadium and throughout the crowd; however, they placed a lower value on these options compared to the other two groups (females, conservative males). Regarding the latter two attribute levels, the value placed by non-conservative male respondents was less than the options of security personnel placed on the way to stadium, at the turnstiles and in the control room. Also, the respondents were insensitive to any improvement at the first two levels to the *visibility of response to a security incident* attribute. However, they were less likely to choose options where an incident would cause some disruption, or lots of disruption and chaos.

Finally, the estimation results provided an indication of the profiles of respondents who were more or less likely to opt out and choose none of the first three options offered to them. As shown in Table 9, the respondents who do not attend major public events, or do attend less than once per year, were more likely to reject all three options. However, individuals with scores on the Distrust Index, those between 18 and 24 years of age and security-concerned, were more likely to choose one of the first three options and actually trade off across privacy, liberty and security.

Table 9: Estimation results in the 'attending a major public event' scenario

Variable	Coefficient (t-ratio)
Delay to pass through security checks[20]	
x (1)	-0.023 (-26.1)
x (1, if delay is longer than 45min; 0 otherwise)	0.013 (11.2)
Security check types	
Bag search and questioning	Base (N/A)
Pat down	
x (1, if individual's age is equal or greater than 55 years; 0 otherwise)	-0.1958 (-4.1)
Metal detector/X-ray	
x (1, if male; 0 otherwise)	0.357 (7.8)
x (1, if female; 0 otherwise)	0.550 (16.4)
Type of identity check required upon arrival	
Check of ticket	Base (N/A)
Check of the ticket and given pass or badge	0.150 (3.5)
Ticket and photographic ID	0.264 (8.5)
Ticket and fingerprint scan	
x (1, if liberty concerned; 0 otherwise)	0.173 (5.9)
x (1, if liberty unconcerned; 0 otherwise)	0.529 (7.9)
Ticket and an iris scan	
x (1, if liberty concerned; 0 otherwise)	0.173 (5.9)
x (1, if liberty unconcerned; 0 otherwise)	0.529 (7.9)
Type of security personnel	
Stewards and private security officials	Base (N/A)
Stewards, private security officials and uniformed police (including public order police)	0.282 (6.4)
x (1, if female born in UK; 0 otherwise)	
Stewards, private security officials, uniformed police (including public order police) and armed police or military personnel	0.282 (6.4)
x (1, if female born in UK; 0 otherwise)	-0.521 (-2.7)
x (1, if male not born in UK; 0 otherwise)	
Location of security personnel	
In control room	Base (N/A)
At the turnstile and in the control room	0.224 (5.6)
On the way to the stadium, at the turnstiles and in the control room	0.431 (13.3)
On the way to the stadium, at the turnstiles, in the control room and inside the stadium	0.557 (12.2)
x (1, if female; 0 otherwise)	0.314 (5.3)
x (1, if male non-conservative; 0 otherwise)	0.431 (13.3)
x (1, if male conservative; 0 otherwise)	
On the way to the stadium, at the turnstiles, in the control room, inside the stadium and throughout the crowd	0.557 (12.2)
x (1, if female; 0 otherwise)	0.314 (5.3)
x (1, if male non-conservative; 0 otherwise)	0.431 (13.3)
x (1, if male conservative; 0 otherwise)	
Additional costs on ticket to cover security	
x (1, if income is less than £40,000; 0 otherwise)	-0.219 (-16.6)
x (1, if income is greater than or equal to £40,000; 0 otherwise)	-0.179 (-8.0)
x (1, if income is unknown; 0 otherwise)	-0.333 (-11.5)
Visibility of response to a security incident	
If an incident occurs, you are not aware of it	Base (N/A)

[20] The following terms are additive.

If an incident occurs, then you are aware of that when you get back home	0.000 (0.0)
If an incident occurs, then things are handled with minimal disruption	0.000 (0.0)
If an incident occurs, then there is some disruption and chaos	-0.308 (-9.6)
If an incident occurs, then there is lots of disruption and chaos	-0.666 (-16.3)
Variables in the "I would choose not to attend the event under any of these conditions" option	
Individual's age is between 18 and 24 years (1, if yes; 0 otherwise)	-0.828 (-3.6)
Individual's Distrust Index is high (1, if Distrust Index = high; 0 otherwise)	-0.342 (-3.2)
Individual attends public events less than once per year or never	0.329 (3.2)
Individual is security-concerned (1, if yes; 0 otherwise)	-1.433 (-8.5)
Constant, Option 1	-0.438 (-2.5)
Constant, Option 2	-0.282 (-1.6)
Constant, Option 3	-0.408 (-2.3)
No. of observations (1,979 x 8)	15,832
Log-likelihood function, L(β) (*d.f.*)	-18,786 (27)
$\rho^2(C)=1-[L(\beta)/L(C)]$	0.144
$\rho^2(0)=1-[L(\beta)/L(0)]$	0.137

4.5 Willingness-to-pay estimates

The SPDCE method is consistent with utility maximisation and demand theory (Louviere et al, 2000; Ortuzar and Willumsen, 2001). Once parameter estimates are obtained by the use of the most appropriate model, a willingness-to-pay (WTP) measure for changes across different levels of attributes can be derived (Hensher et al, 2005). Let V_0 represent the utility of the base level (e.g. no cameras) and V^1 represent the utility of a security improvement compared to base (e.g. standard CCTV cameras). The coefficient of the price increase on ticket to cover security, β_{price}, gives the marginal utility of price:

$$WTP = b_y^{-1} \ln\left\{\frac{\sum_i \exp\left(V_i^1\right)}{\sum_i \exp\left(V_i^0\right)}\right\} \qquad [1]$$

In a simple linear model each attribute in the utility expression and price (cost) are associated with one coefficient each. In that case, equation [1] can be simplified to the ratio of two utility parameters and provide an estimate of willingness to pay:

$$WTP = -1\left(\frac{\beta_{\text{sec urity int ervention/ potential benefit / time-delay}}}{\beta_{\text{increase in price}}}\right) \qquad [2]$$

The best fitting model in this study describes utility functions on the respondents' characteristics (see Table 3). Estimates can be used to calculate the value assigned by the respondents to each of the security improvements, potential benefits and the potential time delay to go through security. In particular, the WTP tables in the following sections present a weighted-average measure of willingness-to-pay (WTP_{wa}) over income groups, which is given as:

$$WTP_{wa} = \sum_i \left(\delta_i * WTP_i\right) \qquad [3]$$

where δ_i is the proportion of respondents in the sample under income band i (e.g. less than £20,000; more than £20,000; unknown). WTP_i is the willingness-to-pay of individuals belonging to income band i.

When attribute levels do not interact with respondent characteristics, the computation of WTP_i becomes analogous to equation [2]. Therefore it is equal to the ratio of the estimated coefficient of an attribute level over the increase in ticket price coefficient each for income band i. To estimate WTP_i when attribute levels interact with respondent characteristics, an extension of equation [1] is used as follows:

$$WTP_i = \sum_j a_j \left[b_y^{-1} \ln \left(\frac{\sum_i \exp\left(V_i^1\right)}{\sum_i \exp\left(V_i^0\right)} \right) \right] \quad [4]$$

Where a_j is the proportion of respondents belonging to a segment of respondent-specific characteristic (e.g. conservative) corresponding to the jth estimated coefficient of an attribute level.

4.5.1 Case study 1: Applying for a passport

The resulting WTP for each attribute in the *applying for a new style passport* case study are shown in Table 10.[21] Comparing the weighted average values of WTP (WTP_{wa}) across attributes, the respondents' highest valuations went towards improving identification of the number of illegal immigrants and terrorists. Moving for the base case of potentially identifying 75,000 illegal immigrants – a best case scenario of 1,000,000 illegal immigrants – the respondents would be willing to pay on average £31.16 on top of the average price of the passport (approximately £72). In the case of the number of terrorists, the respondents would be willing to pay on average up to £37.36 in order to improve the base case situation (500 terrorists) and identify 4,000 terrorists.

An interesting point in these findings is the respondents' willingness to pay in order to extend the processing time from one day to a maximum of 14 days. This contradicts *a priori* expectations, where the respondents would be expected to value higher the shortest processing times possible. In this case, two explanations are possible. First, the respondents may feel that one-day processing time is completely unrealistic for the Identity and Passport Service, and therefore assume that a time range between 2.5 days and two weeks is something more realistic and worth paying for (this correlates with current practice regarding the usual amount of time that it takes to process a passport). Second, respondents may appreciate that passport application is a procedure that is usually pre-planned and should not be left to the last moment. Therefore, they are willing to wait and pay more for their application to be processed and their data to be stored in a suitable way.

With regard to data requirements, the respondents would be willing to pay £7.04 on average in order to provide a photograph and fingerprints compared to the base situation where only photograph would be necessary. However, it would require large subsidies by

[21] It is worth mentioning that stated preference data may overstate the true valuations of respondents, because the situations presented and the choices made are hypothetical. However, the relative valuations of each attribute are less influenced by this problem.

the Identity and Passport Service in order for the passport application to require a DNA sample instead of a simple photograph. Specifically, the average price of the passport should be reduced by an average of £23 in order for respondents to accept a measure that would require a DNA sample.

Table 10: WTP estimates in the applying for a passport scenario (in £)

		Income			
Base level	**Change level**	**< £50,000**	**£50,000+**	**Unknown**	**WTP_{wa}**
Processing time					
1 day	2.5 days	2.27	2.62	1.81	2.23
1 day	7 days	9.06	10.49	7.26	8.91
1 day	14 days	1.39	1.61	1.11	1.37
1 day	21 days	-6.28	-7.27	-5.03	-6.18
1 day	28 days	-13.94	-16.14	-11.17	-13.72
Type of personal information required					
Photograph	Photograph and fingerprints	7.16	8.29	5.73	7.04
Photograph	Photograph and iris scan	0.00	0.00	0.00	0.00
Photograph	Photograph and DNA sample	-19.6	-22.64	-15.66	-19.2
Level of sharing passport data					
Only within the Identity and Passport Service	Across government generally	-16.46	-19.06	-13.19	-16.20
Only within the Identity and Passport Service	Within the private sector	-30.57	-35.39	-24.49	-30.08
Only within the Identity and Passport Service	Within other EU countries	-23.38	-27.07	-18.73	-23.00
Additional uses of passport					
As a personal identification document	As a personal identification document and to speed up the processing time for official forms and documents	0.95	1.10	0.76	0.93
Number of illegal immigrants that may be identified					
75,000	150,000	2.57	2.97	2.06	2.53
75,000	300,000	7.70	8.92	6.17	7.58
75,000	500,000	14.55	16.85	11.66	14.32
75,000	800,000	24.82	28.74	19.89	24.42
75,000	1,000,000	31.67	36.67	25.37	31.16
Number of terrorists that may be identified					
500	1,200	13.12	15.18	10.51	12.90
500	1,600	20.61	23.86	16.51	20.28
500	2,400	35.60	41.21	28.52	35.03
500	3,200	36.79	42.59	29.47	36.19
500	4,000	37.97	43.96	30.42	37.36

Also, respondents were against any intervention that would allow sharing of their personal data across different governmental departments, EU countries or the private sector. Estimates of willingness to pay in this case suggest that the average value of the passport should be reduced on average by £16.20 in order for personal data to be shared across government, £23.00 in order to be shared across EU countries and, £30.08 in order for personal data to be shared across the private sector. Finally, respondents would be willing to pay an average of £0.93 in order to use their passport to speed up the processing time for official forms and documents.

4.5.2 Case study 2: Travelling on the national rail network

Estimates of WTP in the second case study *travelling on the national rail network* are shown in Table 11. The results show that on average, the respondents derive significant values from improved security measures. The highest valuations, £4.44 and £3.54, were placed on efforts to increase the effectiveness of security authorities, namely to able to disrupt terrorist plots – i.e. 20 plots and 10 plots per 10 years, respectively. The next highest valuation of £3.13 was placed for reducing waiting times to pass through security from 13 minutes to 1 minute.

With regard to CCTV cameras at rail stations, the respondents perceived the security benefits of more privacy intrusive cameras to outweigh their possible concerns about privacy, and therefore place a value of £3.10 for advanced CCTV cameras that enable face recognition to be installed at rail stations. In addition, a security check measure involving *metal detectors and X-rays for all* was valued with the one highest WTP, equal to an average of £2.41. Finally, the respondents seem to perceive that more specialised security personnel would be necessary. However, the presence of uniformed military was valued less than other types of security personnel. Therefore, respondents would pay on average £0.72 on top of the average price of their ticket in order for both rail stuff and British Transport Police to be present at rail stations. However, they valued much less the options that included armed police (£0.52) or armed police and uniformed military (£0.28). Finally, the respondents would be willing to pay between £1.08 and £2.38 so that when an incident occurred at a rail station, things would be handled with minimal disruption or respondents would be aware of it when they get home, respectively.

Table 11: WTP estimates in the travel on the national rail network scenario (in £)

		Income			
Base level	**Change level**	**< £20,000**	**£20,000+**	**Unknown**	**WTP_{wa}**
Type of security camera					
None	Standard CCTV	1.66	2.46	1.20	2.03
None	Advanced CCTV	2.55	3.77	1.84	3.10
Type of security check					
No checks	Pat-down and bag search for 1 in 1,000 travellers	0.71	1.04	0.51	0.86
No checks	Pat-down and bag search for 2 in 1,000 travellers	0.71	1.04	0.51	0.86
No checks	Pat-down and bag search for 10 in 1,000 travellers	0.95	1.40	0.69	1.15

No checks	Metal detector and X-rays for all	1.98	2.93	1.43	2.41
Presence of the following type of security personnel					
Rail stuff	Rail staff and British Transport Police	0.59	0.88	0.43	0.72
Rail stuff	Rail staff, British Transport Police and armed police	0.43	0.64	0.31	0.52
Rail stuff	Rail staff, British Transport Police, armed police and uniformed military	0.23	0.34	0.17	0.28
Visibility of response to a security incident					
If an incident occurs there is lots of disruption and chaos	If an incident occurs then you are not aware of it	1.96	2.90	1.42	2.38
If an incident occurs there is lots of disruption and chaos	If an incident occurs then you are aware of it when you get back home	1.96	2.90	1.42	2.38
If an incident occurs there is lots of disruption and chaos	If an incident occurs then things are handled with minimal disruption	0.89	1.31	0.64	1.08
If an incident occurs there is lots of disruption and chaos	If an incident occurs then there is some disruption and chaos	0.00	0.00	0.00	0.00
Time required to pass through security					
13 mins	1 min	2.66	3.73	1.94	3.13
13 mins	2.5 mins	2.23	3.47	1.70	2.82
13 mins	5.5 mins	1.66	2.48	1.21	2.04
13 mins	9 mins	0.89	1.32	0.65	1.08
Number of known terrorist plots that may be disrupted					
1 plot/10 years	20 plots/10 years	3.63	5.41[22]	2.65	4.44
1 plot/10 years	10 plots/10 years	2.89	4.30	2.10	3.54
1 plot/10 years	5 plots/10 years	1.86	2.77	1.36	2.28
1 plot/10 years	2–3 plots/10 years	1.35	2.01	0.98	1.65
1 plot/10 years	1–2 plots/10 years	0.45	0.67	0.33	0.55

4.5.3 Case study 3: Attending a major public event

Results from the last case study *attending a major public event* are reported in Table 12. The maximum amount of respondents' WTP towards improving delays to pass through

[22] In some cases, the WTP estimates may appear rather high: for example, £5.41 on top of the average price of a rail ticket to reduce the number of plots disrupted from 20 to 1 every 10 years. This may be influenced partly by the way that the pricing element was presented to respondents, where the focus was only on the increase in a typical ticket price and the respondents were not reminded of the typical price to which these increases may be applied. As a result, it is possible that respondents may have taken the price increases slightly out of context, which could lead to overstated willingness to pay increases to reduce risk. However, the literature around the value of statistical life does show that people are willing to pay large amounts to reduce human risk, and in this context the values may not be considered so high.

security checks. Therefore, respondents were against scenarios that involved delays longer to the base case of 7.5 mins. In order accept a delay of 150 mins – compared to the base level of 7.5 mins; it would require a remarkable subsidy in the price of the ticket, which on average was estimated at £8.55.

With regard to different security measures, the respondents preferred some identity check, but were more reluctant to pay for checks requiring biometric data. Hence, respondents were willing to pay between £0.70 and £1.19 in order for the identity check to include checks of photographic ID or issuing a pass. In the case that identity checks required fingerprint scan or an iris scan, the respondents were willing to pay up to £1.01.

With regard to the type of security personnel, people were willing to pay more for highly specialised personnel. On the one hand, the range of WTP is between £0.53 for uniformed police, armed police or military personnel and £0.61 for uniformed police. These values are significantly lower compared to the WTP for other interventions, implying that the benefit perceived from the enhancement of security personnel is lower compared with other security interventions. However, the type of security check presents an interesting case, where the respondents were against pat-down search. Thus, a policy to implement pat-down search would require an average reduction of the ticket price by £0.38. On the other hand, people were in favour of metal detector and X-ray checks and were willing to pay an average of £2.06 on top of the average price of the ticket. Finally, it is evident from the WTP estimates that respondents would be willing to pay for an improved degree of reassurance: that is, the visible presence of security personnel on the way and throughout the venue. Compared to the base situation, where security personnel would be located only in control rooms, respondents would be willing to pay up to an average of £2.13 in order for security personnel to be present at the turnstiles, inside the stadium and throughout the crowd. This finding indicates that concerns regarding the potential violation of privacy rights and liberties due to the presence of security personnel may be outweighed by the reassurance of provided security. The latter is also evident when people trade-off situations where different levels disruption may occur, due to an incident (see Table 12).

Table 12: WTP estimates in the attending a major public event scenario (in £)

		Income			
Base level	**Change level**	**< £40,000**	**£40,000+**	**Unknown**	**WTP_{wa}**
Delay to pass through security checks					
7.5 mins	22.5 mins	-1.58	-1.93	-1.03	-1.55
7.5 mins	45 mins	-3.93	-4.82	-2.58	-3.88
7.5 mins	90 mins	-5.96	-7.32	-3.92	-5.88
7.5 mins	150 mins	-8.67	-10.64	-5.69	-8.55
Security check types					
Bag search and questioning	Pat-down	-0.39	-0.47	-0.25	-0.38
Bag search and questioning	Metal detector/X-ray	2.09	2.56	1.37	2.06
Type of identity check required upon arrival					
Check of ticket	Check of the ticket and given pass or	0.71	0.87	0.47	0.70

	badge				
Check of ticket	Ticket and photographic ID	1.21	1.48	0.79	1.19
Check of ticket	Ticket and fingerprint scan	1.02	1.26	0.67	1.01
Check of ticket	Ticket and an iris scan	1.02	1.26	0.67	1.01
Type of security personnel					
Stewards and private security officials	Stewards, private security officials and uniformed police	0.62	0.76	0.41	0.61
Stewards and private security officials	Stewards, private security officials, uniformed police and armed police or military personnel	0.54	0.66	0.35	0.53
Location of security					
In the control room	At the turnstile and in the control room	1.02	1.26	0.67	1.01
In the control room	On the way to the stadium, at the turnstiles and in the control room	1.97	2.42	1.29	1.94
In the control room	On the way to the stadium, at the turnstiles, in the control room and inside the stadium	2.16	2.65	1.42	2.13
In the control room	On the way to the stadium, at the turnstiles, in the control room, inside the stadium and throughout the crowd	2.16	2.65	1.42	2.13
Visibility of response to a security incident					
If an incident occurs, you are not aware of it	If an incident occurs, then you are not aware of it until you get back home	0.00	0.00	0.00	0.00
If an incident occurs, you are not aware of it	If an incident occurs, there is minimal disruption and chaos	0.00	0.00	0.00	0.00
If an incident occurs, you are not aware of it	If an incident occurs, there is some disruption and chaos	-1.41	-1.72	-0.92	-1.39
If an incident occurs, you are not aware of it	If an incident occurs, there is lots of disruption and chaos	-1.41	-3.73	-2.00	-3.00

CHAPTER 5 Key findings and discussion

In this chapter we present some key high level findings regarding the utility of the SPDCE, and illustrate how the most compelling evidence from each case study may relate to some current policy realities.

First, this study has demonstrated the utility of a quantitative research method to understand and monetise the preferences of individuals regarding various policy initiatives that may affect their privacy and liberty in the pursuit of security objectives.

There is a great deal of information that security authorities rely upon when prioritising and making decisions about investment, including information on threats and vulnerabilities and the costs and benefits of security measures. This information can be qualitative or quantitative in nature. Although this can be expected, and indeed in some cases is necessary,[23] the use of quantitative information to represent and understand the non-security related impacts of security measures in this field would appear to be novel. Such an approach presents another way to capture data that may be used by policymakers when making security policy decisions that may affect individuals' privacy or liberty.

As a direct consequence from this, the application of this method illustrates that some rights that are considered as inalienable or fundamental in the legal and policymaking sense may be measured economically. This may be considered to be somewhat controversial, since the exposition of data illustrating how much people are willing to pay for an imposition on their civil liberties or privacy is regarded with some scepticism by those involved with policymaking in this field. This is despite the growing literature in social sciences and economics regarding the use of economic tools to measure such social goods as 'security' or 'privacy'. Indeed, some may view that the existence of such evidence as revealed in this experiment will be instantly attractive to policymakers, leading them to the conclusion that a price may be associated with certain privacy-invasive measures, ignoring the historical, legal and social context of these issues. Nonetheless, this absolutist view ignores the fact that policymakers realistically must make decisions based on available resources, usually in terms of finance or manpower. This has been the case with regard to defence, healthcare and social security for some time (Drummond et al, 2009). However in the contemporary security environment, national security is seen as an issue where the intelligence, law enforcement and security communities demand almost unlimited amounts of resource, despite a recognition that there are not enough resources to reduce all

[23] For example, with the degrees of uncertainty associated with intelligence assessments may be represented best by qualitative information, which permits the grey areas of intelligence to be represented.

risks (Willis et al, 2007). This also highlights another question – that of accountability and transparency. Budgets for security measures aimed at thwarting terrorism are either vague, couched in other numbers (for example, it is still difficult to identify the true budget for Olympics security outside of the total Olympics budget) or subject to scrutiny behind closed doors (for example, by the UK Intelligence and Security Committee). This is beginning to change, albeit slowly: for example, following a freedom of information request, recently the Metropolitan Police was forced to reveal the cost of policing the recent G20 protests of some £200,000.

The evidence collected during this experiment also helps to inform the debate concerning the so-called 'balance between liberty and security'. Crucially, those applicable legal texts (such as the European Convention on Human Rights 1953, the Human Rights Act 1998 or the Data Protection Act 1998) espousing various rights relevant in this domain, such as the right to a private life, right to life, right to a fair trial, etc., also permit these rights to be abrogated in certain circumstances – these include national security, law enforcement or when the actions of one may prevent the exercise of these rights by another. This abrogation is determined as permissible provided that it is legitimate, proportionate, bounded in time and so forth. These laws and the circumstances under which they may be suspended outline the legal background for the somewhat emotive public debate on 'the balance' between security and civil liberties. Aside from media speculation, there is a largely adversarial debate between the strongly-voiced efforts of civil liberties campaigners (such as No2ID and Privacy International) and security and government officials (such as the Identity and Passport Service, Home Office and organisations in the intelligence community, such as the Security Services).

Our experiment revealed notable exceptions as defined by gender, sociodemographic status or perceptions: for example, males expressed a negative utility with the appearance of armed police at a major public event. It is possible that this preference to avoid scenarios in which armed police are present in part is media driven, with an increase in public awareness regarding the heightened security situation. However, when the potential benefits of the security effectiveness of each policy measure (e.g. number of terrorist plots disrupted, number of illegal immigrants identified; or in the case of the public events, the benefit from an incident being dealt with without disruption) are taken into account, it is apparent that even under such heightened awareness and concerns, there are scenarios where the negative value placed on the security intervention can be outweighed by the benefits that it may deliver. A final overall conclusion is that the data illustrated a number of areas where policy and individual preferences are either not matched or in direct opposition. This was most clear in the passport scenario, where the cross-departmental sharing of personal data collected at the point of a passport application is intended to derive efficiencies by creating a single consistent record to allow citizens to be more easily identified with their interactions with the public sector. The strength of preference exhibited toward such measures leads to the conclusion that either a significant discount or subsidy on the price of a passport may be required in order to obtain broader support, or that policymakers will need to take fully into consideration the degree of discomfort associated with sharing this data and factor this into their policy decisions.

5.1 Key findings: discussion

In Sections 5.2 to 5.4 we discuss the key findings from the experiment for each case study. In each example we summarise the way in which privacy, liberty and security might be in conflict, comment on the key discussions, and then conclude each discussion with recommendations intended to illustrate the utility of the data generated by this novel approach for practical policy decisions.

5.2 Case study 1: Applying for a passport

5.2.1 Summary

Under current UK policy, the process of applying for a passport has become an event where concerns over privacy and civil liberties, set against the larger requirements of national security, has come to the fore. Citizens are expected to submit a significant quantity of personal data with their passport application, on the current declared reason that doing so helps in the fight against a number of social 'bads' such as illegal immigration, terrorism and so forth. The conflict of privacy and liberty set against security is relatively abstract in this case, since it concerns aspects of what experts call 'informational self-determination' rather than any perceived immediate threat to the person. Our study has shown that in general, individuals are willing to submit their data for these purposes, except where this might be circulated more widely.

5.2.2 Main findings

The data from this experiment indicated a universal degree of discomfort in the provision of advanced forms of biometric information, such as DNA, as part of the process of passport application. The respondents were willing only to accept (i.e. they derived negative utility from) the collection of DNA and photograph data at the point of application for a passport, if there was a subsidy of £19 on the cost of a passport. A photograph and fingerprint was regarded commonly as preferable type of personal information to be provided, and respondents indicated a willingness to pay £7 for providing this data. This finding is relevant, given recent policy statements which indicate that fingerprint data will be collected as part of the application process (ZDNet, 2009). By contrast, as we have seen, there is no requirement to submit further biometric information at present, since a facial biometric is compiled from the supplied photograph (Directgov, 2009a).

Rather more worryingly from a privacy perspective, there was universal discomfort identified with regard to sharing any personal data collected as part of the passport application process with other organisations in the public or private sectors. As to sharing personal data, all else being equal, the respondents preferred to see their personal data kept within the Identity and Passport Service rather than sharing it either with other government departments, other European nations or the private sector. This has a number of important policy implications, most notably whether the increasing desire to use such datasets by the public sector to achieve efficiencies or help in the fight against organised crime, illegal immigration and international terrorism matches with the preferences of the general public in this regard (Omand, 2009). Furthermore, there is the ongoing question

over consent and choice and whether this may ever be construed as meaningful, given the extent of demand for passports.

The data illustrated that large incentives (for example, a discount on the average price of a passport, perhaps as much as up to £30) would be required in order to reach a threshold where respondents would be comfortable in sharing their personal data with third parties. Respondents indicated that sharing information with the private sector was the least preferred alternative, and would be willing to accept this only if the price of a passport was discounted by £30. For other European nations, a £23 subsidy would be required to elicit this being seen as an acceptable choice, and a subsidy of £16 to share this information with other parts of government (explicitly the intent of this scheme).

The evidence from this case study clearly appears to contradict current government policy, particularly regarding sharing information contained in the NIR, which may be collected as part of the passport application process, with other government departments as part of the 'identity assurance' policy agenda or with the private sector. For example, it has been suggested that banks may wish to use the identity information in the NIR as a government authenticated identity, removing the need for customers to present varying forms of credential when applying for a bank account (BBC, 2008a). Finally, in regard to the sharing of this information with other countries, the European Secure Identity Across Borders Linked (STORK) project (2009) between a number of EU Member States is evaluating methods to do just this, sharing identity information between Member States in order to deliver pan-European services such as the European Electronic Health Insurance Card (EHIC) (NETC@RDS Project, 2009). The existence of such compelling evidence regarding preferences suggests that policymakers ought to explore and consider the implications of this data, and whether a subsidy may be required to manage the possible unintended consequences of the continued implementation of such a policy, such as individuals being deterred from paying certain amounts for a passport on the basis that their personal data may be shared more broadly.

5.2.3 Conclusions: time for a policy rethink?

The widespread sharing of personal data collected as part of the passport application process was shied away from universally by the respondents (they derived negative utility from scenarios involving the sharing of such data). However, there is a policy impetus to share such information across government, the public sector and possibly other nations more widely. In this respect, preferences and policy are clearly in opposition, and policymakers may wish to consider the extent to which this discomfort would affect the implementation of such measures, and whether a reaction is required. Indeed, this may be occurring already, as recently the price of the standard passport was increased by £5.50 (Identity and Passport Service, 2009), while at the same time the Identity and Passport Service confirmed that later versions of the passport would contain iris scan data (ZDNet, 2009).

5.3 Case study 2: Travelling on the national rail network

5.3.1 Summary

In contrast with the passport scenario, security mechanisms which may impact on individuals' privacy or civil liberties when travelling on the national rail network are opposed much less (economically, at least) by the respondents. This may be due to familiarity: in contrast with sharing personal data in the passport case study, which is relatively abstract and distant, the security mechanisms present in this case, such as CCTV and security arches, are much more physically present and perceptively 'closer' to the individual. This can be seen in the example of preferences regarding X-ray machines or a physical pat-down and bag search, with the latter being considered as more invasive, perhaps due to its physical intrusiveness. Despite this, the potential to exercise the right to privacy under this security measure may be less restricted than when personal data is collected when passing through an X-ray arch, where images may be recorded, shared with others and stored for much longer with little informational self-determination by the individual.

5.3.2 Main findings

In relation to the second case study, individuals were comfortable with more intrusive types of security camera (with face-detection type technology), as they seemed to outweigh people's privacy and civil liberties concerns. Indeed, the extent to which this finding is representative of the oft-discussed 'surveillance society' (Ball et al, 2006) is interesting, since it illustrates a degree of familiarity with privacy-invasive forms of technology such as CCTV cameras. However, there remains the question over the extent to which context plays a role, since people may have identified that in the precise and discrete environment of a rail station, being monitored by CCTV of any cause is an acceptable sacrifice to make to obtain security benefits. Similarly, the evidence may illustrate confusion about the perception that CCTV is a tool for detection of low-level street crime such as burglary, mugging or anti-social behaviour, rather than for dealing with more complex forms of criminal behaviour or international terrorism (Farrington and Welsh, 2007).

The findings regarding the degree of comfort attached to different types of security check were counter-intuitive. We anticipated that security checks which may have an obvious implication in terms of privacy would be less preferred than others with which individuals may be more familiar. However, the evidence illustrated that people were comfortable with the idea of passing through an X-ray arch or scanner, much more so than a pat-down or bag search. Understandably, these may be perceived as being more privacy-invasive due to the personal and physical nature of such searches, but in comparison to the data recorded in a metal detector or X-ray scanner, in fact they may adversely affect individuals' privacy in a broader fashion, being shared among more than one individual observing the images and potentially, recorded, stored and passed on to third parties. There is also the extent to which pat-downs and bag searches are more effective from a security perspective – the evidence from the Israeli airline El-Al seems to indicate that alert, trained staff able to spot indicative signs of such behaviour may also prove to be an effective measure.

Finally and somewhat unsurprisingly, there was a high degree of comfort expressed for more specialised security personnel, up to a point. Despite the perception in the security

community that the deployment of armed police or the military creates a fearful atmosphere, in all cases the respondents were willing to pay for security personnel (there was no negative utility identified). Regarding the visible presence of uniformed military, as was seen for example at London Heathrow Airport in 2003 (The Times, 2003), most respondents were willing to pay for these measures (but less so than more 'low-key' forms of security personnel), and felt that their effectiveness was not correlated to the increasing levels of sophistication.

5.3.3 Conclusions: more CCTV equals greater security?

Despite well-publicised statements regarding the use of CCTV and its efficacy in various contexts (for example, as a means to deter crime or as a local law enforcement tool), this study has shown that generally, individuals are welcoming of CCTV, indeed advanced CCTV with automatic detection capabilities, in the context of travel on the national rail network, for the achievement of certain security objectives. This seems to confirm more evocative statements that the extensive CCTV coverage present in the UK (one 2002 estimate indicated that there may be as many as 4.2 million cameras across the UK; (McCahill and Norris, 2002)) has led to us sleepwalking into a 'surveillance society' (Thomas, 2006). Given the comments regarding the effectiveness of CCTV evidence (after the fact), policymakers may wish to consider the utility of more advanced forms of CCTV which may prove to be more effective in an intelligence capacity rather than as an investigative tool for identification of the perpetrator after a crime has been committed.

5.4 Case study 3: Attending a major public event

5.4.1 Summary

The public event scenario presents some similar characteristics regarding the security measures that may be implemented when travelling on the national rail network, but also aspects of what may be termed 'informational self-determination' regarding the use and control of personal data submitted upon entry that are similar to the passport scenario.

5.4.2 Main findings

In the major public event case study, people preferred to have some form of identity check, but all else being equal, were less likely to pay for checks requiring biometric forms of personal data. Based on an expected ticket price of £40 (London Organising Committee of the Olympic Games, 2005) for attendance at the opening ceremony of the Olympic Games, people would be prepared to pay £1.20 for a form of identity check of photographic ID and a check of the ticket. Forms of ticket check covering the use of biometric information (such as a fingerprint scan or iris scan) were less preferred, as individuals would be prepared to pay slightly more than a pound (£1.02) for these forms of identity check. This may be explained by the acceptance that it would be necessary to check the identity of the person presenting the ticket, in order to make sure that they were a legitimate ticketholder. The more interesting finding is that, despite widespread media-reported concern regarding the potential imposition into civil liberties that such technology might bring, individuals were still willing to pay for these intrusions into civil liberties to achieve security objectives. This is reinforced by the finding that respondents

would be willing to pay less (£0.72) for a simple ticket check involving no check of identity information than for forms of ticket check involving some kind of personal or biometric information. This evidence is relevant, given continued discussions over what security technologies might be used to administer entry to Olympic events, with the Olympic Delivery Authority indicating that it would consider the use of 'facial and palm' biometrics for workers at the Olympics site (The Times, 2009).

In addition, the evidence from this part of the experiment indicated that people would be willing to pay more – between around £0.54 and £0.62 on the average likely price of a ticket (£40) – for more specialised forms of security personnel such as uniformed police or even armed police or military. Interestingly, the efficacy is perceived to be lower compared with other security interventions. This evidence confirms the belief held by those in the security community, especially the police, that a visible police presence goes a long way to reassuring the public in crowed places. However, there is continued debate as to whether, from a security perspective, this is the most effective use of personnel for this specific context – indeed, the implementation of new 'behind-the-scenes' systems such as control rooms, aerial surveillance (e.g. via helicopter-based aerial support units) may represent better value for money in terms of achieving security objectives.

5.4.3 Conclusions: a security levy?

Recent evidence illustrating the likely security measures to be implemented for the 2012 Olympics in London highlight the practical utility of these findings. Currently, it is expected that security forces and forms of ticket check are to be deployed as standard security measures for visitors to the Olympics, with athletes and other participants (e.g. media) expected to be subject to further biometric-type measures. Given our findings, that individuals would be willing to pay for measures already envisaged to be implemented and budgeted in the existing likely costs for the Olympics, one possible (although no doubt controversial) approach to reduce pressure on the already-strained London2012 finances (National Audit Office, 2008) would be to issue a security levy on top of the standard ticket price, explicitly to pay for these measures. In this way, some £16 million might be released to cover other costs associated with the event. The use of security taxes is not new, and indeed was a policy tool used in the USA by the Transportation Safety Administration on airlines following the terrorist attacks of 9/11 (Hainmüller, 2003).

5.5 Further work

5.5.1 Privacy impact assessments

We have seen how this methodology may support policymaking and decisions in the security community regarding the sources of data to use as inputs into risk assessments. However, one aspect where this approach may have particular relevance is in Privacy Impact Assessments (PIAs). PIAs are a relatively new policy tool that is being considered as a way to take the privacy perceptions of the 'users' of policy initiatives into account at the time of the design of such measures. Interest in these are growing rapidly, with the UK Information Commissioner's Office launching the second edition of its *Handbook for Privacy Impact Assessments*, in 2009 (ICO, 2009) and further discussion about the use of this tool in Europe and the USA. Other countries such as Australia and Canada have

published guidance on how to conduct PIAs (Office of the Privacy Commissioner of Canada, 2002; Australian Government: Office of the Privacy Commissioner, 2006).

The current state-of-the-art of data-gathering in PIAs foresees evidence collection from the end user of possible privacy-affecting initiatives via qualitative techniques such as focus groups or even expert analysis representing the perspective of end users. As we have seen, the applicability of a method that is able to quantify robustly and monetise preferences regarding abstract concepts such as privacy or civil liberties, and output results in a form of direct utility to policymakers, may be considered as a useful additional evidence-gathering mechanism.

5.5.2 Methodological evolution

Our results demonstrate that we have managed to obtain a robust dataset reflective of current concerns and issues regarding how security measures may affect privacy and liberty. Via a range of diagnostic and evaluative questions asked during the experiment, we were able to discern that individuals understood each attribute and the choices being made available to them. Subsequently, we were able to understand, measure and economically quantify the relative degree of comfort or distaste for these measures.

The study used a stated preference-based methodology which has, at its heart, the expectation that individuals act rationally (for example, when presented with a set of alternatives, they will choose the option that best *satisfies* their need). This is the cornerstone of neoclassical economics. Our study remains at the cutting edge of experiments in this field, as the rational actor model is used for the basis of many other investment decisions in public policy in transportation, healthcare and so on.

Despite this, we identified a range of areas worthy of further exploration in the application of SPDCE in this field.

First, given that this was intended as a proof-of-concept, we used a panel of internet users provided by a third-party market research organisation. The internet panel nature of the data was an example of a pseudo-random sample. Although this panel was demographically consistent with the UK population, there may be less biased random samples which also may be available to undertake data-gathering. For example, because the panel was internet-based, the entirety of the panel was familiar with internet usage (which may be characterised by public concern over identify theft), which in turn may have had an impact in terms of responses to questions regarding technology and privacy.

Second, in terms of definitions, we began with a very pragmatic understanding of liberty and privacy. While this was sufficient for a proof-of-concept experiment such as this, more consideration of the definitions of this earlier on may have resulted in a more focused set of attributes. This may have been possible via using Article 8 of the European Convention on Human Rights 1953, as a starting point, for example.

Third, we used explicit definitions of the stated purpose of security infrastructures from the UK Government. We accept that significant controversy exists as to whether the intended security benefits actually will derive from some of these measures. Furthermore, the stated aim of some of these measures has evolved over time: one only has to observe the controversy surrounding the implementation of ID cards to see that this is the case. Nonetheless, we took government policy at face value for the purposes of this experiment,

since this represents the official stated purposes of which the general public would be aware. Further evolution of our methodology may result in a deeper analysis of this aspect to present a more complex set of factors for the respondent to consider.

Fourth, regarding the attributes themselves, in one or two instances it was necessary to telescope or concatenate them for reasons of space and time. This was the case with some of the basic travel attributes: for example, we could not control effectively for different ticket prices, so had to make assumptions in this respect. Similarly, we made assumptions regarding the time to pass through ticket barriers.

Finally, in terms of grappling with the efficacy of the security measures, we came across the complex challenge of measuring security effectiveness. The deterrent effect of security measures is largely impossible to estimate. To illustrate this, let us consider the question of security plots or conspiracies. Although there have been estimates, as we have seen, regarding the total number of active conspiracies, this may represent only those whom the security forces either know about, or consider to be enough of a risk to count. Thus, the total unbounded population is uncertain. Furthermore, the question of how many of these are deterred by security mechanisms such as identity checks, armed security forces or advanced CCTV *a priori* is complex and difficult for experienced security practitioners to comprehend, let alone the general public. Therefore, while we were hoping that the experiment would reveal correlations between preferences for different security measures on the basis of their perceived security efficacy in addressing intended challenges (such as terrorism or illegal immigration), in reality, the attributes regarding the security impact of different measures (measured in terms of known plots disrupted or illegal immigrants identified) were more useful in contributing as a control for other factors. For example, as the total number of plots cannot be known in advance, and it is well-nigh impossible to observe empirically the efficacy of security measures in prevention, the security authorities must work extremely hard to deal with every eventuality, using risk assessment and intelligence as a means to prioritise resources. This fundamental dilemma was characterised in an IRA statement shortly after the Conservative Party conference was bombed in Brighton in October 1984, which said:

> Today we [the IRA] were unlucky, but remember we only have to be lucky once. You [the Security Services] will have to be lucky always. (An Phoblacht/Republican News, 1984)

5.6 Conclusions

The types of question that this study tried to answer were as follows.

- Given that national security is a form of non-market public good, does the use of stated preference techniques for gathering data on the trade-offs that people are willing to make have merit?
- What drives choice when individuals decide to relinquish or surrender their liberty or privacy to obtain security benefits?
- Is it possible to monetise the trade-offs between security measures and liberty and privacy?

Our work has shown that it is possible to obtain and quantify the views and preferences of citizens as users of security infrastructure. In some cases we have demonstrated also that it is possible to monetise them, and that this would be valuable if conducted in a focused context.

This data may be used as another information source to support consideration of security investment decisions, when balancing the likely risk of an incident versus the costs and implications of the implementation of security infrastructure to mitigate this risk.

Our study can shed light on where policy and preferences differ, and thus can support policymakers and those deploying such security infrastructure to take informed evidence-based decisions as to whether the cost of contravening or ignoring these preferences outweighs the benefit that may be brought from implementing such measures. Similarly, it might be possible to identify where measures might be adjusted to take better account of preferences without undermining any security gains.

Finally, evidence gathered from the application of our methodology can bring a degree of objectivity into a highly-charged and emotive debate, particularly when policy discussion turns to talk of 'finding the right balance' between civil liberties and security. Ultimately, this study has shown that use of the metaphor of balance to characterise the civil liberties versus security challenge is counterproductive without robust measurement of the weight of each factor to be balanced.

REFERENCES

Acquisti, A., "The Economics of Privacy", 2009. Online at http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm#new (as of Nov. 2009).

ALOGIT, HCG Software, 2005.

American Civil Liberties Union, "Internet Service Provider's NSL Challenge - Doe v. Holder", 2005. Online at http://www.aclu.org/free-speech_national-security/internet-service-providers-nsl-challenge-doe-v-holder.

An Phoblacht/Republican News, "IRA bombs British Cabinet in Brighton, October", 1984. Online at http://www.anphoblacht.com/ (as of Jan. 2010).

Article 29 Working Party of the EU Data Protection Directive, "Opinion on processing of personal data by the society of Worldwide Interbank Financial Telecommunication (SWIFT) (WP128)", 2006. Online at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf (as of Jan. 2010).

Australian Government: Office of the Privacy Commissioner, "Privacy Impact Assessments Guide", 2006. Online at http://www.privacy.gov.au/materials/types/download/9349/6590 (as of Nov. 2009).

Ball, K., D. Lyon, D.M. Wood, C. Norris, and C. Raab, "A report on the Surveillance Society", 2006. Online at http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf (as of Jan. 2010).

BBC, "Extracts from MI5 chief's speech (Interview of Eliza Manningham-Buller)", 2006. Online at http://news.bbc.co.uk/2/hi/uk_news/6135000.stm (as of May 2008).

BBC, "Guildford four released after 15 years", 1989. Online at http://news.bbc.co.uk/onthisday/hi/dates/stories/october/19/newsid_2490000/2490039.stm (as of Nov. 2009).

BBC, "In Full Smith ID Card speech, 6th March ", 2008a. Online at http://news.bbc.co.uk/2/hi/uk_news/politics/7281368.stm (as of Jan. 2010).

BBC, "Open verdict at Menezes inquest", 2008b. Online at http://news.bbc.co.uk/1/hi/uk/7764882.stm (as of Nov. 2009).

BBC News, "CCTV Boom "failing to cut crime", May 6th", 2008a. Online at http://news.bbc.co.uk/2/hi/uk_news/7384843.stm (as of Nov. 2009).

BBC News, "Illegal immigrant figure revealed", 2005. Online at http://news.bbc.co.uk/2/hi/uk_news/politics/4637273.stm.

BBC News, "MI5 watch 2000 terror suspects", 2007. Online at http://news.bbc.co.uk/2/hi/uk_news/6613963.stm.

BBC News, "Police Announce London 2012 Plans", 2008b. Online at http://news.bbc.co.uk/sport2/hi/olympics/london_2012/7277918.stm (as of Jan. 2010).

Ben-Akiva, Moshe and Steven R. Lerman, *Discrete Choice Analysis: Theory and Application to Travel Demand*, Cambridge: MIT Press, 1985.

Bissell, A. and R. Ferguson, "The Jack-knife: Toy, Tool or Two-Edged Weapon?" *Statistician,* Vol. 24, 1975, pp. 79-100

Blick, A and S. Weir, "The Rules of the Game: the governments counter terrorism laws and strategy: A democratic Audit Scoping Report for the Joseph Rowntree Reform

Trust", 2005. Online at http://www.jrrt.org.uk/uploads/terrorism_scoping_report.pdf (as of Nov. 2009).

Bliemer, M. and J. Rose, "Designing stated choice experiments: The state of the art" *11th International Conference on Travel Behaviour Research*, Kyoto, Japan, 2006.

Brown, G., "42-day detention; a fair solution: The complexity of today's terrorist plots means the Government needs more powers" *The Times*, 2008. Online at http://www.timesonline.co.uk/tol/comment/columnists/guest_contributors/article4045210.ece (as of Jan. 2010).

Central Office of Information Research Unit, *Identity and Passport Service; National Identity Scheme Tracking Research Wave 3*, London Home Office, 2008.

Centre for the Protection of the National Infrastructure, "What is at risk? What is critical infrastructure in an interdependent global economy? What are critical infrastructures? The distinction between criticality of asset (e.g. national grid) and criticality of consequence of attack" *Critical Infrastructure Protection and Resilience: Trans-border Challenges*, 18 - 21 February, Wilton Park Conference, 2008.

Cirillo, C., A. Daly, and K. Lindveld, "Eliminating Bias due to the repeated measurements problem in SP Data" *Operations Research and Decision Aid Methodologies in Traffic and Transportation Management*, Balatonfüred, Hungary, March 10-21, 1998.

Clarke, P., "DAC Peter Clark's speech on counter terrorism", 2007. Online at http://cms.met.police.uk/news/major_operational_announcements/terrorism/dac_peter_clark_s_speech_on_counter_terrorism (as of May 2008).

Clarke, Peter, "Benefits and disbenefits of security initiatives", London (personal communication), 2008.

Collins, M., "Strathclyde PTE focuses on safety of women passengers" *Modern Railways,* Vol. 50, No. 534, March, 1993, p. 141.

Coogan, T.P., *The IRA*, Glasgow: William Colins and Sons, Inc., 1987.

Cozens, P.M., R.H. Neale, J. Whitaker, and D. Hillier, "Investigating perceptions of personal security on the valley lines network in South Wales" *World Transport Policy & Practice,* Vol. 8, No. 1, 2002, pp. 19-29.

Cragg, S and P. Mahy, "The Law Gazette: European Court Judgement on DNA retention 8th January 2009", 2009. Online at http://www.lawgazette.co.uk/in-practice/european-court-judgment-dna-retention (as of Jan. 2010).

Crime Concern/Transport and Travel Research, *Perceptions of safety from crime public transport. Research report for the Department of Environment, Transport and Regions*, London: Department for Transport, 1997.

Directgov, "Table of Passport Fees, how to pay and refunds", 2009a. Online at http://www.direct.gov.uk/en/TravelAndTransport/Passports/howlongittakesandurgentappplications/DG_174109 (as of Mar. 2009).

Directgov, "Travel and transport - timetable for passport applications", 2009b. Online at http://www.direct.gov.uk/en/TravelAndTransport/Passports/howlongittakesandurgentappplications/DG_174148 (as of Mar. 2008).

Drummond, M., Brixner D., Gold M., P. Kind, A. McGuire, and E. Nord, "Toward a consensus on the QALY" *Value in Health,* Vol. 12, No. Suppl. 1, 2009 pp. S31-35.

ETS 155, "Convention for the protection of human rights and fundamental freedoms", 1998. Online at http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm.

Farrington, D.P. and B.C. Welsh, *Closed Circuit Television: Surveillance and Crime Prevention: A Systematic Review report*, Stockholm: prepared for Brå (Swedish National Council for Crime Prevention), 2007.

Gallup Organisation - Hungary, *Data Protection in the European Union Citizens Perceptions: Analytical Report Flash Eurobarometer 225*: The Gallup Organisation, 2008.

Genewatch UK, "The DNA expansion programme: Reporting real achievement?", 2006. Online at http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/DNAexpansion_brief_final.pdf (as of Nov. 2009).

Gerrard, G., G. Parkins, I. Cunningham, W. Jones, S. Hill, and S. Douglas, "National CCTV Strategy", 2007. Online at http://www.crimereduction.homeoffice.gov.uk/cctv/National%20CCTV%20Strategy%20Oct%202007.pdf (as of Jan. 2010).

Gill, M. and A. Spriggs, "Assessing the Impact of CCTV Home Office Research Study 292 ", 2005. Online at http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf (as of Dec. 2009).

Glass, D., "IPCC Independent Investigations into Complaints Made Following the Forest Gate Counter-Terrorist Operation on June 2006", 2007. Online at http://www.ipcc.gov.uk/forest_gate_2_3report.pdf (as of Nov. 2009).

Gregory, F., "Police and counter-terrorism in the UK, a study of one of the highest and most pressing challenges for police nationally " in *Homeland Security in the UK: Future Preparedness for Terrorist Attack since 9/11*, Wilkinson, P., ed. London: Routledge, 2007.

Hainmüller, J.Lemnitzer, J.M., "Why do Europeans Fly Safer? The politics of airport security in Europe and the US" *Terrorism and Political Violence,* Vol. 15, No. 4, 2003, pp. 1-36.

Hall, J., "Question the head of the Identity and Passport Service", 2006. Online at http://www.number10.gov.uk/Page10364 (as of Nov. 2009).

Harris, T., "London Underground and National Railways Passenger Screening Trials", 2008. Online at http://www.dft.gov.uk/pgr/security/land/lunr (as of Jan. 2010).

Hayman, Andy, "Why I suspect jittery Americans nearly ruined efforts to foil plot" *The Times, Sept. 8*, 2009. Online at http://www.timesonline.co.uk/tol/news/uk/crime/article6825262.ece (as of Nov. 2009).

Hensher, David A., John M. Rose, and William H. Greene, *Applied Choice Analysis - A Primer*, New York: Cambridge University Press, 2005.

Hess, S., J. Rose, and J. Polak, "Non-trading lexicographic and inconsistent behaviour in SP choice data" *87th Annual Meeting of the Transportation Research Board*, January 13-17, Washington D.C., 2008.

Heyman, Andy, "Letter from Assistance Commissioner (SO) Andy Heyman to the Home Secretary", 2005. Online at www.statewatch.org/news/2005/oct/met-letter-terror-law.pdf.

HM Government, "Countering International Terrorism: The United Kingdom's Strategy", Vol. CM 6888, 2006. Online at http://www.fco.gov.uk/resources/en/pdf/contest-report (as of Nov. 2009).

HM Treasury, "Meeting the Aspiration of the British People: 2007 Pre-budget and Comprehensive Spending Review", 2007. Online at http://www.hm-treasury.gov.uk/d/pbr_csr07_completereport_1546.pdf (as of Nov. 2009).

HM Treasury, "Service transformation: A better service for citizens and businesses, a better deal for the taxpayer", 2006. Online at http://www.hm-treasury.gov.uk/d/pbr06_varney_review.pdf (as of Nov. 2009).

Home Affairs - Fourth Report, "Appendix: Police briefing note", 2006. Online at http://www.publications.parliament.uk/pa/cm200506/cmselect/cmhaff/910/91010.htm (as of Jan. 2010).

Home Affairs Committee, "A Surveillance Society?", 2008. Online at http://www.official-documents.gov.uk/document/cm74/7449/7449.pdf (as of Nov. 2009).

Home Office, "Counter-Terrorism Powers: Reconciling Security and Liberty in an Open Democracy: A Discussion Paper," 2004. Online at http://www.statewatch.org/news/2004/feb/uk-CT-discussion-paper.pdf (as of Nov. 2009).

Home Office, "Identity Card Scheme Cost Report", 2007. Online at http://www.ips.gov.uk/cps/files/ips/live/assets/documents/2007-11-06-Identity-Cards-Scheme-Cost-Report-November-2007.pdf (as of Nov. 2009).

Home Office, "Identity Cards: An Assessment of Awareness and Demand for the Identity Card Scheme", 2005. Online at http://www.ips.gov.uk/cps/files/ips/live/assets/documents/2005-10-12-Trade-Off-final-report.pdf (as of Dec. 2009).

Home Office Security: Counter-Terrorism Strategy, "The CONTEST counter-terrorism strategy to reduce the risk from international terrorism is based on four principles: Pursue, Protect, Prevent and Prepare", 2009. Online at http://security.homeoffice.gov.uk/counter-terrorism-strategy/ (as of Nov. 2009).

Hood, J., "Closed circuit television systems: a failure in risk communication?" *Journal of Risk Research,* Vol. 6, No. 3, 2003, pp. 233-251.

Hosein, Gus, "National Identity Register, National DNA Databank, Data protection law", London (personal communication), 2008.

ICO, "Information Commissioner Office Privacy Impact Assessment Handbook (v2)", 2009. Online at http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx (as of Jan. 2010).

Identity and Passport Service, "New Passport Fees Announced, 7th July", 2009. Online at http://www.ips.gov.uk/cps/rde/xchg/ips_live/hs.xsl/1167.htm.

Johnson, M. and C. Gearty, *Civil liberties and the challenge of terrorism' in British Social Attitudes: the 23rd Report - Perspectives on a changing society*, London Sage for NatCen, 2006.

Joinson, A. N. and Carina Paine, "Watching me, watching you: Privacy attitudes and reactions to identity card implementations scenarios in the United Kingdom" *Journal of Information Science,* Vol. 32, No. 4, 2006, pp. 334-343.

Klug, F., K. Starmer, and Weir S., *The Three Pillars of Liberty: Political Rights and Freedoms in the UK*, London: Routledge, 1996.

Kuhfeld, W., *Marketing Research Methods in SAS: Experimental Design, Choice, Conjoint and Graphical Techniques*, Cary, NC, USA: SAS Institute Inc., 2005.

Kumaraguru, P. and L.F Cranor, *Privacy indexes: A survey of Westin's studies*, Pittsburgh: Institute for Software Research International, Carnegie Mellon University, CMU-ISRI-5-138, 2005.

Liberty, "Protecting Civil Liberties: Promoting Human Rights", 2009. Online at http://www.liberty-human-rights.org.uk/issues/human-rights-act/index.shtml.

London Organising Committee of the Olympic Games, "Stunning image of a London Games", 2005. Online at http://www.london2012.org/en/news/archive/2005/february/2005-02-18-12-30.htm.

London School of Economics, "An assessment of the UK identity cards bill and its implications: ID cards - UK's high tech scheme is high risk", 2005. Online at http://eprints.lse.ac.uk/741/1/PressRelease_5-09-05.pdf (as of Jan. 2010).

Louis Harris, & Associates, and Alan F. Westin, *Equifax-Harris Consumer Privacy Survey*, New York: Louis Harris & Associates, 1994.

Louviere, J., "Experimental choice analysis: introduction and overview" *Journal of Business Research,* Vol. 24, 1992, pp. 89-96.

Louviere, J. and G. Woodworth, "Design and analysis of simulated consumer choice or allocation experiments: an approach based on aggregated data" *Journal of Marketing Research,* Vol. 20, 1983, pp. 350-367.

Louviere, Jordan J., David A. Hensher, and Joffre D. Swait, *Stated Choice Methods: Analysis and Application*, Cambridge: Cambridge Press, 2000.

McCahill, M and C. Norris, "CCTV in London, Urbaneye Working Paper No. 6, RTD-Project, 5th Framework Programme of the European Commission", 2002. Online at www.urbaneye.net/results/ue_wp6.pdf (as of Jan. 2010).

McFadden, Daniel, "Conditional logit analysis of qualitative choice behaviour" in *Frontiers in Econometrics*, Zerembka, P., ed. New York: Academic Press, 1973, pp. 105-142.

Merrick, J. , "Security bill for London's 2012 Olympics to hit £1.5bn - triple the original estimate", 2008. Online at http://www.independent.co.uk/news/uk/politics/security-bill-for-londons-2012-olympics-to-hit-16315bn--triple-the-original-estimate-944766.html (as of Nov. 2009).

Miller, R., "The Jack-knife: A Review" *Biometrica,* Vol. 61, 1974, pp. 1-14.

National Audit Office, "Preparations for the London 2012 Olympic and Paralympic Games: Progress Report", Vol. HC: 490 2007-2008, 2008. Online at http://www.nao.org.uk/idoc.ashx?docId=d338b55b-c90f-403b-9e8e-5ca98e691ddf&version=-1.

National Commission, July 22, 2004, "The 9/11 Commission Report on Terrorist Attacks Upon the United States", 2004. Online at http://govinfo.library.unt.edu/911/report/911Report.pdf.

NETC@RDS Project, "A step towards the electronic European Health Insurance Card", 2009. Online at http://netcards-project.com/web/frontpage (as of Jan. 2010).

NISTIR-7349, *Users manual for version 2.0 of the cost-effectiveness tool for capital asset protection*, Gaithersburg, Md.: U.S. Department of Commerce, Technology Administration, National Institute of Standards and Technology. Office of Applied Economics, Building and Fire Research Laboratory, 2006.

Odlyzko, A.M., "Privacy, economics, and price discrimination on the Internet" *ICEC2003: Fifth International Conference on Electronic Commerce*, Pittsburgh, Pennsylvania, USA, 2003, pp. 355-366.

Office of the Privacy Commissioner of Canada, "Privacy Impact Assessment Policy", 2002. Online at http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12450 (as of Jan. 2010).

Omand, D., "The National Security Strategy: Implications for the UK intelligence community" *Commission on National Security for the 21st Century*, 2009. Online at http://www.ippr.org.uk/members/download.asp?f=/ecomm/files/National%20Security%20Strategy.pdf&a=skip (as of Nov. 2009).

Ortuzar, Juan Dios and Luis G. Willumsen, *Modelling Transport*, Third Edition ed., Chichester: John Wiley & Sons, Ltd, 2001.

Pearce, D. and E. Ozdemiroglu, *Economic valuation with stated preference techniques*, Rotherham: Department for Transport, Local Government and the Regions, 2002.

Privacy International, "Privacy International's leading surveillance societies in the EU and the World", 2006. Online at http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-545269 (as of Dec. 2009).

Research Now, "About Us - The International online Fieldwork and Panel Specialists", 2007. Online at http://www.researchnow.co.uk (as of Jan. 2010).

Robinson, L.A., *Valuing Mortality Risk Reductions in Homeland Security Regulatory Analyses prepared for U.S. Customs and Border Protection, Department of Homeland Security*, 2008.

Rouwendal, J. and T. Arianne De Blaeij, "Inconsistent and lexicographic choices in stated preference analysis" Tinbergen Institute Discussion Paper, Dept. of Economics, Amsterdam, Netherlands, Free University of Amsterdam, 2004.

Ryan, M., A. Bate, C.J. Eastmond, and A. Ludbrook, "Use of discrete choice experiment to elicit preferences" *Quality in Health Care,* Vol. 10, No. Supplement 1, 2001, pp. i55-i60.

Stewart, M.G. and J. Mueller, "Cost Benefit Assessment of United States Homeland Security Spending Research, Report No. 273.01.2009", 2009. Online at http://hdl.handle.net/1959.13/33114.

STORK Project, "Secure Identity Across Borders Linked (STORK) Project", 2009. Online at http://www.eid-stork.eu/ (as of Nov. 2009).

Taylor, H., "Most People Are "Privacy Pragmatists" Who, While Concerned about Privacy, Will Sometimes Trade It Off for Other Benefits: The Harris Poll No. 17", 2003. Online at http://www.harrisinteractive.com/harris_poll/index.asp?PID=365 (as of Nov. 2009).

The Daily Telegraph, "Shami Chakrabarti answers your questions, December 3rd", 2007. Online at http://www.telegraph.co.uk/news/yourview/1571330/Shami-Chakrabarti-answers-your-questions.html (as of Jan. 2010).

The Daily Telegraph, "Yard is watching thousands of terror suspects", 2006. Online at http://www.telegraph.co.uk/news/1527844/Yard-is-watching-thousands-of-terror-suspects.html (as of Dec. 2009).

The Guardian, "MI5: 30 terror plots being planned in the UK, November 10th ", 2006. Online at http://www.guardian.co.uk/uk/2006/nov/10/politics.topstories3 (as of Jan. 2010).

The Job, *Ready for an Olympic Task*, London Metropolitan Police, 2008

The Times, "Biometrics Screening for Olympic Workers, 5th March", 2009. Online at http://www.timesonline.co.uk/tol/sport/olympics/london_2012/article3486089.ece (as of Jan. 2010).

The Times, "Heathrow Show of Force after terror alert, Feb 12th", 2003. Online at http://www.timesonline.co.uk/tol/news/world/article874722.ece (as of Jan. 2010).

Thomas, R., "Waking up to a surveillance society", 2006. Online at http://www.ico.gov.uk/upload/documents/pressreleases/2006/waking_up_to_a_surveillance_society.pdf (as of Jan. 2010).

Thornton, A. and A. Goldstein, "Transport Security Measures: Attitudes towards and acceptability of Security screening trial at Greenford station: " 2006. Online at http://www.dft.gov.uk/pgr/security/sectionsocresearch/security/greenford/greenfordqualtrial.pdf (as of Jan. 2010).

Train, Kenneth, *Discrete Choice with Simulations*, Cambridge: Cambridge University Press, 2003.

Travis, A., "Poll shows growing opposition to ID cards over data fears" *The Guardian*, 2008. Online at http://www.guardian.co.uk/uk/2008/feb/06/politics.idcards (as of Nov. 2009).

UK Dept. for Transport, "Research findings: Attitudes to transport security after July 2005 London bombings", 2005. Online at http://www.dft.gov.uk/pdf/pgr/security/sectionsocresearch/attitudestotransportsecurity (as of Dec. 2009).

UK Dept. for Transport, "Responsibilities of Transport Security's Land Transport Division", 2006. Online at http://www.dft.gov.uk/pgr/security/land/responsibilitiesoftransports4898 (as of Nov. 2008).

UK Dept. for Transport, "Summary report of the 'LUNR' passenger screening trials", 2008a. Online at http://www.dft.gov.uk/pgr/security/land/lunr (as of Dec. 2008).

UK Dept. for Transport, "Transport Security Directorate (TRANSEC) - Annual report to the Secretary of State for Transport April 2007-March 2008", 2008b. Online at http://www.dft.gov.uk/pgr/security/about/transecannualreports/transecannualreport0708.pdf (as of Nov. 2009).

Viscusi, W.K., "The Value of Life in Legal Contexts: Survey and Critique" *American Law and Economics Association,* Vol. 2, No. 1, 2000, pp. 195-222.

Westin, A., L. Harris, and Associates, *Equifax-Harris Consumer Privacy Survey*: Tech rep. Conducted for Equifax Inc, 1994.

Willis, Henry H., Tom LaTourrette, Terrence K. Kelly, Scot Hickey, and Neill Samuel, "Terrorism Risk Modelling for Intelligence Analysis and Infrastructure Protection", 2007 Online at http://www.rand.org/pubs/technical_reports/TR386/ (as of Oct. 2009).

ZDNet, "Security management toolkit: Government U-turns on passport pledge", 2009. Online at http://news.zdnet.co.uk/security/0,1000000189,39783123,00.htm (as of Nov. 2009).

APPENDICES

Appendix A: Survey questionnaire

Introduction

As part of an independently funded research study, RAND Europe* is conducting a survey of the general public to investigate individual preferences about privacy, security and liberty in the context of travel, attendance at events and passport application.

The results of this research will be made publicly available on the RAND Europe website and in presentations and openly published research papers.

Your responses will be anonymous and treated confidentially.

This survey is split into five parts.

- The first part asks you some background questions about yourself.
- The second part asks some introductory questions about how often you use public transport, whether you have a passport and your attendance at major public events.
- The third part asks you to provide your preference in a series of choice exercises for three different scenarios, including issuing a new passport, travelling on the national rail system and attending a major public event. There are eight choice exercises per scenario.
- The fourth part asks you general questions about your attitudes toward security, liberty and privacy.
- Finally, the last part asks you some short questions about your media preferences.

If you would like more information on this survey, please contact Neil Robinson at RAND Europe on 01223 353329 or Neil_Robinson@rand.org.

*RAND Europe is an independent, not-for-profit research organisation based in Cambridge. We produce objective and evidence-based research to help those in government deal with important concerns in areas such as healthcare, security and transportation.

Your background

Are you…?

1. Male
2. Female

How old are you?

1. 18–24
2. 25–34
3. 35–44
4. 45–54
5. 55–64
6. 65+

What level of qualifications do you hold?

1. None
2. O-level/GCSE
3. A-level/CSE
4. Graduate

Are you currently…?

1. Working full time
2. Working part time
3. Student
4. Retired
5. Seeking work
6. Other (please state)

How would you describe the place where you live?

1. Inner London Area (e.g. Earls Court, Kensington or Holborn)
2. Outer London Area (e.g. Enfield or Hounslow or Croydon)
3. Other large city (e.g. Bristol, Manchester or Leeds)
4. Medium-sized city (e.g. Exeter, Sutton Coalfield or Blackburn),
5. Small town (e.g. Buxton, St Ives or Oswestry)
6. Rural area (e.g. Lake District or Dartmoor)

What is your postcode?

This information is for research purposes only and will not be passed on to any third parties. You may enter the first part of your postcode in the first box, the full postcode or leave it blank.

What is your country of birth?

1. England
2. Wales
3. Scotland
4. Northern Ireland
5. Republic of Ireland
6. Elsewhere

What is your ethnic group?

1. White
    - 11 British
    - 12 Irish
    - 13 Any other White background (please write in)
2. Mixed
    - 21 White and Black Caribbean
    - 22 White and Black African
    - 23 White and Asian or any other mixed background (please write in)
3. Asian or Asian British
    - 31 Indian
    - 32 Pakistani
    - 33 Bangladeshi
    - 34 Any other Asian background (please write in)
4. Black or Black British
    - 41 Caribbean
    - 42 African
    - 43 Any other Black background (please write in)
5. Chinese or other ethnic group
    - 51 Chinese
    - 52 Any other (please write in)

Introductory questions

How often do you use a bus for travel?

1. More than once a day
2. Once a day
3. Two or three times a week
4. One or two times a week
5. Three or four times a month
6. Once or twice every two months
7. A couple of times a year
8. Do not use buses

How often do you use the rail network (including Underground, monorail or tram networks)?

1. More than once a day
2. Once a day
3. Two or three times a week
4. One or two times a week
5. Three or four times a month
6. Once or twice every two months
7. A couple of times a year
8. Do not use rail

How often do you attend public events (e.g. sporting activities, concerts exhibitions, etc)?

1. Once a week
2. Two or three times a month
3. Once or twice every three months
4. Once every year
5. Less than once a year
6. Never

Has your frequency of attending events changed over the last 3 years?

1. Yes
2. No
3. Do not know/refuse

Finally, we would like to know if you have a passport and how often you travel abroad.

Do you have a passport?

1. Yes
2. No

When your passport was last renewed?

<<*YEAR*>>

In which country was this issued?

<<*LIST OF COUNTRIES*>>

How frequently do you travel abroad?

1. Never
2. Once a week
3. Once a month
4. Once every six months
5. Once a year
6. Once every three years or longer

Stated choice scenarios

In this section, we will present you with different scenarios related to three situations when applying for a passport, travelling on the national rail system, or attending a major public event.

Passport application

Imagine you are applying for a new style[24] passport **for the first time or in order to renew your old passport.** During the application process there are a number of factors associated with this, such as the price, processing time, type of personal information required and the way your personal data are stored and possibly shared with other organisations.

Following this screen we will present you with a total of eight choice cards and each card presents you with three alternative situations, named Option 1, Option 2 and Option 3, under which you may obtain your new passport. Each option is described with a set of characteristics including:

- **Price** in British pounds (£) and refers to the total price of passport.
- **Processing time.** This is the time required to receive the passport after you successfully submitted your application and necessary paperwork. In the following scenarios, the processing time varies from the same day up to four weeks.
- **Type of personal information required.** This refers to your personal data that must be collected and are held as means to categorically identify you. These requirements range from a photograph to a DNA sample. The scenarios presented in the following card may include:
    - **photograph –** that is, you need to supply a photograph of a standard size and quality;
    - **photograph and fingerprint scans** – that is, the application requires a standard size and quality photograph and an electronic reading is taken of your fingerprint;
    - **photograph and iris scan** – in this case, the application requires a standard size and quality photograph and an electronic reading is taken of your iris (retina) by looking into a machine;
    - **photograph and DNA sample** – in this case the application requires a standard size and quality photograph and a sample of DNA is taken and transferred into an electronic database
- **Level of sharing of passport data**: Your personal data collected may be stored in variety of ways either within government or by other agencies or organisations. The different levels of data sharing included in the following exercises include:
    - **only within the Identity and Passport Service (IPS)**

[24] A new style passport is one containing biometric information such as a facial biometrics and where the data is entered into the National Identity Register (NIR)

    - **across government generally** that is within other government department other than the Identity and Passport Service
    - **within the private sector**, for example companies that need to identify you (e.g. banks, insurance companies or healthcare providers)
    - **with other European Union (EU) countries** as for example to facilitate easier travel, working or living in Europe
- **Additional uses of passport**. New identity documents will be linked into the National Identity Register (NIR), a database that may support identification across a whole range of government and business activities. In this way as well as using your passport to enter or exit a country the data can be used:
    - **as personal identification document**, e.g. that you can provide when completing your tax return or applying for a bank account.
    - **as personal identification document & to speed up the processing time for official forms & documents** e.g. so you don't have to repeat entering the same information such as your address, name, date of birth etc
- **Number of illegal immigrants identified**: Currently, one of the functions of these new identity documents such as passports will be to support the fight against illegal immigration. In the following exercises, the number of illegal immigrants that may be identified range between 75,000 to 1,000,000.
- **Number of terrorists identified**: It has been said that new style identity documents such as passports will help identify terrorists. In this exercise, the number of terrorists identified range between "Less than 750" to "More than 3200" based on government estimates

Please, consider each case carefully and indicate your choices concerning passport application procedures, in the following 8 scenarios.

<< 8 choice scenarios to follow>>

We would now like to ask you a few questions about the choice exercises that you have undertaken.

Were you able to make the comparisons in the choices we presented you?

1. Yes
2. No

Why weren't you able to make the comparisons in the choices?

Did you feel that the levels of service we have been asking about in the choices were realistic?

1. Yes
2. No
3. Don't know

Why do you think that?

In the choices, did you understand each of the characteristics we described?

1. Yes
2. No
3. Don't know

Which characteristics weren't clear to you? CODE ALL THAT APPLY
1. Total price
2. Processing time
3. Type of personal information required
4. Level of sharing of passport data
5. Uses of passport
6. Number of illegal immigrants that may be identified
7. Number of terrorists that may be identified

Which passport enrolment characteristic was most important to you?
1. Total price
2. Processing time
3. Type of personal information required
4. Level of sharing of passport data
5. Uses of passport
6. Number of illegal immigrants that may be identified
7. Number of terrorists that may be identified

Which service characteristic was second most important to you?
1. Total price
2. Processing time
3. Type of personal information required
4. Level of sharing of passport data
5. Uses of passport
6. Number of illegal immigrants that may be identified
7. Number of terrorists that may be identified

And were any characteristics not at all important to you?
1. Total price
2. Processing time
3. Type of personal information required
4. Level of sharing of passport data
5. Uses of passport
6. Number of illegal immigrants that may be identified
7. Number of terrorists that may be identified
8. All characteristics were important

Travel on the national rail system

Now, we would like you to imagine that you are making a journey using public transport, such as on the national railway system. We would like you then to consider three ways in

which you might make this journey. These are described by the following levels of security or privacy:

- **Type of camera** at the station premises. Situations in the following scenarios can vary from:
  - **none**. no cameras at all.
  - **standard CCTV cameras**
  - **standard CCTV cameras and new cameras that automatically identify individuals**
- **Time required to pass through security.** The total time it takes to pass through security between the station concourse and the platform including queuing up, presenting your ticket and entering and exiting any security barriers. In the following scenarios, time may vary between 1 and 15 minutes.
- **Type of security check**. The type of security checks that you have to go through when passing from the station concourse to the platform. These may include the following:
  - **no checks** at all
  - **"pat-down" and bag search for 1 in 1000 travellers**. One in every 1,000 travellers may have to undergo a thorough hand search of their person and looking through their bag(s) by security officials as sometimes happens at airports
  - **"pat-down" and bag search for 2 in 1000 travellers**
  - **"pat-down" and bag search for 10 in 1000 travellers**.
  - **Metal detector / X-ray for all** in addition to placing bags and possessions on a conveyor belt to go through an X-ray machine, all passenger may be asked to walk through a metal arch in order to detect particular types of object
- **Presence of the following type of security personnel.** There may be different forms of security personnel on typical journey, ranging from the usual rail network personnel to British Transport Police or even armed police. In particular, scenarios may involve:
  - **rail staff**. uniformed staff from the rail operator (e.g. Virgin Trains) are only present
  - **rail staff and British Transport Police**. uniformed staff from the rail operator and uniformed specialised transport police are present
  - **rail staff, British Transport Police and armed police.** uniformed staff from the rail operator, uniformed specialised transport police and uniformed police carrying firearms are present
  - **rail staff, British Transport Police, armed police and uniformed military.** uniformed staff from the rail operator, uniformed specialised transport police, uniformed police carrying firearms and military personnel in combat dress are present
- **Increase on price of ticket to cover security.** The additional cost onto a ticket to cover security measures. The increase in the price of the ticket may range from £0.75 to £3
- **Number of known terrorist plots disrupted**. The number of ongoing terrorist conspiracies known to security authorities that could be disrupted due to security

measures. Although ideally all terrorist plots would be stopped or disrupted, realistically a conservative estimate of the most that might be stopped or disrupted is 2-3 major plots every year. Scenarios range between "1 plot disrupted every 10 years" to "20 plots disrupted every 10 years"

- **Visibility of response to a security incident**. How the rail network staff, police and other security staff respond to a security incident due to increased security measures. In the scenarios presented the following cases apply:
  - **If an incident occurs you are not aware of it**
  - **If an incident occurs then you are aware of that when you get back home**
  - **If an incident occurs things are handled with minimal disruption**
  - **If an incident occurs there is some disruption and chaos**
  - **If an incident occurs there is lots of disruption and chaos**

Please, indicate your choices concerning travel, in the following 8 scenarios.

<< 8 choice scenarios to follow>>

Were you able to make the comparisons in the choices we presented you?

1. Yes
2. No

Why weren't you able to make the comparisons in the choices?

Did you feel that the levels of service we have been asking about in the choices were realistic?

1. Yes
2. No
3. Don't know

Why do you think that?

In the choices, did you understand each of characteristics we described?

1. Yes
2. No
3. Don't know

Which characteristics weren't clear to you?

1. Type of camera
2. Time required to pass through security
3. Type of security check
4. Presence of the following on a typical journey
5. Increase on price of ticket to cover security
6. Number of known terrorist plots disrupted
7. Visibility of response to a security incident

Which characteristic was most important to you?

1. Type of camera
2. Time required to pass through security
3. Type of security check

4. Presence of the following on a typical journey
5. Increase on price of ticket to cover security
6. Number of known terrorist plots disrupted
7. Visibility of response to a security incident

Which characteristic was second most important to you?
1. Type of camera
2. Time required to pass through security
3. Type of security check
4. Presence of the following on a typical journey
5. Increase on price of ticket to cover security
6. Number of known terrorist plots disrupted
7. Visibility of response to a security incident

And were any of the service characteristics not at all important to you?
1. Type of Camera
2. Time required to pass through security
3. Type of security check
4. Presence of the following on a typical journey
5. Increase on price of ticket to cover security
6. Number of known terrorist plots disrupted
7. Visibility of response to a security incident
8. All characteristics were important

Attending a major public event

Finally, imagine you are attending the opening ceremony of the 2012 Olympics or any sort of large-scale public event such as a football match or music concert. Again, we would like you to consider carefully the different ways that the event is managed through the following eight scenarios. Again, each scenario involved three alternative options, which have different implications e.g. on the cost of your ticket and amount of personal information you have to provide to enter the stadium or arena. In particular, the different factors involved are as follows:

- **Delay to pass through security.** The time it takes to queue, pass through the turnstile and other security measures and enter the stadium. The time to pass through security ranges between "15 mins or less" to "2-3 hours".

- **Security check types**. Security check may involve different types including:
    - **bag search & questioning**. security officials may look through bags and question persons as sometimes happens at airports
    - **"Pat down"**. individuals may undergo a thorough hand search of their person by security officials as sometimes happens at airports

  - **Metal detector / X-ray**. in addition to placing bags and possessions on a conveyor belt to go through an X-ray machine, all passenger may be asked to walk through a metal arch in order to detect some forms of object regarded as suspicious

- **Type of identity check required upon arrival.** Different types of identity check may be required upon arrival at the stadium, ranging from presenting your ticket to more in-depth forms of identity check such as having a photograph, fingerprint scan or iris-scan taken and verified against a database to identify individuals of interest to the security authorities.

- **Type of security personnel**. A variety of personnel may be used to maintain security. Scenarios may include:
  - **stewards** that is staff identified as employees of the stadium
  - **private security officials** that is private contractors (e.g. security guards) hired by the stadium
  - **Police Community Support Officers (PCSOs)** that is police support staff providing a visible and uniformed presence
  - **police officers** that is uniformed police officers
  - **armed police** that is uniformed police carrying firearms
  - **uniformed military** that is military personnel in combat dress

- **Location of security personnel**. Security personnel may be stationed in different places at the stadium. Case may include instance where security personnel are visible (at the turnstile, on the way to stadium, etc) or not visible (e.g. in a control room).

- **Additional costs on ticket to cover security**. Increase in ticket price to cover security e.g. an additional £4 would mean a 10% increase on the estimated average ticket price of £40 for the London 2012 Olympics. The cost range in the scenarios may range from £0 to over £4.

- **Visibility of response to a security incident.** How the stadium stewards, police and other security staff respond to a security incident. In the scenarios presented the following cases apply:
  - **If an incident occurs you are not aware of it**
  - **If an incident occurs then you are aware of that when you get back home**
  - **If an incident occurs things are handled with minimal disruption**
  - **If an incident occurs there is some disruption and chaos**
  - **If an incident occurs there is lots of disruption and chaos**

We would again like you to look carefully at the following eight scenarios and indicate your choices concerning attendance at the event.

<< 8 choice scenarios to follow>>

We would now like to ask you a few questions about the choice exercises that you have undertaken.

Were you able to make the comparisons in the choices we presented you?

1. Yes
2. No

Why weren't you able to make the comparisons in the choices?

Did you feel that the levels of service we have been asking about in the choices were realistic?

1. Yes
2. No
3. Don't know

Why do you think that?

In the choices, did you understand each of the characteristics we described?

1. Yes
2. No
3. Don't know

Which of the characteristic weren't clear to you?

1. Delay to pass through security checks
2. Security check types
3. Type of identity check required upon arrival
4. Type of security personnel
5. Location of security personnel
6. Additional costs on ticket to cover security
7. Visibility of response to a security incident

Which characteristic was most important to you?

1. Delay to pass through security checks
2. Security check types
3. Type of identity check required upon arrival
4. Type of security personnel
5. Location of security personnel
6. Additional costs on ticket to cover security
7. Visibility of response to a security incident

Which characteristic was second most important to you?

1. Delay to pass through security checks
2. Security check types
3. Type of identity check required upon arrival
4. Type of security personnel
5. Location of security personnel
6. Additional costs on ticket to cover security

7. Visibility of response to a security incident

And were any of the characteristics not at all important to you?

1. Delay to pass through security checks
2. Security check types
3. Type of identity check required upon arrival
4. Type of security personnel
5. Location of security personnel
6. Additional costs on ticket to cover security
7. Visibility of response to a security incident
8. All characteristics were important

Attitudes

We would now like to present you with some general statements about security, liberty and privacy and ask you to indicate how important these are to you.

	Very important	Somewhat important	Not very important	Not at all important	Don't know
Protecting the privacy of my personal information is…					
Taking action against important security risks (e.g. international terrorism, organised crime) is…					
Defending current liberties and human rights is…					

Please indicate the extent to which you agree or disagree with the following:

Distrust Index	Agree strongly	Agree somewhat	Disagree somewhat	Agree strongly	Don't know
Technology has almost got out of control					
Government can generally be trusted to look after our interests					
The way one votes has no effect on what the Government does					
In general business helps us more than it harms us					

Post questions

Finally, we would like to ask you some questions about what sort of newspaper you read and your income and religion.

What daily newspaper do you normally read?

1. The Sun
2. The Daily Mail
3. The Daily Mirror
4. The Daily Telegraph
5. The Times
6. The Guardian
7. The Independent
8. Daily Express
9. Other, please specify
10. Do not read a newspaper

What TV news channel do you normally watch?

1. BBC News
2. ITV News
3. Sky News
4. CNN News
5. Fox News
6. Channel 4
7. Other, please specify
8. Do not watch news channels

What is your annual income, including all persons in your household?

1. Under £4,999
2. £ 5,000 - £10,000
3. £10,000 - £19,999
4. £20,000 - £29,999
5. £30,000 - £39,999
6. £40,000 - £49,999
7. £50,000 - £59,999
8. £60,000 - £69,999
9. £70,000 - £79,999
10. £80,000 - £89,999
11. £90,000 - £99,999
12. £100,000 or higher

What is your religion?

1. Christian
2. Buddhist
3. Hindu
4. Jewish
5. Muslim
6. Sikh
7. Another religion, please specify
8. Would rather not say
9. None

Thank you very much for participating in this survey. If you have any further comments on the questions in this survey or wish to add anything please use the box below

Comments:

<<*Comment box*>>

RAND Europe is an independent not for profit research organisation based in Cambridge, United Kingdom. We produce objective and evidence based research to help those in government deal with important concerns in areas such as healthcare, security and transportation.

If you would like more information on this survey, please contact Neil Robinson at RAND Europe on 01223 353329 or Neil_Robinson@rand.org

Appendix B: Definition of attributes and levels

Passport application scenario

Total price	The total price of passport in British pounds (£)
Processing time	The time required to receive the passport after you successfully submitted your application and necessary paperwork. In the following scenarios, the processing time varies from the same day up to four weeks.
Type of personal information required	Refers to your personal data that must be collected and are held as means to categorically identify you. These requirements range from a photograph to a DNA sample. The scenarios presented in the following card may include: ○ **photograph**, that is you need to supply a photograph of a standard size and quality ○ **photograph & fingerprint scan**, that is the application requires a standard size and quality photograph and an electronic reading is taken of your fingerprint ○ **photograph & iris-scan**, in this case the application requires a standard size and quality photograph and an electronic reading is taken of your iris (retina) by looking into a machine ○ **photograph & a DNA sample**, in this case the application requires a standard size and quality photograph and a sample of DNA is taken and transferred into an electronic database
Level of sharing of passport data	Your personal data collected may be stored in variety of ways either within government or by other agencies or organisations. The different levels of data sharing included in the following exercises include: ○ **only within the Identity and Passport Service (IPS)** ○ **across government generally**, that is within other government department ○ **within the private sector**, for example companies that need to identify you ○ **with other European Union (EU) countries** as for example to facilitate easier travel, working or living in Europe
Additional uses of passport	New identity documents will be linked into the National Identity Register, a government database that may support identification across a whole range of government and business activities. In this way as well as using your passport to enter or exit a country the data can be used: ○ **as personal identification document**, e.g. that you can provide when completing your tax return or applying for a bank account. ○ **as personal identification document & to speed up the processing time for official forms & documents** e.g. so you don't have to repeat entering the same information such as your address, name, date of birth, etc.
Number of illegal immigrants identified	Currently, one of the functions of these new identity documents such as passports will be to support the fight against illegal immigration. In the following exercises, the number of illegal immigrants that may be identified range between 75,000 and 1,000,000.
Number of terrorists identified	It has been said that new style identity documents such as passports will help identify terrorists. In this exercise, the number of terrorists identified range between "Less than 750" to "More than 3200" based on government estimates.

Travel on the national rail system

Type of camera	Situations in the following scenarios may vary from: ○ **None**. no cameras at all. ○ **Standard CCTV cameras** ○ **Standard CCTV cameras and new cameras that automatically identify individuals**
Time required to pass through security	The total time it takes to pass through security between the station concourse and the platform including queuing up, presenting your ticket and entering and exiting any security barriers. In the following scenarios, time may vary between 1 and 15 minutes.
Type of security check	The type of security checks that you have to go through when passing from the station concourse to the platform. These may include the following: ○ **no checks** at all; ○ **pat-down and bag search for 1 in 1000 travellers**. one in every 1,000 travellers may have to undergo a thorough hand search of their person and, looking through their bag(s) by security officials as sometimes happens at airports ○ **pat-down and bag search for 2 in 1000 travellers** ○ **pat-down and bag search for 10 in 1000 travellers** ○ **metal detector / X-ray for all** in addition to placing bags and possessions on a conveyor belt to go through an X-ray machine; all passengers may be asked to walk through a metal arch in order to detect particular types of object
Presence of the following type of security personnel:	There may be different forms of security personnel on typical journey, ranging from the usual rail network personnel to British Transport Police or even armed police. In particular, scenarios may involve: ○ **rail staff**. uniformed staff from the rail operator (e.g. Virgin Trains) are only present; ○ **rail staff and British Transport Police**. uniformed staff from the rail operator and uniformed specialised transport police are present; ○ **rail staff, British Transport Police and armed police.** uniformed staff from the rail operator, uniformed specialised transport police and uniformed police carrying firearms are present; ○ **rail staff, British Transports Police, armed police and uniformed military.** uniformed staff from the rail operator, uniformed specialised transport police, uniformed police carrying firearms and military personnel in combat dress are present.
Increase on price of ticket to cover security	The additional cost onto a ticket to cover security measures. The increase in the price of the ticket may range from £0.75 to £3
Number of known terrorist plots disrupted	The number of ongoing terrorist conspiracies known to security authorities that could be disrupted due to security measures. Although ideally all terrorist plots would be stopped or disrupted realistically, a conservative estimate of the most that might be stopped or disrupted is 2-3 major plots every year. Scenarios range between "1 plot disrupted every 10 years" to "20 plots disrupted every 10 years".
Visibility of response to a security incident	How the rail network staff, police and other security staff respond to a security incident due to increased security measures. In the scenarios presented the following cases apply: ○ **If an incident occurs you are not aware of it** ○ **If an incident occurs then you are aware of that when you get back home** ○ **If an incident occurs things are handled with minimal disruption** ○ **If an incident occurs there is some disruption and chaos** ○ **If an incident occurs there is lots of disruption and chaos**

Attending a major public event

Delay in passing through security checks	The time it takes to queue, pass through the turnstile and other security measures and enter the stadium. The time to pass through security ranges between "15 mins or less" and "2-3 hours".
Security check type	Security checks may involve different types including: ○ **bag search and questioning**. security officials may look through bags and question suspicious persons as sometimes happens at airports ○ **pat-down**. individuals may undergo a thorough hand search of their person by security officials as sometimes happens at airports ○ **metal detector / X-ray**. in addition to placing bags and possessions on a conveyor belt to go through an X-ray machine, all passenger may be asked to walk through a metal arch in order to detect particular types of object
Type of identity check upon arrival	Different types of identity check may be required upon arrival at the stadium, ranging from presenting your ticket to more in-depth forms of identity check such as having a photograph, fingerprint scan or iris-scan taken and verified against a database to identify individuals of interest to the security authorities.
Type of security personnel	A variety of personnel may be used to maintain security. Scenarios may include: ○ **stewards** that is staff identified as employees of the stadium ○ **private security officials** that is private contractors (e.g. security guards) hired by the stadium ○ **Police Community Support Officers (PCSOs)** that is police support staff providing a visible and uniformed presence ○ **police officers** that is uniformed police officers ○ **armed police** that is uniformed police carrying firearms ○ **uniformed military** that is military personnel in combat dress
Location of security personnel	Security personnel may be stationed in different places at the stadium. Case may include instance where security personnel are visible (at the turnstile, on the way to stadium, etc) or not visible (e.g. in a control room).
Additional costs on ticket to cover security	Increase in ticket price to cover security, e.g. an additional £4 would mean a 10% increase on the estimated average ticket price of £40 for the London 2012 Olympics. The cost in the scenarios may range from £0 to over £4.
Visibility of response to a security incident	How the stadium stewards, police and other security staff respond to a security incident. In the scenarios presented the following cases apply: ○ **If an incident occurs you are not aware of it** ○ **If an incident occurs then you are aware of that when you get back home** ○ **If an incident occurs things are handled with minimal disruption** ○ **If an incident occurs there is some disruption and chaos** ○ **If an incident occurs there is lots of disruption and chaos**

Appendix C: The jack-knife procedure

The jack-knife is a parametric approach to estimate the 'true' standard errors of estimates in cases where the theory does not provide an exact estimate of the error. It is possible to model explicitly this correlation between observations using panel analysis techniques, and in the case of logit choice models a mixed logit formulation; however, this would necessitate the transfer of the model to a different modelling package where we may find disadvantages in other aspects of the modelling, e.g. having the flexibility in the tree specification to set up a model that allows us to pool the data from across the experiments, etc. For the purposes of this project, therefore, we have employed the jack-knife technique to provide an improved estimate of the standard errors over those provided by the naïve estimation that assumes independence between observations.

The jack-knife works by dividing the sample into R non-overlapping random sub-samples of roughly the same size, where R should be at least 10, and in the case of these runs a value of 30 has been used. The procedure is set up such that all observations from a given individual fall in the same sub-sample. One model is estimated on the full sample and then R additional models are estimated, each excluding one of the sub-samples in turn. Therefore, each estimation is performed on approximately (R-1)/R of the observations.

For a given variable, suppose that we get estimate β_0 from the full sample, and an estimate β_r for each of the sub-samples r = 1 to R.

The jack-knife estimate of β is then:

$$\beta = R * \beta_0 - (R-1)/R * \Sigma_{r=1,R} \beta_r$$

The variance of that estimate is:

$$\sigma^2(\beta) = (R-1)/R * \{ (\Sigma_{r=1,R} \beta_r^2) - (\Sigma_{r=1,R} \beta_r)^2 / R \}$$

In general, the application of the jack-knife procedure to stated preference data has confirmed that the coefficient estimates themselves are not affected greatly by the specification error of assuming independent observations. However, the significance of the coefficient estimates often is substantially overstated by the naïve estimation. Thus, when there is an important issue about the significance of a specific variable, it is necessary to test that variable in a jack-knife procedure rather than in a naïve estimation. Generally it is found that when variables are significant at very high levels in a naïve estimation, they remain significant in the jack-knife estimation; but when the significance of a variable in the naïve estimation is marginal, a jack-knife estimation may show that it is not truly significant.