Security, at what cost? A stated preference approach toward understanding individuals' privacy and civil liberties trade-offs regarding security measures[1]

Neil Robinson & Dimitris Potoglou[2]
RAND Europe, Westbrook Centre, Milton Rd., Cambridge, CB4 1YG
e-mails: neilr@rand.org; dimitris@rand.org

Abstract

In the presently heightened security environment there are a number of examples of 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 data informs these arguments. This paper outlines the results of a study that sought to objectively understand the real privacy, liberty and security trade-offs of individuals, so that policymakers can be better informed about individuals' preferences in this area.

1. Background and Context

1.1 The problem

Those responsible for the protection of critical infrastructures such as transportation networks or physical assets often have to make difficult decisions in the face of extensive uncertainty regarding the imposition of security measures to mitigate the risks from a

[1] *The authors are grateful to the RAND Europe Board of Trustees, without whose support this study would not have been possible*

[2] *Also at OTB Research Institute, Delft University of Technology, Delft, Netherlands*

particular threat. Where individuals are involved in critical infrastructures (as user or consumers of a service or product that the specific CI sector provides) their civil liberties or privacy may be affected.

1.1.1 Security measures

Contemporary examples of security measures that affect privacy or civil liberties include:

- New forms of x-ray and radar scanning technologies which are increasingly being deployed at airports following the attempted bombing of a Delta Airlines civilian passenger aircraft in the United States on Christmas Day 2009.
- Closed Circuit Television (CCTV) footage was used in the identification of those responsible for bombing the London Underground in 2005 as they entered into the transportation network at Luton rail station. More advanced forms of CCTV with facial recognition capabilities are coming into mainstream use.
- Fingerprint identification, facial recognition systems and other 'biometric' identification systems that use digitised biological data to uniquely identify an individual are increasingly deployed in order to aid in identification.
- Personal data collected from a wide variety of sources is increasingly shared, mined and distributed to support intelligence efforts on terrorist suspects. Examples include the use of Passenger Name Record data and the monitoring of financial data from the Society for Worldwide Interbank Financial Transactions SWIFT network. (Article 29 Working Party of the EU Data Protection Directive, 2006).

1.1.2 Current approaches to understanding individuals views on security infrastructure

Existing attempts to provide an evidence base for understanding the preferences and views of users of security measures are 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 practically faced 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 (Kumaraguru and Cranor, 2005), a Gallup Organisation Flash Eurobarometer survey conducted for the European Commission (Gallup Organisation - Hungary, 2008); a British Social Attitudes Survey (Johnson and Gearty, 2007) and tracking research conducted for the Home Office National Identity Scheme (Central Office of Information Research Unit, 2008). These approaches suffer from three main challenges:

- 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;
- 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?'
- 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.

2. 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, liberty and security.

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.

As national security and privacy may be considered as examples of non-market public goods (such as healthcare or the environment), there is some validity in the application of these techniques in 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. Appendix 2 describes in more detail the characteristics and analysis of a SPDCE.

2.1 Research Question

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).

2.2 Case Studies

We began by conducting a literature review on the topic and three semi-structured interviews with proponents of all sides of the security–civil liberties debate. We then devised a set of real-life choice contexts in which we presented the experimental methodology, in order to circumvent the difficulties of dealing with abstract and difficult to define concepts with respondents. These were:

- *Application for a passport* – where privacy and convenience (e.g. obtaining the passport early) may interact given the requirements to capture various forms of biometric information upon application.
- *Travelling on the national rail network* – where security and inconvenience interact as individuals may be subject to different forms of checks or under the scrutiny of CCTV cameras.
- *Attendance at a major public event* where again security and inconvenience come into play as there may be a presence of security officials, delay to go through security checks and monitoring of individuals.

Once the attributes of each case study were identified, 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 (realistic) changes of the reference values within a realistic context, known as levels.

The data we used to generate the attributes and 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, 2008) and reviewed security measures trialled at stations on the UK rail infrastructure (UK Dept. for Transport, 2008).

The experiment was administered via a web-browser. An example of the presentation of the instrument is shown in Figure 1. Respondents had the opportunity to click hyperlinks to discover a more detailed description about each measure, as well as the option to opt out of participating in the scenario under any circumstances.

Figure 1 ***Example of a choice scenario in the case of passport application***

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	I would opt not to have a passport under any of these conditions
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	
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:	○	○	○	○

2.3 Data collection

The stated choice experiments were conducted through the Internet between 17 and 19 September 2008.[4] 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 1, 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

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

Table 1). 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.

We also collected responses with regard to attitudes relevant to 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. Finally, based on newspaper preferences, the respondents were classified into conservative (55.8%) and non-conservative (44.2%).

Table 1 Sample characteristics compared to 2001 UK Census

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	32	19.8
higher	-	6.9
Other		
Occupational		
status	42	59.6
Working full time	16	
Working part-time	4	7.2
Student	28	13.4
Retired	3	4.5
Seeking work	7	15.3
Other		
Income		
Less than	58	
£30,000	26	
£30,000–	2	
£69,999	14	
£70,000 or		
higher		
Not reported		

2.4 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 various aspect of the respondents' socio-economic and demographic status.

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.[5] 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

[5] 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.

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 4.) This procedure was applied to all models, in order to provide corrected estimates of the coefficients and their standard errors.

2.4.1 Willingness to Pay

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). Further detail on how we derived WTP is contained at Appendix 4.

3. Results and discussion

3.1 Passport application

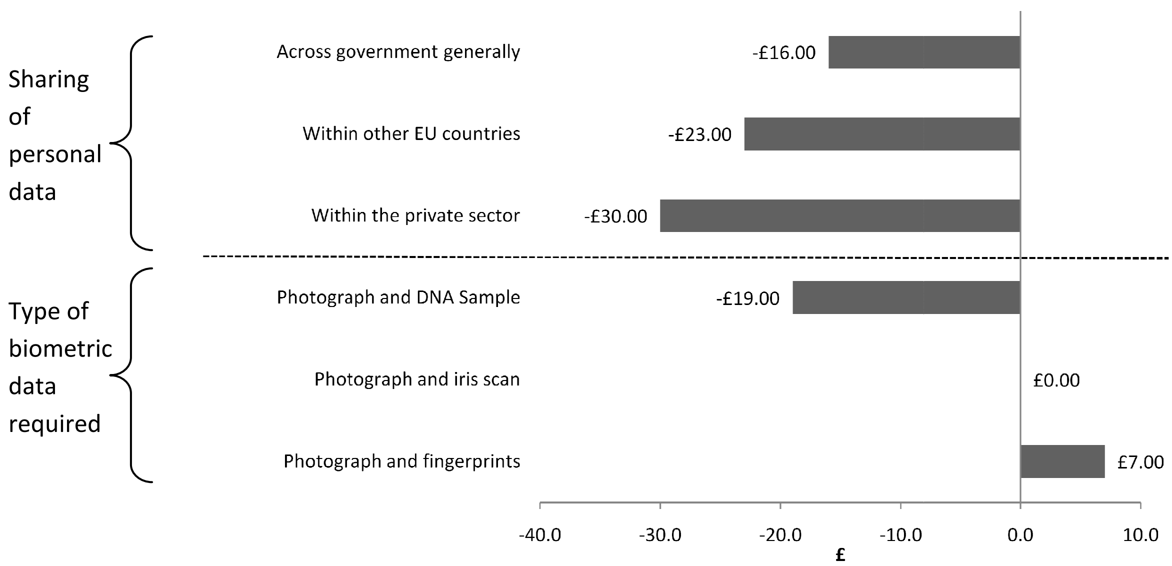
Under current UK policy, the process of applying for a passport has become an event where concerns over privacy and civil liberties, set against the larger requirements of national security, have come to the fore. Citizens are expected to submit a significant quantity of personal data with their passport 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.

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, the National Identity Register (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 attributes and their levels used in the choice experiment are shown in Table 2-3 in Appendix 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.

Figure 2 Willingness to Pay for Security Measures in the Passport Application Case Study



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, 2008). 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.

3.2 Travel on the national rail network

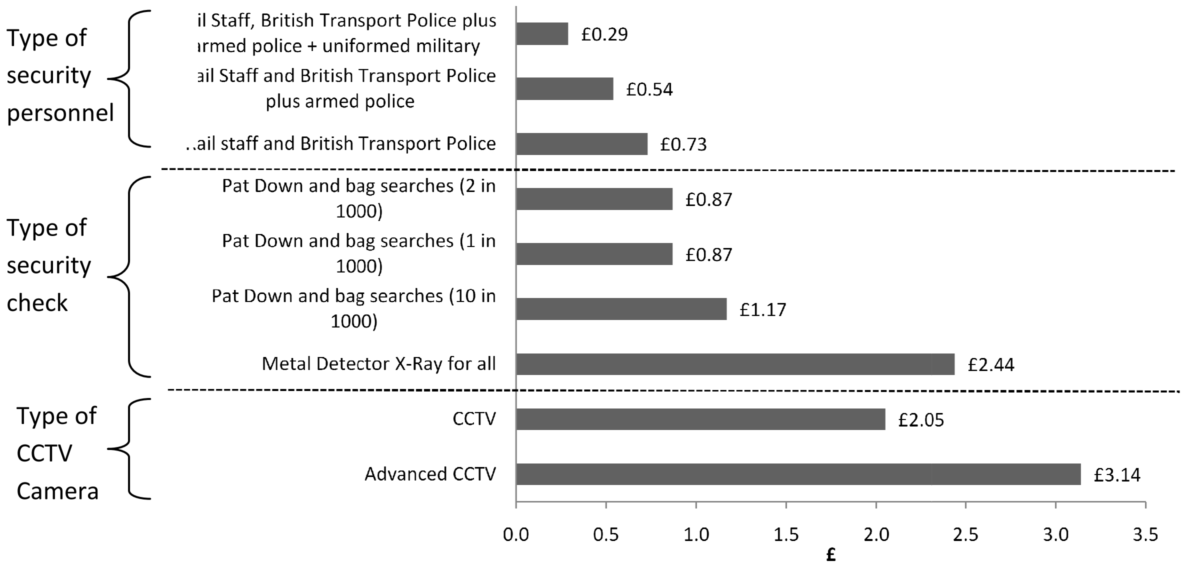
Following terrorist attacks targeting public transport systems worldwide, safety and security have become a top priority in the policy agenda of many countries, and particularly the UK. Security measures for air travel have historically received a great deal of attention, but security authorities are now increasingly focusing upon land-based mass transit systems. These have become a target for terrorist groups due to their vulnerability and ease of access arising from their intrinsically open nature. Additionally, mass transit systems can be both the means and the target for the attack. Terrorists understand how the widespread use of such transportation infrastructure under the fear of terrorist attack has the potential to cause mass panic, disruption and fear. A range of measures may be adopted by authorities in seeking to deal with these challenges. In the UK, these have included legislation and regulations as well as other measures such as campaigns raising awareness of the risk of attacks. Additionally, the UK Department of Transport's Transport Security and Contingencies Team (TRANSEC) (UK Dept. for Transport, 2006) has an important role to play in regard to security arrangements for multi-modal transportation systems. The picture is complicated by the fact that many of these transportation systems are privately owned.

The complete list of attributes and levels used in the choice experiment is shown in Table 4-5 in Appendix 1.

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).

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.

Figure 3 Willingness to Pay for Security Measures in the Rail Travel 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.

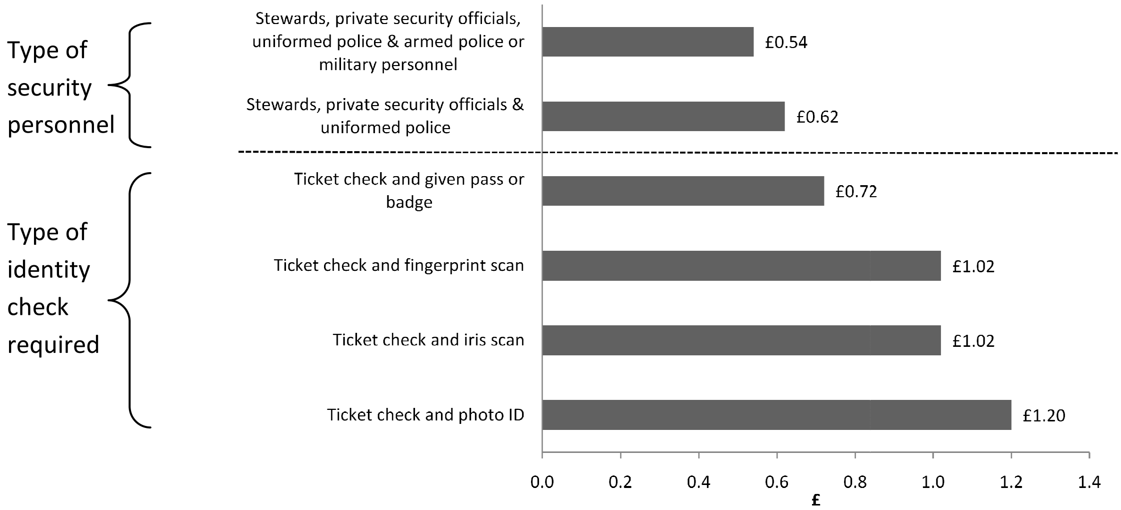
Finally, and somewhat unsurprisingly, there was a high degree of comfort expressed for more specialised security personnel, up to a point. Despite the perception in the security community that the deployment of armed police or the military creates a fearful atmosphere, in all cases the respondents were 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.

3.3 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. Concern regarding security risks to major sporting or entertainment events is widespread particularly given terrorist attacks at for example the Munich Olympics in 1972 and the bombing of the Conservative Party Conference in Brighton in 1984. Such events are of concern for the authorities due to the large concentration of members of the public (so called 'crowded places') and have been recognised as preferred terrorist targets (HM Government, 2006) and the complexity of managing security due to the porous nature of the perimeter to many venues. For the London Olympics in 2012, a number of security measures are being considered including various types of monitoring and access control, overhead surveillance and CCTV (Merrick, 2008), (The Job, 2008). The complete list of attributes and levels used in the choice experiment is shown at Tables 6-7 in Appendix 1.

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.

Figure 4 Willingness to Pay for Security Measures in the Major Public Event 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).

4. Policy Impact

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. 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.

5. Conclusions

5.1 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 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.

5.2 Overall Conclusions

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.

Although the philosophical and moral aspects of the valuation of human life, privacy or civil liberties may be difficult to accept, the real uncertainty is in understanding and quantifying the expected security benefits of certain types of infrastructure. These benefits might be expressed in terms of lives saved or terrorist incidents prevented. Studies have quantified the overall loss of life and economic damage arising from terrorist incidents (Enders and

Sandler, 2006) but as of yet there is little or no actuarial data to link the measures to benefits.

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.

References

ARTICLE 29 WORKING PARTY OF THE EU DATA PROTECTION DIRECTIVE (2006) Opinion on processing of personal data by the society of Worldwide Interbank Financial Telecommunication (SWIFT) (WP128). Brussels, European Commission.

BALL, K., LYON, D., WOOD, D. M., NORRIS, C. & RAAB, C. (2006) A report on the Surveillance Society. London, Surveillance Studies Network.

BBC (2008) In Full Smith ID Card speech, 6th March London.

BBC NEWS (2005) Illegal immigrant figure revealed. London.

BBC NEWS (2007) MI5 watch 2000 terror suspects. London.

BBC NEWS (2008) Police Announce London 2012 Plans. London.

BEN-AKIVA, M. & LERMAN, S. R. (1985) *Discrete Choice Analysis: Theory and Application to Travel Demand,* Cambridge, MIT Press.

BISSELL, A. & FERGUSON, R. (1975) The Jack-knife: Toy, Tool or Two-Edged Weapon? *Statistician,* 24**,** 79-100

CENTRAL OFFICE OF INFORMATION RESEARCH UNIT (2008) Identity and Passport Service; National Identity Scheme Tracking Research Wave 3. London Home Office.

CIRILLO, C., DALY, A. & LINDVELD, K. (1998) Eliminating Bias due to the repeated measurements problem in SP Data. IN LABBE, M., LAPORTE, G., TANCZOS, K. & TOINT, P. (Eds.) *Operations Research and Decision Aid Methodologies in Traffic and Transportation Management.* Balatonfüred, Hungary, March 10-21, Springer.

DIRECTGOV (2009a) Table of Passport Fees, how to pay and refunds.

DIRECTGOV (2009b) Travel and transport - timetable for passport applications. London.

ENDERS, W. & SANDLER, T. (2006) Distribution of transnational terrorism among countries by income class and geography after 9/11. *International Studies Quarterly,* 50**,** 367-393.

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

GALLUP ORGANISATION - HUNGARY (2008) Data Protection in the European Union Citizens Perceptions: Analytical Report Flash Eurobarometer 225. The Gallup Organisation.

HALL, J. (2006) Question the head of the Identity and Passport Service. London.

HENSHER, D. A., ROSE, J. M. & GREENE, W. H. (2005) *Applied Choice Analysis - A Primer,* New York, Cambridge University Press.

HM GOVERNMENT (2006) Countering International Terrorism: The United Kingdom's Strategy. London.

ICO (2009) Information Commissioner Office Privacy Impact Assessment Handbook (v2). Wilmslow, Cheshire.

JOHNSON, M. & GEARTY, C. (2007) A Price worth paying? Changing public attitudes to civil liberties under the threat of terrorism. *British Social Attitudes: the 23rd Report - Perspectives on a changing society.* London, Sage Publications for NatCen.

KUMARAGURU, P. & CRANOR, L. F. (2005) Privacy indexes: A survey of Westin's studies. *Institute for Software Research International, Carnegie Mellon University.* Pittsburgh.

LOUIS HARRIS, & ASSOCIATES & WESTIN, A. F. (1994) Equifax-Harris Consumer Privacy Survey. *Technical Report Conducted for Equifax Inc. 1,005 adults of the U.S. public.* New York, Louis Harris & Associates.

LOUVIERE, J. (1992) Experimental choice analysis: introduction and overview. *Journal of Business Research,* 24**,** 89-96.

LOUVIERE, J. & WOODWORTH, G. (1983) Design and analysis of simulated consumer choice or allocation experiments: an approach based on aggregated data. *Journal of Marketing Research,* 20**,** 350-367.

LOUVIERE, J. J., HENSHER, D. A. & SWAIT, J. D. (2000) *Stated Choice Methods: Analysis and Application,* Cambridge, Cambridge Press.

MERRICK, J. (2008) Security bill for London's 2012 Olympics to hit £1.5bn - triple the original estimate. *The Independent.* London.

MILLER, R. (1974) The Jack-knife: A Review. *Biometrica,* 61**,** 1-14.

NETC@RDS PROJECT (2009) A step towards the electronic European Health Insurance Card.

OMAND, D. (2009) The National Security Strategy: Implications for the UK intelligence community. *Commission on National Security for the 21st Century.* London, Institute of Public Policy Research, Discussion Paper.

ORTUZAR, J. D. & WILLUMSEN, L. G. (2001) *Modelling Transport,* Chichester, John Wiley & Sons, Ltd.

RESEARCH NOW (2007) About Us - The International online Fieldwork and Panel Specialists.

RYAN, M., BATE, A., EASTMOND, C. J. & LUDBROOK, A. (2001) Use of discrete choice experiment to elicit preferences. *Quality in Health Care,* 10**,** i55-i60.

STORK PROJECT (2009) Secure Identity Across Borders Linked (STORK) Project.

THE DAILY TELEGRAPH (2006) Yard is watching thousands of terror suspects. London.

THE GUARDIAN (2006) MI5: 30 terror plots being planned in the UK, November 10th London.

THE JOB (2008) Ready for an Olympic Task. London Metropolitan Police.

THE TIMES (2003) Heathrow Show of Force after terror alert, Feb 12th. London.

THE TIMES (2009) Biometrics Screening for Olympic Workers, 5th March. London.

TRAIN, K. (2003) *Discrete Choice with Simulations,* Cambridge, Cambridge University Press.

UK DEPT. FOR TRANSPORT (2006) Responsibilities of Transport Security's Land Transport Division. London.

UK DEPT. FOR TRANSPORT (2008) Summary report of the 'LUNR' passenger screening trials. London.

ZDNET (2009) Security management toolkit: Government U-turns on passport pledge. London.

Appendices

Appendix 1: Attributes, levels and model estimation tables

Table 2 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

Table 3 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[6]	
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)

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

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)
Number of terrorists that may be identified[7]	
x (1)	0.00039 (17.7)
x (1, if number of terrorists that may be identified > 2,400; 0 otherwise)	-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 (3.0)
Constant, Option 2	1.050 (3.3)
Constant, Option 3	0.806 (2.5)
No. of observations (1,940 x 8)	15,520
Log-likelihood function, L(β) (*d.f.)*	-18,369.5 (26)
$\rho^2(C)=1-[L(\beta)/L(C)]$	0.146
$\rho^2(0)=1-[L(\beta)/L(0)]$	0.114

[7] The following two terms are additive.

Table 4 Attributes and levels in the rail travel 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

Table 5 Estimation results in the rail travel 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

Table 6 Attributes and levels in the major 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

Table 7 Estimation results in the major event scenario

Variable	**Coefficient (t-ratio)**
Delay to pass through security checks[8]	
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	0.557 (12.2)
the stadium	0.314 (5.3)
x (1, if female; 0 otherwise)	0.431 (13.3)
x (1, if male non-conservative; 0 otherwise)	
x (1, if male conservative; 0 otherwise)	
On the way to the stadium, at the turnstiles, in the control room, inside the	0.557 (12.2)
stadium and throughout the crowd	0.314 (5.3)
x (1, if female; 0 otherwise)	0.431 (13.3)
x (1, if male non-conservative; 0 otherwise)	
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)
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	

[8] The following terms are additive.

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

Appendix 2: Stated Preference Discrete Choice Models

Discrete choice modelling provides an evidence based quantitative framework that enables researchers and policy makers to understand how individuals make choices when faced with different policy options or, in general, a number of alternative situations. In particular, discrete choice modelling helps to (Ortuzar and Willumsen, 2001):

- Identify what is the relative importance of factors (attributes) that drive individual choice,
- Construct alternative scenarios and predict public acceptance of policy interventions or proposed service improvements, demand and market shares of products over the whole population.

In an ideal case, we would develop discrete choice models using information on choices made in a real situation. From these data, we can quantify the influence of particular attributes or individual characteristics in real choice contexts (i.e., revealed preferences). There are, however, potentially a number of problems with such data (Hensher et al., 2005, Louviere et al., 2000):

- What we think people are considering, and what they are actually considering may be different,
- The alternatives individuals consider may ambiguous,
- The range and variation of the product or service attributes may be limited,
- The attributes may be highly correlated (e.g. quality and price), and
- The attributes may include measurement errors.

Moreover, there might be cases where direct observation is not be possible, because some alternatives or certain characteristics of them do not exist yet (e.g. new technologies, new policy interventions, new environmental protection plans, etc). These problems could be overcome if we could undertake real-life controlled experiments. The stated preference discrete choice experiments provide an approximation to this, a sort of quasi-experiment undertaken in a survey environment based on hypothetical (though realistic) situations set up by the researcher (Ortuzar and Willumsen, 2001). The main features of the SP discrete choice experiments can be summarised into the following (Ortuzar and Willumsen, 2001):

- Respondents evaluate *hypothetical* alternative options and choose one of the alternatives within a choice set. The choice decision is dependent upon the levels offered and individuals' own preferences,
- Each alternative is described as a composite *package* of different attributes,
- The combination of attribute levels used to describe each alternative are defined using *experimental design* techniques that ensure the variation in the attributes in each *package* allows estimation of the influence of the different attributes on the choices made,
- The alternatives offered to respondents in the experiment should be understandable, appear plausible and realistic.

Discrete choice models are then used to gain insight into what drives the decisions that individuals make when faced with these 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). These model coefficients 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.

Appendix 3: Willingness-to-Pay

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). For example, 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:

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

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:

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

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:

$$WTP_{wa} = \sum_{i} \left(\delta_i * WTP_i \right) \quad [3]$$

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.

Appendix 4: 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:

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

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.