Chapter 1

SECURITY AT WHAT COST?

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

Abstract In the presently heightened security environment in the United Kingdom there are a number of examples of policy that must strike a delicate balance between strengthening security and endangering civil liberties and personal privacy. The introduction of national identity cards and biometric passports, expansion of the National DNA Database and interdepartmental sharing of personal information raise a number of privacy issues. Human rights may also be suspended by the exercise of stop-and-search powers by the police or the detention of suspects prior to trial. However, much of the current debate concerning civil liberties and security is adversarial, and little robust research data informs arguments on both sides. This paper outlines the results of a study that attempts to objectively understand the real privacy, liberty and security trade-offs made by individuals, so that policymakers can be better informed about the preferences of individuals with regard to these important issues.

Keywords: Security measures, stated preferences, trade-offs

1. Introduction

The entities responsible for protecting critical infrastructures such as transportation networks and physical assets often have to make difficult decisions in the face of considerable uncertainty regarding the imposition of security measures to mitigate the risks due to a particular threat. Where individuals are involved in critical infrastructures – as users or consumers of a service or product that the specific sector provides – their civil liberties or privacy may be affected. Contemporary examples of security measures that affect privacy or civil liberties include: (i) new forms of body scanning technologies; (ii) closed-circuit television (CCTV); (iii) fingerprint identification, facial recognition and other biometric identification systems; and (iv) the sharing, mining and use of personal information by government agencies.

Most 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. These approaches have limitations because they only permit absolute (Yes/No) responses to questions, and are generally not conducive to instances in which individuals are faced with a series of realistic choices that may have different effects on their privacy, liberty or security. Recent examples include the Westin-Harris privacy surveys [17], a Gallup Flash Eurobarometer survey conducted for the European Commission [31], a British Social Attitudes Survey [15], and tracking research conducted for the Home Office's National Identity Scheme [5]. These approaches suffer from three main limitations: (i) they are generally one-dimensional, unrealistic, and ask abstract, one-off questions that lead to polarized preferences towards absolutes instead of grading choices involving privacy, liberty and security trade-offs; (ii) they do not quantify the extent to which people may be prepared to give up civil liberties or privacy; and (iii) they cannot be integrated easily into an economic appraisal toolkit.

This paper reports on the application of stated preference discrete choice experiments (SPDCEs) for understanding, quantifying and, in some cases, monetizing the privacy, liberty and security trade-offs made by individuals. In particular, the research questions addressed are:

- Given that national security is a non-market public good, does the use of stated preference techniques have merit for gathering data on the willingness of individuals to make trade-offs?
- 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 monetize the impacts of these security measures on liberty and privacy?

2. Research Methodology

Our study used SPDCEs to investigate the importance of specific drivers for the choices made by individuals (see, e.g., [11]). These techniques have been used extensively in marketing, healthcare, environmental and transportation economics [18–20, 29]. In combination with discrete choice analysis, SPDCEs offer the potential to provide empirical evidence for making informed decisions, for example, regarding the importance that individuals attach to advanced CCTV cameras supported by real-time, face recognition technology. As national security and privacy may be considered to be examples of non-market public goods (like healthcare and the environment), there is some validity to the application of these techniques in the domain of interest. Furthermore, the use of a methodology that permits the identification of real choices and the trade-offs that individuals are prepared to make contrasts well with the "top-down" risk-based approach in use by government, which matches vulnerabilities and threats against resource investments (see, e.g., [13]). Finally, the methodology

may assist cost-benefit decision-making processes dealing with the economic evaluation of security measures, since it can determine the threshold at which individuals are prepared to tolerate privacy and civil liberty intrusions in the name of security.

2.1 Case Studies

Based on a review of the literature and semi-structured interviews with representatives from both sides of the national security versus civil liberties debate, we identified three contexts for applying the experimental methodology: (i) applying for a passport, where individuals provide personal information; (ii) traveling on the national rail network, where individuals may be under the surveillance of CCTV networks; and (iii) attending a major public event, where individuals may be subject to identification processes and interact with various security officials.

Attributes describing each case study and their values were derived from information available in the public domain such as estimates of the numbers of terrorist suspects [16], ongoing conspiracies [22] and illegal immigrants [3]. Information about the processing time of passport applications and the personal data collected during the application process was obtained from [7, 32]. The design and specification of the case studies are described in more detail in [28].

2.2 Data Collection

The SPDCEs were conducted over the Internet between September 17 and 19, 2008. The survey was pre-tested and modified in accordance with post-survey cognitive questions by 260 individuals between June 27 and 29, 2008.

Invitations to participate in the survey were emailed to 15,214 individuals registered with Research Now [27], a market research company with the largest panel of Internet users in the United Kingdom. Individuals who did not meet the eligibility criteria (e.g., 18 years or older), provided incomplete information or belonged to sample quotas that were already filled were eliminated. A total of 2,058 participants were recruited.

Table 1 presents the descriptive statistics of the survey sample compared with those from the 2001 U.K. Census [24]. While the survey sample is not representative of the U.K. population, it covers an active segment of the population that matches the demographic profiles (i.e., age and gender) in the 2001 U.K. census.

2.3 Model Development

Following an initial discrete choice model that used only the attribute levels of the experiments, alternative specifications of the model that included socio-demographic characteristics of respondents and their attitudes were employed to test whether certain groups of respondents placed different valuations on any of the attributes. Possible differences were identified by examining cross tables

Table 1. Sample characteristics compared with the 2001 U.K. Census.

Variable	**Sample (%)**	**2001 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+	22	20
Education Level		
None	10	29.1
O Level/GCSE	32	59.6
A Level/CSE	26	8.3
Degree	32	19.8
Other		6.9
Occupational Status		
Fulltime	42	59.6
Parttime	16	
Student	4	7.2
Retired	28	13.4
Seeking Work	3	4.5
Other	7	15.3
Income		
Below £30,000	58	
£30,000 to £69,999	26	
£70,000 and Higher	2	
Not Reported	14	

that summarized the in-sample predictive ability of the model. This approach enabled us to address key differences in the choices made by individuals within the sample. The SPDCE method is consistent with utility maximization and demand theory [19, 26]. After the parameter estimates were obtained using the most appropriate model, a willingness-to-pay (WTP) measure for changes across different levels of attributes was computed using the equation [11]:

$$WTP = -\beta_{price}^{-1} \ln \frac{\sum_i \alpha_i e^{V_i^1}}{\sum_i \alpha_i e^{V_i^0}}$$

where β_{price} is the coefficient of the price increase on a ticket to cover security; V_i^0 is the utility of the base level (e.g., no CCTV) for a segment of the sample (e.g., males) with proportion α_i; and V_i^1 is the utility of the same segment

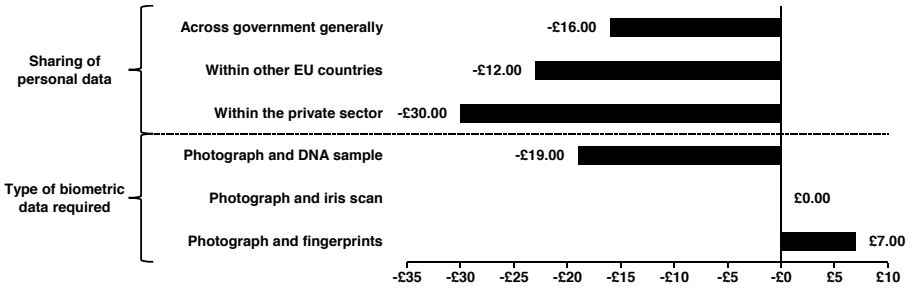

Figure 1. Willingness to pay for security (passport application).

for a security improvement (e.g., CCTV) compared to the base level. Complete details about the results of the model estimation and WTP estimates are provided in [28].

3. Results and Discussion

This section discusses the experimental results for the case studies involving passport applications, national rail travel and public event attendance.

3.1 Passport Applications

Due to heightened concerns about national security and identity theft, there is considerable debate and political pressure to implement ID cards, a National Identity Register (NIR) and biometric passports, all of which will have significant amounts of personal information. It is expected that this information will be shared among government organizations responsible for security, border management and immigration. The current U.K. passport application process is already raising concerns about privacy and civil liberties being relegated in favor of national security. Citizens are required to provide a significant quantity of personal information with their passport applications because the information can help fight against "social bads" such as illegal immigration and terrorism.

The security characteristics of biometric passports may affect privacy and liberty in several ways. For example, personal information collected for the purpose of law enforcement may be shared (mistakenly or deliberately) with other organizations not associated with achieving security objectives, possibly resulting in discrimination or disenfranchisement of individuals based on the identity information stored in their passports. As more organizations are permitted to use this personal information, the risk of abuse and mistakes increases.

Our experimental data indicated a universal degree of discomfort in the provision of advanced forms of biometric information (e.g., DNA) as part of the passport application process (Figure 1). Respondents were only willing to accept (i.e., they derived negative utility from) the collection of DNA and photograph data at the time of a passport application if there was a subsidy of

£19 in the cost of a passport. The respondents preferred to provide personal information in the form of a photograph or fingerprint, and they indicated a willingness to pay £7 for this privilege. This finding is relevant given recent policy statements that indicate that fingerprint biometrics will be collected as part of the passport application process [34]. Note that there is no requirement to submit further biometric information at this time because a facial biometric is compiled from the passport photograph [8].

More worrisome from a privacy perspective were the responses to the question of the sharing of personal information collected during the passport application process with other organizations in the public or private sectors. Indeed, this question provoked universal discomfort in the respondents. All else being equal, the respondents preferred to see their personal information kept within the Identity and Passport Service, and not shared with other government departments, other European nations or the private sector. This has a number of important policy implications – most notably, if the desire by the public sector to use the collected information to achieve efficiencies or help in the fight against organized crime, illegal immigration and terrorism matches the preferences of the general public [25]. Furthermore, there is the question of consent and choice and if this may ever be construed as meaningful given the extent of the demand for passports.

The survey also shows that large incentives (e.g., a discount on the passport fee of as much as £30) would be required to reach a threshold where the respondents would be comfortable sharing their personal information 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. A subsidy of £23 would have to be provided in order to share information with other European nations, and £16 to share information with other government departments.

Evidence from this case study appears to contradict current government policy, particularly regarding the sharing of NIR information (which may be collected as part of the passport application process) with the private sector or other government departments as part of the "identity assurance" policy agenda. 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 other credentials when applying for a bank account [4]. Finally, with regard to sharing information with other countries, the European Secure Identity Across Borders Linked (STORK) Project [30] is evaluating methods to do just this – sharing information between EU member states to deliver pan-European services such as the European electronic health insurance card [33]. The existence of such compelling evidence regarding the preferences of the survey participants suggests that policymakers ought to explore and consider the implications of collecting and sharing personal information, whether a subsidy is necessary, or whether to consider (at the very least) the unintended consequences of implementing policies that are contradictory to individual preferences.

Figure 2. Willingness to pay for security (rail travel).

3.2 National Rail Travel

The terrorist attacks on public transportation systems around the world have made safety and security a top priority in the policy agenda of many countries, particularly the United Kingdom. Security measures for air travel have historically received a great deal of attention, but authorities are now increasingly focusing on land-based mass transit systems. These systems have become targets for terrorist groups due to their vulnerability and ease of access arising from their intrinsically open nature.

In the United Kingdom, measures to address security threats include legislation and regulations as well as campaigns that raise public awareness of the risk of attacks. The Transport Security and Contingencies Team (TRANSEC) of the U.K. Department of Transport [6] plays an important role with regard to security arrangements for multi-modal transportation systems. Its task is complicated by the fact that many transportation systems are privately owned.

Several attributes compete with privacy and liberty in this case study: most notably, the presence of security personnel who may inadvertently detain individuals. The presence of CCTV cameras has an impact on privacy as do other types of security checks, which could be regarded as an invasion of personal space (e.g., security personnel going through bags and personal effects).

Security mechanisms that may affect personal privacy or civil liberties when traveling on the national rail network were viewed more favorably by the survey respondents (Figure 2). This may be due to familiarity: in contrast with sharing personal information 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 is seen in the preferences regarding X-ray machines or physical "pat downs" and bag searches; the latter being considered as more invasive, perhaps due to their physical intrusiveness. Despite this, the poten-

tial to exercise the right to privacy under this security measure may be less restricted than when personal information is collected when passing through an X-ray arch, where data may be recorded, shared with others and stored for a longer period of time with little, if any, self-determination by the individual.

Individuals were comfortable with more intrusive types of security cameras (e.g., face detection systems) as they seemed to outweigh concerns related to personal privacy and civil liberties. 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 [1].

However, there remains the question about the extent to which context plays a role. Many individuals have identified that being monitored by CCTV of any form in the environment of a railway station is an acceptable sacrifice to obtain the security benefits. Similarly, the evidence may illustrate confusion about the perception that CCTV is a tool for detecting low-level street crime such as burglary, mugging and anti-social behavior, rather than for dealing with more complex forms of criminal behavior or terrorism [10].

The findings regarding the degree of comfort attached to different types of security checks are counterintuitive. We anticipated that security checks with an obvious privacy implication would be less preferable than others with which individuals are more familiar. However, the evidence indicates that individuals are much more comfortable with passing through an X-ray arch or scanner than being subjected to a security pat down or bag search. Understandably, these are more privacy-invasive due to their personal and physical nature but, by comparison, the information recorded by a metal detector or X-ray scanner may adversely affect personal privacy in a broader manner as it may be recorded 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 indicates that alert, trained staff who can spot indicative behavior patterns can be a very effective security measure.

Finally, and somewhat unsurprisingly, there was a high degree of comfort expressed for more specialized security personnel, albeit up to a point. Despite the perception in the security community that the deployment of armed police or the military creates an atmosphere of fear, in all cases, the survey respondents were willing to pay for security personnel; in fact, no negative utility was identified. Regarding the visible presence of uniformed military personnel, as was seen, for example, at London's Heathrow Airport in 2003 [2], most survey respondents were willing to pay for these measures, but less so than other "low key" forms of security personnel. Also, the respondents felt that the effectiveness of uniformed military personnel was not correlated with an increasing level of sophistication.

3.3 Public Event Attendance

There is widespread concern regarding security at major sporting and entertainment events, particularly given the terrorist attacks at the 1972 Munich

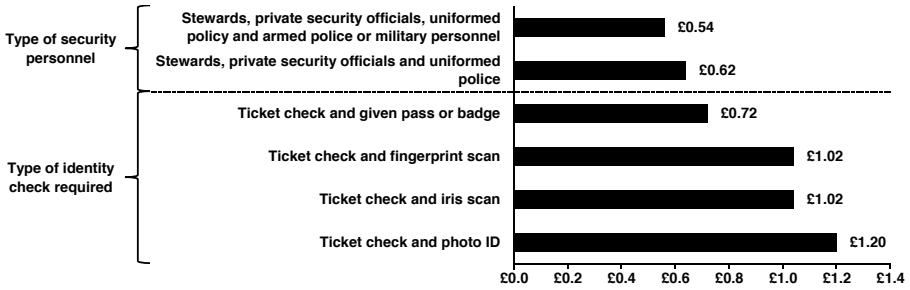

Figure 3. Willingness to pay for security (public event attendance).

Olympics and the 1984 Conservative Party Conference in Brighton. Such events are recognized as prime terrorist targets because they involve large concentrations of members of the general public [12]. This is on top of the challenge of maintaining security given the porous perimeters of most venues. In preparation for the 2012 London Olympics, a number of security measures are being considered, including monitoring, access control, overhead surveillance and CCTV systems [21].

The measures implemented at major public events to deal with security may affect liberty in a number of ways. These include the impact on privacy resulting from the collection of personal information upon entry to an event, various forms of personal information being used to verify the identity of an individual, and the possibility of detention by security authorities.

In the major public event case study, the survey respondents preferred to have some form of identity check. However, all else being equal, they were less likely to pay for checks that would require biometric identification (Figure 3). Based on an expected ticket price of £40 for attending the opening ceremonies of the 2012 Olympic Games, the respondents were willing to pay £1.20 for an identity check based on a picture ID and an examination of the ticket. Biometric checks such as fingerprint and iris scans were less preferable; individuals were prepared to pay £1.02 for these forms of identity checks. This could be explained by the acceptance that it would be necessary to check the identity of the individual presenting the ticket in order to ensure that he/she is a legitimate ticket holder.

The more interesting finding is that, despite media reports about concerns regarding the use of biometric technologies, individuals are willing to pay for the checks and accommodate civil liberty intrusions to achieve the security objectives. This is reinforced by the finding that survey respondents were willing to pay less (£0.72) for a simple ticket check that does not involve identity information than one involving some form of personal or biometric information. This evidence is relevant to the discussions regarding possible security technologies for administering entry to events at the 2012 London Olympics. As such, it is pertinent to note that the Olympic Delivery Authority is considering "facial and palm" biometric identification for workers at Olympic sites [23].

4. Conclusions

The views and preferences of citizens as users of security infrastructures can be quantified and, in some cases, monetized. This information can be used to support security investment decisions that balance the risk of an incident versus the costs and implications of implementing security infrastructures to mitigate the risk.

The methodology used is based on the expectation that individuals act rationally. For example, when presented with a set of alternatives, individuals tend to choose the option that best satisfies their needs. This notion is the cornerstone of neoclassical economics. The diagnostic and evaluative questions asked of the survey respondents facilitated the understanding, measurement and economical quantification of the relative degree of comfort or distaste for security measures. The results provide useful indicators of current concerns about how security measures may affect privacy and liberty.

The rational actor model employed in this work is the basis of many investment decisions in public policy. This study can shed light on where policy and preferences differ and, thus, assist policymakers in making informed, evidence-based decisions as to whether the cost of contravening or ignoring user preferences outweighs the benefits of implementing security measures. Similarly, it might be possible to identify where the measures could be adjusted to take better account of preferences without undermining security gains.

Although the philosophical and moral aspects of the valuation of human life, privacy and 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. Some studies [9] have quantified the overall loss of life and economic damage arising from terrorist incidents, but as of yet there is little or no actuarial data to link the measures to benefits.

This methodology can also support policymaking and security decisions regarding the data to use as input in risk assessments. The approach may have particular relevance in privacy impact assessments, a relatively new policy tool that considers the privacy perceptions of the "users" of policy initiatives when designing security measures [14]. Finally, the application of the methodology can bring a degree of objectivity to the highly charged debate on striking the right balance between civil liberties and security. Ultimately, this study shows that using the metaphor of "balance" is counterproductive without robust measurements of the weights of the factors that are balanced.

References

[1] K. Ball, D. Lyon, D. Wood, C. Norris and C. Raab, A Report on the Surveillance Society, The Surveillance Studies Network, London, United Kingdom, 2006.

[2] P. Barkham, Heathrow show of force after terror alert, *The Times*, February 12, 2003.

[3] BBC News, Illegal immigrant figure revealed, London, United Kingdom (news.bbc.co.uk/2/hi/uk_news/politics/4637273.stm), June 30, 2005.

[4] BBC News, In full: Smith ID card speech, London, United Kingdom (news.bbc.co.uk/2/hi/uk_news/politics/7281368.stm), March 6, 2008.

[5] Central Office of Information, Identity and Passport Service, National Identity Scheme Tracking Research Wave 3, Home Office, London, United Kingdom, 2008.

[6] Department for Transport, Responsibilities of Transport Security's Land Transport Division, London, United Kingdom (www.dft.gov.uk/pgr/security/land/responsibilitiesoftransports4898).

[7] Directgov, Timetable for passport applications, Her Majesty's Government, London, United Kingdom (www.direct.gov.uk/en/TravelAndTransport/Passports/howlongittakesandurgentappplications/DG_174148), 2008.

[8] Directgov, Table of passport fees, Her Majesty's Government, London, United Kingdom (www.direct.gov.uk/en/TravelAndTransport/Passports/howlongittakesandurgentappplications/DG_174 109), 2009.

[9] W. Enders and T. Sandler, Distribution of transnational terrorism among countries by income class and geography after 9/11, *International Studies Quarterly*, vol. 50(2), pp. 367–393, 2006.

[10] D. Farrington, M. Gill, S. Waples and J. Argomaniz, The effects of closed-circuit television on crime: Meta-analysis of an English national quasi-experimental multi-site evaluation, *Journal of Experimental Criminology*, vol. 3(1), pp. 21–28, 2007.

[11] D. Hensher, J. Rose and W. Greene, *Applied Choice Analysis: A Primer*, Cambridge University Press, Cambridge, United Kingdom, 2005.

[12] Her Majesty's Government, Countering International Terrorism: The United Kingdom's Strategy, London, United Kingdom (www.fco.gov.uk/resources/en/pdf/contest-report), 2006.

[13] Her Majesty's Treasury, The Green Book: Appraisal and Evaluation in Central Government, London, United Kingdom (www.hm-treasury.gov.uk/d/green_book_complete.pdf), 2003.

[14] Information Commissioner's Office, Privacy Impact Assessment Handbook (Version 2.0), Wilmslow, United Kingdom (www.ico.gov.uk/upload/documents/pia_handbook_html_v2/files/PIAhandbookV2.pdf), 2009.

[15] M. Johnson and C. Gearty, *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*, Sage Publications, London, United Kingdom, 2007.

[16] P. Johnston, Yard is watching thousands of terror suspects, *Daily Telegraph*, September 2, 2006.

[17] P. Kumaraguru and L. Cranor, Privacy Indexes: A Survey of Westin's Studies, Technical Report CMU-ISRI-5-138, Institute for Software Research International, Carnegie Mellon University, Pittsburgh, Pennsylvania, 2005.

[18] J. Louviere, Experimental choice analysis: Introduction and overview, *Journal of Business Research*, vol. 23(4), pp. 89–96, 1991.

[19] J. Louviere, D. Hensher and J. Swait, *Stated Choice Methods: Analysis and Applications*, Cambridge University Press, Cambridge, United Kingdom, 2000.

[20] J. Louviere 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(4), 350–367, 1983.

[21] J. Merrrick, Security bill for London's 2012 Olympics to hit £1.5bn – Triple the original estimate, *The Independent*, September 28, 2008.

[22] R. Norton-Taylor, MI5: 30 terror plots being planned in the UK, *The Guardian*, November 10, 2006.

[23] A. O'Connor and J. Sherman, Biometrics screening for Olympic workers, *The Times*, March 5, 2008.

[24] Office for National Statistics, Census 2001, London, United Kingdom (www.statistics.gov.uk/census2001/census2001.asp).

[25] D. Omand, The National Security Strategy: Implications for the UK Intelligence Community, Discussion Paper, Institute of Public Policy Research, London, United Kingdom, 2009.

[26] J. Ortuzar and L. Willumsen, *Modeling Transport*, John Wiley, Chichester, United Kingdom, 2001.

[27] Research Now, Welcome to Research Now, London, United Kingdom (www.researchnow.co.uk).

[28] N. Robinson, D. Potoglou, C. Kim, P. Burge and R. Warnes, Security at What Cost? Quantifying People's Trade-offs Across Liberty, Privacy and Security, Technical Report TR-664, RAND Europe, Cambridge, United Kingdom, 2010.

[29] M. Ryan, A. Bate, C. Eastmond and A. Ludbrook, Use of discrete choice experiments to elicit preferences, *Quality in Health Care*, vol. 10(1), pp. 55–60, 2001.

[30] STORK, The Secure Identity Across Borders Linked (STORK) Project, Madrid, Spain (www.eid-stork.eu).

[31] The Gallup Organization, Data Protection in the European Union – Citizens' Perceptions: Analytical Report, Flash Eurobarometer 225, Brussels, Belgium (ec.europa.eu/public_opinion/flash/fl_225_en.pdf), 2008.

[32] The National Archives, Question the head of the ID card scheme, London, United Kingdom (www.number10.gov.uk/Page10364), November 14, 2006.

[33] The NETC@RDS Project, NETC@RDS: A step towards the electronic European health insurance card, Luxembourg (netcards-project.com/web/frontpage).

[34] ZDNet UK, Government U-turns on passport pledge, London, United Kingdom, October 1, 2009.