



EUROPE

THE ARTS
CHILD POLICY
CIVIL JUSTICE
EDUCATION
ENERGY AND ENVIRONMENT
HEALTH AND HEALTH CARE
INTERNATIONAL AFFAIRS
NATIONAL SECURITY
POPULATION AND AGING
PUBLIC SAFETY
SCIENCE AND TECHNOLOGY
SUBSTANCE ABUSE
TERRORISM AND
HOMELAND SECURITY
TRANSPORTATION AND
INFRASTRUCTURE
WORKFORCE AND WORKPLACE

This PDF document was made available from www.rand.org as a public service of the RAND Corporation.

[Jump down to document](#) ▼

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world.

Support RAND

[Browse Books & Publications](#)

[Make a charitable contribution](#)

For More Information

Visit RAND at www.rand.org

Explore [RAND Europe](#)

View [document details](#)

Limited Electronic Distribution Rights

This document and trademark(s) contained herein are protected by law as indicated in a notice appearing later in this work. This electronic representation of RAND intellectual property is provided for non-commercial use only. Unauthorized posting of RAND PDFs to a non-RAND Web site is prohibited. RAND PDFs are protected under copyright law. Permission is required from RAND to reproduce, or reuse in another form, any of our research documents for commercial use. For information on reprint and linking permissions, please see [RAND Permissions](#).

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

TECHNICAL REPORT



Security, At What Cost?

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

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

Sponsored by the RAND Europe Board of Trustees

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

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark.

© Copyright 2010 RAND Corporation

Permission is given to duplicate this document for personal use only, as long as it is unaltered and complete. Copies may not be duplicated for commercial purposes. Unauthorized posting of RAND documents to a non-RAND Web site is prohibited. RAND documents are protected under copyright law. For information on reprint and linking permissions, please visit the RAND permissions page (<http://www.rand.org/publications/permissions.html>).

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

Summary

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

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

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

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

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

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

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

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

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

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

- Given that national security is a form of non-market public good, does the use of stated preference¹ techniques for gathering data on the trade-offs that people are willing to pay have merit?
- What drives choice when individuals decide to relinquish or surrender their liberty or privacy to obtain security benefits?

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

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

Methodology

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

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

Case studies

Applying for a passport

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

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

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

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

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

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

Travel on the UK national rail network

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

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

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

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

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

Attendance at a major public event

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

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

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

Conclusion

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

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

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

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

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