Literature Review of Approaches for Measuring Preferences with Respect to Privacy, Security and Surveillance
The Privacy & Security - Research Paper Series

Edited by Christian Fuchs, University of Westminster, Communication and Media Research Institute
ISSN 2279-7467

Research Paper Number 10
Date of Publication: August 22, 2014

Literature Review of Approaches for Measuring Preferences with Respect to Privacy, Security and Surveillance
Authors:
Dimitris Potoglou; Neil Robinson; Tess Hellgren; Svitlana Kobzar and Sunil Patil

This paper is an output of PACT's Work Package “WP 2 – Survey Design”

Acknowledgement: The research presented in this paper was conducted in the project “PACT – Public Perception of Security and Privacy: Assessing Knowledge, Collecting Evidence, Translating Research into Action”, funded by EU FP7 SECURITY, grant agreement no. 285635
Literature Review of Approaches for Measuring Preferences with Respect to Privacy, Security and Surveillance

Dimitris Potoglou; Neil Robinson; Tess Hellgren; Svitlana Kobzar and Patil, Sunil

Abstract: This paper aims to inform the identification and selection of relevant, robust and validated methods for measuring individuals’ preferences related to privacy and security. It reports on the results of a targeted search of peer reviewed and grey literature concerning measurement scales and valid attitudinal indicators relating to privacy, security and surveillance. This search was conducted in the context of Work Package 2 of the FP7 PACT project and was intended to inform the selection of appropriate methods in the subsequent fieldwork stage of Work Package 3 of PACT.

Keywords: Preferences; Econometrics; Measuring attitudes; Privacy; Security; Surveillance;

Short biography of the authors:

Dr. Dimitris Potoglou is an adjunct member of staff in RAND Europe’s Choice Modelling and Valuation group and lecturer in transport and applied choice analysis in the School of Planning and Geography, Cardiff University. Potoglou received his Ph.D. in urban transportation geography from McMaster University, Canada.

Neil Robinson is a Research Leader at the RAND Europe Brussels office and is the management lead for RAND Europe’s involvement in PACT. Robinson received his BA from King’s College London and an MSc in Information Systems from City University.

Tess Hellgren is an Associate Analyst with the Defence and Security programme at RAND Europe. Hellgren holds an M.Sc. in Migration Studies from the University of Oxford and a B.A. in social studies from Harvard University.

Dr. Svitlana Kobzar is a Policy Analyst at RAND Europe and an Assistant Professor at Vesalius College, Vrije Universiteit Brussel. Since 2011, Kobzar has served as the Research Fellow at the University of Cambridge. She has PhD in International Relations from the University of Cambridge.

Dr. Sunil Patil is an Analyst in the Cambridge office of RAND Europe. Patil is the scientific lead for RAND Europe’s contribution to PACT. Prior to joining RAND Europe, Patil worked as a research assistant with the Texas Transportation Institute while working toward his Ph.D. from Texas A&M University in the field of transportation economics.
1. Context

1.1. Security measures are often in tension with individual expectations of privacy and convenience

In the current security environment, there is increasing emphasis on the need for security in the face of new forms of threats such as terrorism, identify theft, and cybercrime. In the efforts to protect populations against these security threats, risk reduction strategies have the potential to encroach upon individuals’ privacy and convenience. This reality results in a tension between security measures and their impact on the rights and privileges of the citizens they aim to protect.

The potential conflict between security requirements and individual rights to privacy and convenience is inherent in the social contract between a state and its citizens. On one hand, citizens depend upon governments for the provision of their own and national security. In order to achieve this security, however, the government may employ methods of protection which infringe on individuals’ perceptions of their reasonable expectations to privacy and convenience. These methods may be direct and physical in nature, such as the imposition of mandatory checks of individuals and luggage at transport hubs. They may also be indirect; as security measures are enhanced by new technological capabilities, measures such as surveillance and personal data mining have the potential to become increasingly intrusive.

The question about the value that individuals place on privacy and security is at the heart of the privacy/security trade-off debate. However, the concepts of privacy, security and/or inconvenience are challenging to value in any quantifiable manner. Practically, it is difficult for policymakers to gather and accommodate individuals’ views regarding privacy and security into a comprehensive policy. At the same time, security is a public rather than a market-based good or service. While there have been studies that analyse the value of health or time, efforts to estimate the value of security or privacy remain challenging. Several approaches have attempted to address such questions as:

- What specific factors drive individuals’ valuation of security/privacy/inconvenience?
- What are the other contextual factors that may affect these valuations?

---

1 Crossman et al: “Overlooked; Surveillance and Personal Privacy In Modern Britain”; Liberty; London; 2007


1.2. The PACT project aims to measure individual preferences for security, privacy and surveillance

It is in the context of these research questions that the PACT project aims to introduce evidence on the security-privacy trade-offs that individuals are willing to make in real-life situations. Work Package 2 (WP2) of PACT develops an empirical data gathering instrument that attempts to measure individuals’ security and privacy preferences in an effective and reliable way. This instrument involves a combination of a standard survey questions and stated choice experiments. It also includes a set of attitudinal indicators or scales that are used to indirectly measure latent variables such as individuals’ privacy and security concern, risk aversion and trust. As the PACT project includes from the outset the notion of empirical data gathering using stated preference techniques, we highlight from the literature how methods to elicit preferences have been deployed in the domain of privacy, security and surveillance. We also report on attitudinal questions which respondents are asked to rate statements related to concern risk aversion and trust using a Likert scale both generally and in relation to specific contexts.

1.3. A survey of studies on measuring individuals’ preferences and attitudes on privacy and security

This literature review is a survey of existing research on validated attitudinal indicators, which may qualify for inclusion in the PACT questionnaire, which forms WP2 of the PACT project. Existing research on privacy and security includes legal literature, secondary analysis, theoretical works and increasingly experimental research. Among this evidence, this literature review aims to identify examples of studies, publications and journal articles which either develop and/or validate indicators or scales related to individuals' trust, privacy, concern, and risk aversion.

The objectives of the literature review are thus to:

- Map existing approaches for eliciting individuals’ preferences on privacy and security,
- Identify relevant attitudinal indicators (also known as scales) for measuring individuals’ attitudes towards privacy, concern, risk aversion and trust; which ideally have been validated in previous studies;
- To identify the most relevant, preferably validated, indicators for the choice contexts considered in the PACT project.\(^4\)

To address these objectives, we conducted keyword searches on the EBSCO Host and Google Scholar databases. Search terms included: "privacy concern", "privacy scales", "privacy attitudes", "security measures", "security concern scales", "surveillance atti-

tude", "trust" and "concern". Once relevant literature was identified, a snowballing technique was further used to establish other relevant materials through the list of references of the papers. Further methodological details regarding the literature search are included in Appendix A.

The selection of studies reviewed in this paper is guided by the specific privacy, security and surveillance dimensions of the three choice contexts of PACT, namely:

1. Travelling on metro (surveillance of urban mass transport)
2. Choice of Internet Service Provider (surveillance of Internet usage)
3. Electronic health record storage device / system (surveillance and monitoring of healthcare records)

Based on our search, we identified studies that use various techniques to capture respondent preferences towards security and privacy and attitudes towards security and privacy, trust of government, trust of businesses, fundamental rights, societal and human security, and data protection. In addition to mapping a number of preference elicitation methods and identifying attitudinal scales, these sources also offer some general conclusions on privacy-security preferences that are useful to inform the PACT project.

2. A variety of research techniques have been deployed to measure individuals’ privacy and security preferences

The literature we reviewed revealed a number of promising research techniques which presented different strengths and weaknesses in understanding privacy-security attitudes. The assumption from the outset was that PACT would adopt stated preference techniques but it was judged to be worthwhile to review where alternative approaches had been used to measure privacy, security and surveillance preferences to compare with the benefits of the stated preference discrete choice technique.

2.1. Preferences regarding privacy, security and surveillance have been measured through four main empirical research techniques

Our literature review suggests that opinion polls are a widely used approach for eliciting individuals’ preferences for security and privacy. Overall, opinion polls that we consider sufficiently robust are those that utilise market research standards using telephone polling of representative samples and had a plus/minus margin of error of between 1 and 3% and involve more than 1,000 participants (see, Robinson et al., 2010). For instance, Cornig (2008) provides a particularly useful descriptive meta-analysis of opinion polls, which incorporates a robust understanding of privacy-security trade-offs across time.

A number of studies also rely on observational methods which can indicate preferences. Such studies occur in close proximity to real-life situations in which people
have expressed their preferences through directly observable behaviour. Thorton and Goldstien (2006) and Wolsley (2010) report on observational analysis of attitudes to different types of passenger transport security measures. In addition, revealed preference-based methods can analyse actual (ex-post) behaviour and “utilise complementary and substitutive relationships between public and various market goods to infer the value attributed to public goods from transactions in private goods” (Frey et al, 2004). However, we found no use of revealed preference based methods in the domain of privacy, security and surveillance.

**Stated preference-based methods**, by comparison to revealed preference-based methods, rely on collecting individuals’ stated preferences for hypothetical scenarios. These methods encompass both (a) contingent valuation methods, where respondents are asked to report directly their willingness to pay for a public good, or are asked questions about whether they would agree to pay a given price for a public good, and (b) discrete choice experiments, where respondents choose between hypothetical alternatives, and if the choice alternatives contain cost/price information this information can be to elicit willingness to pay. To produce reliable conclusions, studies based on discrete choice experiments need to consider carefully the hypothetical scenarios through which individuals reflect upon their choices. For example, the scenarios need to be described neutrally and made as accessible as possible to the layman. This is particularly challenging in the domain of privacy, security and surveillance because the issues can be highly nuanced and abstract Acquisti and Grossklags (2004). Grossklags and Acquisti (2007) and Robinson & Potoglou et al. (2010) present experimental examples of stated preference-based approaches for valuing trade-offs in respect of privacy, inconvenience, trust and public discomfort (Grossklags and Acquisti, 2007; Robinson & Potoglou et al., 2010).

Another approach used to measure individuals’ valuation of public goods such as security is the life satisfaction method (Frey et al., 2004). This correlates the degree of public ‘goods’ (e.g. clean air, health, security) or ‘bads’ (e.g. crime, terrorist incidents or lack of security) with individuals’ subjectively reported wellbeing to directly evaluate such ‘goods’ and ‘bads’ in terms of life satisfaction. This approach is regarded as less cognitively demanding than stated preference-based approaches which, in the domain of privacy and security, ask respondents to weigh benefits and risks (Frey et al., 2004).

As noted earlier, from the outset, the PACT project adopts stated preference discrete choice experiments to measure individuals’ preferences for privacy and security.

---

5 For example, see: Accent & RAND Europe (2010) Review of Stated Preference and Willingness to Pay Methods, April 2010 available at:  
However, from this summary, it is instructive to explore the strengths and weaknesses of the different possible approaches, summarised in Table 1 below.

<table>
<thead>
<tr>
<th>Method</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opinion Poll</td>
<td>Easy to deploy; Very accessible to the layman</td>
<td>People can rank everything similarly, i.e. highly; Difficult to establish policy-relevant measurement (e.g. WTP)</td>
</tr>
<tr>
<td>Observational studies and Revealed Preference (RP)</td>
<td>Allows collection of rich evidence from directly observed or practiced behaviour</td>
<td>Complex and costly to implement Hard to find real-life situations where people make trade-offs; Unsuitable for completely new alternatives, which do not already exist in some form</td>
</tr>
<tr>
<td>Stated Preference (SP)</td>
<td>In choice experiments, people are asked to make trade-offs, and this information provides indirect evidence on attribute values; Can be used to examine new alternatives</td>
<td>Hypothetical; Can appear arbitrary</td>
</tr>
<tr>
<td>Life Satisfaction</td>
<td>Accessible to the layman Evaluation of life as a whole, not current feelings</td>
<td>Can be abstract and too subjective</td>
</tr>
</tbody>
</table>

**Table 1**: Summary of advantages and disadvantages of different methods used to elicit individuals preferences with regard to privacy, security and surveillance

### 2.2. Different types of indicators and scales have been developed to measure security and privacy attitudes

Alongside the use of different research methods to measure and model preferences, our literature review identified a range of indicators and scales used to measure security-privacy concerns or behavioural preferences, more generally. Some studies use
a Likert scale to measure the strength of respondents’ attitudes (Burgoon et al., 1989). Others develop and robustly validate composite indices as a result of a set of Likert-scale questions for measuring attitudes. The most prominent example is the Westin’s “privacy index” which was developed through a series of surveys between 1978 and 2004 (Kumaraguru and Cranor, 2005). Indices have similarly been developed for the concept of ‘trust’ and even looking at specific cases such as trust of e-commerce or trust of government regulators, etc (Chellappa and Sin, 2005; Walls et al., 2004). Additional studies use new or existing personality scales to measure behavioural proclivity towards risk or impulsivity (Whiteside and Lynam, 2001; Borjesson et al., 2001).

A summary of some sources using attitudinal indicators and scales can be found in Appendix B. These articles were identified by the study team as relevant examples general privacy, trust and security concern scales as well as others being relevant to the choice contexts of PACT. Appendix C summarises questions which were eventually used to directly inform the design of the PACT survey questionnaire.

To construct indices for attitudes toward security, privacy, surveillance and other individual attitudes (e.g. trust and risk-taking behaviour) we selected a number of the indicators as a starting point.

Concerning the Internet scenario, we found and subsequently included three sets of relevant scales. We firstly used Jensen et al. (2005), who compared self-reported and observed privacy practices of Internet users. Secondly, we adapted measures introduced by Dinev and Hart (2006) in regard to understanding privacy calculus models used by consumers. Finally, we adapted questions from Buchanan (2007) who reported on the development of measures on online privacy concern and protection in the context of Internet use.

Regarding the healthcare scenario, we adopted two sets of scales to measure attitudes to health privacy concerns. The scales from research by Angst and Agarwal (2009) refer to regarding adoption of electronic health records in the presence of privacy concerns. The second set of scales is adopted from a study by Hwang et al (2012) and cover privacy concerns regarding exchange of Electronic Medical Records.

It is worth noting that the literature does not explicitly identify any validated attitudinal indicators relevant to the travel choice context. Those discovered are either purely focused on safety or cover road travel, but not public transport. Therefore, we construct questions following the structure of those identified for the Internet and healthcare domains.
To derive overall measure of privacy and trust, we included questions from the Westin-Harris index which helped us to establish an adapted ‘concern’ and ‘distrust’ index (Kumaraguru and Cranor, 2005). The Westin-Harris questions were particularly useful due to their general nature and validity demonstrated over a series of longitudinal studies. Since the 1970s, Westin has conducted various privacy related surveys across the United States using the same questions. Westin’s surveys measure attitudes about privacy concerns and trust and provide evidence on how these attributes and concerns have changed over time (Kumaraguru and Cranor, 2005).

Finally, the Domain Specific Risk Attitude Scale presented in Weber et al (2002) was seen as useful due to the broad range of questions and their accessibility for the layman. We included questions from this scale in order to derive a general measure of respondents’ attitudes toward risk.

As far as possible the questions and their scales were kept similar to the original attitudinal indicators. In many cases, however, we had to slightly alter or paraphrase the statements in order to make them suitable for the survey and choice contexts; for example we aimed to introduce statements that were less technical (following feedback from the cognitive interviews), to accommodate differences when the reviewed studies were conducted outside Europe, and to clarify potentially abstract terms in the original statements.

2.3. Across all research techniques, persistent challenges arise in attempts to measure security and privacy preferences

Across the research techniques surveyed, we identified a number of challenges for eliciting individuals’ privacy and security preferences. In opinion surveys, the use of binary or one dimensional "yes/no" questions can lead to individuals’ answers being unrealistically polarised, rather than reflecting the complex nature of views which may include a wider spectrum of choices involving privacy and security trade-offs. Even in studies that use more rigorous techniques and phrase questions so as to avoid binary bias, it remains fairly challenging to quantify individuals’ views. As it is difficult to enumerate the extent to which people may be willing to give up privacy in return for greater security or vice-versa, much of the existing research is unable to be integrated into cost-benefit assessments since it does not provide usable economic data.

Regardless of the research method employed, the context of the study also plays a crucial role in affecting findings on individuals’ preferences for greater security and/or privacy. For example, individuals’ preferences for security, privacy and/or inconvenience may be inextricably linked to the timing of a data collection exercise, such as its proximity to a key event like the attacks of September 11th 2001 (Lewis, 2005). Following the 9/11 attacks, it was reported that individuals were increasingly
willing to sacrifice some of their privacy for greater national security (Sanquist, 2008; Finkelstein, 2009). As time has passed, this attitude changed (Corning, 2008).

3. The literature reviewed reveals a number of useful findings for measuring security-privacy attitudes

Our literature review reveals some key findings that help to inform the design of the PACT EU27-wide survey instrument.

3.1. Findings from the literature highlight the importance of individual perceptions of the perceived costs and benefits of security-privacy trade-offs

The provision of information on benefits and costs is highlighted as an important factor that shapes public views (Acquisti and Grossklags, 2004; Sanquist, 2008; Finkelstein, 2009). Similarly, perceptions around the effectiveness of and trust in government (Westin, 2005) in addressing the threat to perceptions on how government programmes may be intruding upon privacy are also identified as important (Identity & Passport Service, 2009). Finally, general forms of convenience; for example becoming aware of a product or service that is in demand in the context of e-commerce are also noted in the literature covering online privacy trade-offs (LaRose, 2006).

As shown in Figure 1, the reviewed literature identifies three ways upon which individuals’ perceived costs and benefits as applied to security and privacy may be classified:

- Direct benefits or costs; reflecting reduced or increased fee burden (Finkelstein, 2009) or taxes (Finkelstein, 2009; Ludwig, 2001);
- Indirect benefits or costs; reflecting some type of monetary compensation or reward or monetary charges;
- Other forms of non-monetary personal benefits or costs including time; for example, time spent waiting (Finkelstein, 2009) or additional travel time (Liu, 2006), safety (Liu, 2006; Moore, 2006) and reliability of service.

![Figure 1. Types of benefits and costs related to security and privacy](image-url)
Evidence from the use of economic valuation approaches to crime control problems also highlight reduction in various types of crime (e.g. gun crime or drug use) as an important benefit (Ludwig J. & Cook P.J., 2001). Other benefits have been expressed in terms of Quality Adjusted Life Years (QALYs – Dolan et al., 2005). A body of literature also describes reduced civil liberties and further infringements on personal freedom as potential costs (Identity & Passport Service, 2009). More general forms of convenience (for example, becoming aware of a product or service that was in demand in the context of e-commerce – Larose, 2006) are also noted in the literature covering online privacy trade-offs.

3.2. Existing research suggests the presence of a ‘privacy valuation paradox’

Another important conclusion reached by several studies is the concept of ‘the privacy valuation paradox’. This notion implies that even though at a general level individuals report that they highly value their privacy – something which is repeatedly noted in the opinion polls (Gallup, 2008) – in practice, individuals’ behaviour seems to contradict their views. This is demonstrated in more complex experimental research studies that point to the paradox that ‘while individuals profess to value privacy in the abstract very highly or above other factors, they appear to express differing preferences in the immediate practical sense when it concerns priorities that they deem important in the immediate context, usually money or time’ (Robinson at al., 2010: 20; see Finkelstein, 2009, Liu, 2006). Overall, studies that employed revealed or stated preference methods have been able to demonstrate this paradox particularly well.

The existence of a ‘privacy paradox’ is illustrated by the findings of Beresford et al. (2011). This study was able to create an experiment where participants were given a choice to purchase DVDs from one of two online stores. One store required customers to provide more sensitive personal information, including their income, while offering a 1 Euro discount. The other store had more privacy friendly policy but did not offer any discount to its customers. Participants were also asked about their views on privacy. Overall, there were 225 participants in the study. Results of this study revealed that ‘the more privacy friendly firm failed to attract more customers’ (Beresford, Kubler, Preibush, 2011: 5). The conclusion was that ‘most of the participants of the study were unwilling to pay for greater privacy and chose the discounted product’ (Beresford, Kubler, Preibush, 2011: 2). Moreover, the post-experimental questionnaire revealed that 75% of the participants stated that they greatly value data protection, with 95% indicating that ‘they are interested in the protection of their personal information’, thus illustrating the notion of ‘privacy paradox’ (ibid.).
4. Conclusion

Existing research on security-privacy trade-offs provided valuable evidence for the design of the empirical instrument in WP2 of the PACT study. Our review highlighted four research techniques which have been used to elicit preferences relating to the topics of interest to PACT, as well as a range of different indicator scales (further detailed in Appendices B and C). Subsequent to this, a small number were adapted and included in the finalised survey design. The reviewed research also introduces some useful findings for the ongoing work on security-privacy trade-offs in PACT, namely the perceived benefits and disadvantages of cost-benefit analyses and the potential ‘privacy valuation paradox’.
References


Hsin-Ginn Hwang, Hwai-En Han, Kuang-Ming Kuo, Chung-Feng Liu. 2012. “The Differing Privacy Concerns Regarding Exchanging Electronic Medical Records of Internet
Users in Taiwan”, Journal of Medical Systems, December 2012, Volume 36, Issue 6, pp 3783-3793


University of Huddersfield. 2012 “Evaluating measures to improve personal security and the value of their benefits”, Rail Safety and Standards Board


Appendix A: Methodology

This was composed of a two stage process: a systematic search of the literature and a qualitative summary assessment.

Databases of abstracts were searched using the following strategy. Substantive keywords relevant to PACT (“Privacy”; “Security”; “Surveillance”; “Trust” Risk”; “Travel”; “Internet”; ) were combined with qualifiers of: “Attitude”; “Scales”; “Concern”).

In conducting this exercise, we searched both academic and ‘grey’ literature. In order to identify the former we are able to use the extensive resources of the RAND library - and electronic resource which provides RAND staff access to 1,000 individual academic, peer-review journals and subscription data bases.

The following databases were searched:

- Cambridge Scientific Abstracts
- Homeland Security Digital Library
- Ingenta Connect
- ISI web of knowledge/ web of science
- JSTOR
- National Criminal Justice Reference Service
- PsycInfo
- Social Science Abstracts
- Policy Hub
- Open Sigle
- Google Scholar
Appendix B: Summary of relevant articles with indicators concerning attitudes and preferences regarding privacy and security

Privacy/Security Concerns

Westin/Kumaraguru and Cranor 2005 - Privacy indexes: A survey of Westin’s Studies

One of the most widely cited studies on privacy concern has been the Westin-Harris series of privacy surveys. Since the 1970s, Westin has conducted various privacy related surveys across the United States. Westin’s surveys measure attitudes and concerns about privacy and provide data on how these attributes and concerns have changed over time (Kumaraguru and Cranor, 2005). Through conducting over 30 surveys and opinion polls between 1978 and 2004, Westin developed a “privacy index” which was used to explain the differences in individuals’ privacy concerns. The privacy index identified the following three classifications, which categorised participants:

- Privacy fundamentalists
- Privacy pragmatists
- Privacy unconcerned

This segmentation has been widely adopted by other researchers seeking to understand privacy concerns and values.

Smith et al 1996 - Information Privacy: Measuring Individuals’ Concerns about Organizational Practices

This study measured individuals’ concerns about organisational privacy policies through the development of an original instrument with 15 variables and four subscales. The instrument went through a series of reliability tests and was tested across several sample populations.

Buchanan et al 2007 - Development of measures of online privacy concern & protection for use on the Internet

This study developed and validated three scales measuring attitudes towards privacy and behaviours through an internet-administered 82 question survey. The 515 person sample was run against validation tests, and correlations between the three scored scales and measures of privacy concern were examined. The study concluded that the scales developed were reliable and valuable for future applications in privacy-related research.

Burgoon et al 1989 - Maintaining and Restoring Privacy through Communication in different types of relationships

This study uses a self-reported survey and pilot study with open-ended interviews to develop a questionnaire. The questionnaire is answered by 444 respondents who rate
39 different tactics to restore privacy. The focus is on six different relationships e.g. spouses and doctor-patient relationships. The authors use a five point Likert scale to say how strongly the respondents agreed that an action constitutes a privacy invasion.

**Chellappa and Sin 2005 - Personalization versus Privacy An Empirical examination of the online consumer's dilemma**

The paper aims to develop a parsimonious model of consumers’ personalization to privacy tradeoff. This study built upon existing instruments designed to measure consumer privacy preferences online. Consumer privacy attitudes were disaggregated to encompass concerns about information that was anonymous to personally identifiable.

**Hui et al 2007 - The Value of Privacy Assurance - An exploratory field experiment in Singapore that assessed the values of two types of privacy assurance: privacy statements and privacy seals**

This study evaluated the value that was placed on privacy statements and privacy seals through a field observation of a Singaporean sample of subjects’ behavioural responses towards the two types of privacy assurances. The implications of the study were that privacy statements provided a stronger inducement for subjects to disclose their personal information than a privacy seal. Additionally, financial incentives incentivized users to disclose information, while ‘information request[s]’ disincentivized disclosure. These results passed replicability tests, and had implications for broader privacy issues.

**Trust concerns**

**Mcknight et al 2002 - Developing and Validating Trust Measures for e-commerce**

This research paper proposed a multifaceted, four levelled model of trust in e-commerce. This model measured dispositions to disposition to trust, institution-based trust, and trusting beliefs and intentions. The study was designed around a hypothetical legal advice website which explored the psychometric properties of the various forms of ‘trust’ in the paper and their relationship to each other and other e-commerce constructs, such as experience on the internet and the quality of the website. The study concluded with some implications for future research and practice.

**National Research Council (2008) - Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment – Annex M**

This annex examines the relevant research surveys of major organizations following the 11 September 2001 terrorist attacks in Washington D.C. and New York City, examining convergences with earlier, similar data. This review attempts to analyze the
results from similar questions asked over time when possible, occasionally interpreting single-point results when they were relevant.

**Walls et al 2004 – Critical trust: understanding lay perceptions of health and safety risk regulation**

This paper explores public perceptions of trust in governmental health and safety regulatory agencies, using both qualitative and quantitative data from 30 focus groups conducted across Great Britain. The study considers individual responses to two government agencies, the Health and Safety Executive and the Railway Inspectorate. Expressions of trust depended on a variety of influences such as relevant evidence, past experience, and inferred perceptions based on general impressions of government’s success as a risk regulator. Conclusions demonstrated a wide range of public trust levels in relation to different government bodies, suggesting the presence of ‘critical trust’ that lies on the spectrum between complete scepticism/rejection and uncritical emotional acceptance.

**Poortinga and Pidgeon 2003 – Exploring the Dimensionality of Trust in Risk Regulation**

This article investigates the various dimensions of trust in relation to governmental regulation in general. The study uses data from a major quantitative survey conducted in 2002 across Great Britain, in which respondents were asked to react to one of five policy scenarios to share their views on government policy, the ‘value similarity’ of government and personal opinions, and trust in governmental risk regulation. Results showed that public sentiments varied across the five thematic scenarios, with trends showing moderate levels of lack of endorsement for government, lack of perceived value similarity, and lack of trust in risk regulation. Additional analysis run on quantitative data led to the creation of a trust matrix with dimensions of ‘general trust’ and ‘scepticism’ to work towards a typology of public trust in government regulators.

**Measurement scales for individual behaviours**

**Whiteside and Lynam 2001 – The Five Factor Model and impulsivity: using a structural model of personality to understand impulsivity**

This article sought to develop a more comprehensive scale for determining the multiple aspects of impulsivity. The study combined several pre-existing personality scales, drawing particularly on the Five Factor Model of personality (McCrae and Costa 1990), to apply a composite scale of comparable Likert-type four-point measurements to over 400 university students. Based on their results, researchers derived a model of four main facets through which to measure impulsivity: urgency, (lack of) premeditation, (lack of) perseverance, and sensation seeking.
*Borjesson et al. 2011 – Risk and Safety Attitudes Among Conscripts During Compulsory Military Training*

This study considered how the organisational factors of leadership and group cohesion interact with individual predispositions to influence new military conscripts’ risk-taking behaviours. Researchers used an individual-level approach to examine the varying importance of leaders, group solidarity, and individual personality on the formation of safety and risk attitudes in conscripts within 12 Swedish military platoons. Risk and safety attitudes, individual proclivities to sensation seeking, and leadership behaviours were ranked on tri-partite scales, with group cohesion considered using the Group Environment Questionnaire (Carron et al. 1985). Results showed that both safety awareness and risk willingness are valued attitudes among conscripts, and both leadership and individual characteristics impact these attitudes. While group cohesion was not shown as a strong indicator of safety attitudes, task cohesion did impact likelihood of taking risks.


In this paper a psychometric scale is designed and tested that asks respondents to rate the likelihood they would engage in risk-taking activity in five domains: financial decisions; health and safety; recreational; ethical and societal decisions. The validity of the scale is assessed against a sample of American undergraduate students. Differences were discovered between men and women and the research showed how risk taking is highly context specific. The scale is separated into two parts Part I uses a Likert scale and Part II assesses respondent perceptions of the magnitude of risks and expected benefits.

*Indicators relating to PACT Scenario 1: Travelling on metro (surveillance of urban mass transport)*

*University of Huddersfield 2012 - Evaluating measures to improve personal security and the value of their benefits*

The purpose of this study was to evaluate two specific interventions designed to reduce personal security risk at railway stations and railway station car parks, namely the Secure Stations and Safer Parking schemes. Secure Stations is a scheme for rewarding station operators, through accreditation by the British Transport Police (BTP), for managing security and demonstrating to customers their desire to reduce crime.
This paper proposes that willingness-to-pay values of security on public railways should be set higher than willingness-to-pay values on the road. This premium is due to the subject’s feelings of control, voluntariness, and responsibility rather than the possibility of a catastrophic accident on a railway.

Cheng 2010 - Exploring passenger anxiety associated with train travel
This study offers a conceptual model of railway-passenger anxieties, based upon the passenger service chain, and measured via an existing psychometric model. The study relies upon a sample of 412 passengers, and the results implicated that auxiliary events such as transferring trains can enhance overall passenger anxiety.

Indicators relating to PACT Scenario 2: Choice of Internet Service Provider (surveillance of Internet usage)

Jensen et al 2005 - Privacy practices of Internet users Self-reports Versus Observed Behaviour
This paper reports on a study in which users privacy concerns regarding online decision making were analysed and what users said was contrasted with what they did in an experimental e-commerce scenario. The study was divided into four separate but interrelated sections: (1) A basic demographic survey. (2) A survey of privacy values and attitudes. (3) A set of questions challenging users’ knowledge of specific technologies and how they affect privacy. (4) An experiment presenting subjects with a series of pair-wise comparison tasks to determine the effect privacy indicators have on actual behaviour.

Dinev & Hart 2006 - An Extended Privacy Calculus Model for E-Commerce Transactions
The goal of the study was to develop and empirically test an extended model of privacy calculus in which a set of contrary beliefs was hypothesized to affect individuals’ willingness to provide personal information to complete transactions on the Internet. A theoretical model that incorporated contrary factors representing elements of a privacy calculus was tested using data gathered from 369 respondents. Structural equations modelling (SEM) using LISREL validated the instrument and the proposed model.
Indicators relating to PACT Scenario 3: Crisis management and response (surveillance and monitoring of healthcare records)

This study considered whether individuals’ attitudes towards Electronic Health Records (EHRs) can change in light of significant concerns surrounding the privacy of personal information. A likelihood model was used to investigate attitudinal change by using the opting-in to an EHR system as the dependent variable, and the findings of the model were complemented by a 366 person sample which was used to investigate attitudes supporting EHRs.

Hwang et al (2012) - The Differing Privacy Concerns Regarding Exchanging Electronic Medical Records of Internet Users in Taiwan
This study was concerned with the privacy concerns of internet users’ electronic medical records and the relation to individuals’ demographic background and electronic medical record awareness. Based upon an existing scale, the authors conducted an online survey that explored the dimensions of collection, unauthorized access, secondary use, and errors to calculate users’ privacy concerns in regards to electronic medical records.
Appendix C: Detailed list of indicators

**JENSEN et al 2005 - Privacy practices of Internet users Self-reports Versus Observed Behaviour**

Participant privacy attitudes and concerns – 5 point Likert scale (Strongly agree – Strongly Disagree)

- I am concerned about online identity theft*
- I am concerned about online credit card fraud
- I am concerned about my privacy on line*
- I am concerned about my privacy in everyday life*
- I am likely to read the privacy policy of a site I visit for the first time
- I am likely to read the privacy policy of a site which does not ask me for information
- I am likely to read the privacy policy of an ecommerce site before buying anything*
- I am likely to re-check the privacy policies of sites I frequently visit
- What privacy policies say frequently influences my decision whether to visit or use a websites
- Privacy policies accurately reflect what companies do*
- Privacy policies are easy to find
- It is important to me that websites publish privacy policies
- Response rates to privacy attitudes survey items.

(Questions used to map participants to the three Westin categories are marked with a “*”)

**Dinev & Hart 2006 - An Extended Privacy Calculus Model for E-Commerce Transactions**

<table>
<thead>
<tr>
<th>Latent Variable</th>
<th>Item</th>
<th>Scales</th>
</tr>
</thead>
<tbody>
<tr>
<td>Willingness to provide personal information to transact on the Internet (PPIT)</td>
<td>To what extent are you willing to use the Internet to do the following activities?</td>
<td>Not at all–Very much</td>
</tr>
<tr>
<td>PPIT 1: Purchase goods (e.g., books or CDs) or services (e.g., airline tickets or hotel reservations) from websites that require me to submit accurate and identifiable information (i.e., credit card information)</td>
<td>PPIT 2: Retrieve information from websites that require me to submit accurate and identifiable registration information, possibly including credit card information (e.g., using sites that provide personalized stock quotes, insurance rates, or loan rates; or using sexual or gambling websites)</td>
<td></td>
</tr>
<tr>
<td>PPIT 3: Conduct sales transactions at e-commerce sites that require me to provide credit card information (e.g., using sites for purchasing goods or software)</td>
<td>PPIT 4: Retrieve highly personal and password-protected financial information (e.g., using websites that allow me to access my bank account or my credit card account)</td>
<td></td>
</tr>
<tr>
<td>Perceived Internet privacy risk (PR)</td>
<td>What do you believe is the risk for regular Internet users due to the possibility that</td>
<td>Very low risk–Very high risk</td>
</tr>
<tr>
<td>PR1: Records of transactions could be sold to third parties?</td>
<td>PR2: Personal information submitted could be misused?</td>
<td></td>
</tr>
<tr>
<td>PR3: Personal information could be made available to unknown individuals or companies without your knowledge?</td>
<td>PR4: Personal information could be made available to government agencies?</td>
<td></td>
</tr>
</tbody>
</table>
Internet privacy concerns (PC)

Indicate the extent to which you are concerned about the following:

PC1: I am concerned that the information I submit on the Internet could be misused.
PC2: I am concerned that a person can find private information about me on the Internet.
PC3: I am concerned about submitting information on the Internet, because of what others might do with it.
PC4: I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee.

Internet trust (T)

Rate the extent to which you agree with the following statements:

T1: Internet websites are safe environments in which to exchange information with others.
T2: Internet websites are reliable environments in which to conduct business transactions.
T3: Internet websites handle personal information submitted by users in a competent fashion.

Personal Internet interest (PI)

Rate the extent to which you agree with the following statements:

PI1: I find that personal interest in the information that I want to obtain from the Internet overrides my concerns of possible risk or vulnerability that I may have regarding my privacy.
PI2: The greater my interest to obtain a certain information or service from the Internet, the more I tend to suppress my privacy concerns.
PI3: In general, my need to obtain certain information or services from the Internet is greater than my concern about privacy.

Chellappa and Sin 2005 - Personalization versus Privacy: An Empirical examination of the online consumer's dilemma

Survey instrument

(Items were modified to match the specifics of each industry and relevant examples were provided to the participants)

Consumers' concern for privacy

- PRI1 I am sensitive about giving out information regarding my preferences
- PRI2 I am concerned about anonymous information (information collected automatically but cannot be used to identify me, such as my computer, network information, operating system, etc.) that is collected about me.
- PRI3 I am concerned about how my personally un-identifiable information (information that I have voluntarily given out but cannot be used to identify me, e.g., Zip Code, age-range, sex, etc.) will be used by the firm.
- PRI4 I am concerned about how my personally identifiable information (information that I have voluntarily given out AND can be used to identify me as an individual, e.g., name, shipping address, credit card or bank account information, social security number, etc.) will be used by the firm.

Consumer comfort in using personalization services (proxy for likelihood)

- LIK1 I am comfortable providing information about me to this firm in return for personalized services and products.
- LIK2 I am comfortable in using the Web to purchase services and products.

Trust building factors in the usage personalization services

- FAM I am familiar with the Web site(s) of (names of firms omitted).
- EXP I have previously used or purchased services or products from (names of firms omitted).
Hui et al 2007 - The Value of Privacy Assurance - An exploratory field experiment in Singapore that assessed the values of two types of privacy assurance: privacy statements and privacy seals

Personal Information Requested in Survey

The sensitivity scores were obtained by asking subjects to rate (on a seven-point scale of not sensitive to extremely sensitive), in the follow-up survey, the sensitivity of each of the information items that they were asked to provide in the main survey. We then averaged the scores across subjects to obtain the scores in the second column. Note that since we varied how much information was requested, not all subjects rated every item. The number of subjects who were asked to provide each item is shown in the last column.

Items 1, 2, 3, and 9 can be roughly classified as personal identifier information, 4 through 8 and 10 and 11 can be classified as demographics information, 12 through 19 can be classified as financial information, and, finally, 20 through 23 can be classified as education information.

<table>
<thead>
<tr>
<th>Requested information</th>
<th>Average sensitivity</th>
<th>Number of subjects</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Name</td>
<td>3.83</td>
<td>109</td>
</tr>
<tr>
<td>2. E-mail address</td>
<td>3.87</td>
<td>109</td>
</tr>
<tr>
<td>3. Address</td>
<td>5.02</td>
<td>109</td>
</tr>
<tr>
<td>4. Citizenship</td>
<td>2.74</td>
<td>109</td>
</tr>
<tr>
<td>5. Gender</td>
<td>2.31</td>
<td>103</td>
</tr>
<tr>
<td>6. Marital status</td>
<td>2.51</td>
<td>99</td>
</tr>
<tr>
<td>7. Ethnicity</td>
<td>2.46</td>
<td>93</td>
</tr>
<tr>
<td>8. Country of residence</td>
<td>2.55</td>
<td>87</td>
</tr>
<tr>
<td>9. Phone number</td>
<td>5.79</td>
<td>84</td>
</tr>
<tr>
<td>10. Occupation</td>
<td>3.04</td>
<td>77</td>
</tr>
<tr>
<td>11. Household size</td>
<td>3.60</td>
<td>70</td>
</tr>
<tr>
<td>12. Monthly household income</td>
<td>5.25</td>
<td>64</td>
</tr>
<tr>
<td>13. Identity card/passport number</td>
<td>5.81</td>
<td>62</td>
</tr>
<tr>
<td>14. Banks/financial companies that you have accounts</td>
<td>5.27</td>
<td>55</td>
</tr>
<tr>
<td>15. Bank account balance</td>
<td>6.53</td>
<td>49</td>
</tr>
<tr>
<td>16. Personal monthly expenditure</td>
<td>4.90</td>
<td>42</td>
</tr>
<tr>
<td>17. Types of credit cards owned</td>
<td>4.50</td>
<td>38</td>
</tr>
<tr>
<td>18. Types of personal debt</td>
<td>5.37</td>
<td>30</td>
</tr>
<tr>
<td>19. Amount of personal debt</td>
<td>5.92</td>
<td>24</td>
</tr>
<tr>
<td>20. Highest education achieved</td>
<td>2.79</td>
<td>19</td>
</tr>
<tr>
<td>21. Name of educational institution corresponding to (20)</td>
<td>3.19</td>
<td>16</td>
</tr>
<tr>
<td>22. Average grade point average</td>
<td>4.20</td>
<td>10</td>
</tr>
<tr>
<td>23. Number of courses failed in the past</td>
<td>3.75</td>
<td>4</td>
</tr>
</tbody>
</table>

Measurement Items

Trust propensity

- I feel that people are generally trustworthy.
- I feel that people are generally reliable.

Information misuse experience

- How many times of personal information misuse have you encountered in the past?

Internet shopping experience

- In the past year, how many times have you shopped via the Internet?

Privacy concerns

(a) Cookie setting: We asked subjects to select their cookie policy from the following list (subjects who chose one of the last three options were considered more concerned about privacy):

- My preferences are set to always accept cookies.
- I don’t know what a cookie is.
- I don’t know what my cookie preferences are set to.
- My browser doesn’t support cookies.
- My preferences are set to only accept cookies from the same site I am browsing.
• My preferences are set to warn me before accepting cookies.
• My preferences are set to ignore/never accept cookies.

(b) Measures of Smith et al. (1996): The eight items were:
• I’m concerned that companies are collecting too much personal information about me.
• Companies should have better procedures to correct errors in personal information.
• Companies should never sell the personal information in their computer databases to other companies.
• Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.
• Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.
• When companies ask me for my personal information, I sometimes think twice before providing it.
• Computer databases that contain personal information should be protected from unauthorized access—no matter how much it costs.
• Companies should devote more time and effort to verifying the accuracy of the personal information in their databases.

The responses to these eight questions were averaged to produce a privacy concern score for each subject.

Note: For information misuse and Internet shopping experiences, because the subjects’ responses were noisy (some subjects entered rounded or wide ranges of numbers), we coded their responses as binary variables: having or not having the experiences. All Likert scale items in this study (including the manipulation checks and the measures in the following two tables) had the anchors 1 = totally disagree and 7 = totally agree.

Privacy assurances
• Company X has a privacy statement.
• Company X has a TRUSTe privacy seal.

For those who were presented a privacy statement:
I have read through Company X’s privacy statement and understood it fully (mean = 4.62, standard deviation = 1.47).

For those who were also presented a privacy seal:
I understand the purpose of TRUSTe’s privacy seal fully (mean = 4.48, standard deviation=1.53).

Monetary incentive
• The amount of money I received is adequate to compensate my effort and time spent in participating in the mobile device survey.
• The reward I received from participating in the mobile device survey is worth the information I gave. (mean = 4.66, standard deviation = 1.45)

Information request
• I feel that the mobile device survey is collecting too much personal information about me.
• I am giving out a lot of information. (mean = 4.54, standard deviation = 1.46)

Familiarity with privacy seals
• I am familiar with foreign privacy seals such as TRUSTe, WebTrust and BBB Online (mean = 6.58; standard deviation = 0.87).
• I am familiar with local privacy seals such as TrustSg and CaseTrust (mean = 2.62, standard deviation = 1.77)

Tendency to lie
• Sometimes, I give false information (mean = 2.51, standard deviation = 1.60)

Trust in information handling practice
• I trust Company X in handling my information (mean = 5.46, standard deviation = 1.34).

Smith et al 1996 Information Privacy: Measuring Individuals’ Concerns about Organizational Practices

Here are some statements about personal information. From the standpoint of personal privacy, please indicate the extent to which you, as an individual agree or disagree with each statement by circling the appropriate number.*

A. It usually bothers me when companies ask me for personal information.
B. All the personal information in computer databases should be double-checked for accuracy—no matter how much this costs.
C. Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.
D. Companies should devote more time and effort to preventing unauthorized access to personal information.
E. When companies ask me for personal information, I sometimes think twice before providing it.
F. Companies should take more steps to make sure that the personal information in their files is accurate.
G. When people give personal information to a company for some reason, the company should never use the information for any other reason.
H. Companies should have better procedures to correct errors in personal information.
I. Computer databases that contain personal information should be protected from unauthorized access—no matter how much it costs.

J. It bothers me to give personal information to so many companies.

K. Companies should devote more time and effort to verifying the accuracy of the personal information in their databases.

L. Companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.

N. Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.

O. I'm concerned that companies are collecting too much personal information about me.

Items A, E, J, and 0 comprise the "Collection" subscale; items B, F, H, and L comprise the "Errors" subscale; items C, G, K, and M comprise the "Unauthorized Secondary Use" subscale; and items D, I, and N comprise the "Improper Access" subscale. Subscale scores are calculated by averaging the responses to the items for each subscale; an overall score is then calculated by averaging the subscale scores.

Buchanan et al 2007 - Development of measures of online privacy concern & protection for use on the Internet

Privacy attitude factor loadings.

Privacy Concern
1 In general, how concerned are you about your privacy while you are using the internet?
2 Are you concerned about online organisations not being who they claim they are?
3 Are you concerned that you are asked for too much personal information when you register or make online purchases?
4 Are you concerned about online identity theft?
5 Are you concerned about people online not being who they say they are?
6 Are you concerned that information about you could be found on an old computer?
7 Are you concerned who might access your medical records electronically?
8 Are you concerned about people you do not know obtaining personal information about you from your online activities?
9 Are you concerned that if you use your credit card to buy something on the internet your credit card number will obtained/intercepted by someone else?
10 Are you concerned that if you use your credit card to buy something on the internet your card will be mischarged?
11 Are you concerned that an email you send may be read by someone else besides the person you sent it to?
12 Are you concerned that an email you send someone may be inappropriately forwarded to others?
13 Are you concerned that an email you send someone may be printed out in a place where others could see it?
14 Are you concerned that a computer virus could send out emails in your name?
15 Are you concerned about emails you receive not being from whom they say they are?
16 Are you concerned that an email containing a seemingly legitimate internet address may be fraudulent?

Note. The instructions accompanying the scale were "For this part of the survey, we are interested in any privacy concerns you might have when online. Please answer every question using the full scale provided." Participants responded using a 5-point scale for each item (not at all – very much).

Mcknight et al 2002 - Developing and Validating Trust Measures for e-commerce

Measures

Disposition to Trust

Benevolence
1. In general, people really do care about the well-being of others.
2. The typical person is sincerely concerned about the problems of others.
3. Most of the time, people care enough to try to be helpful, rather than just looking out for themselves.

Integrity
1. In general, most folks keep their promises.
2. I think people generally try to back up their words with their actions.
3. Most people are honest in their dealings with others.

Competence
1. I believe that most professional people do a very good job at their work.
2. Most professionals are very knowledgeable in their chosen field.
3. A large majority of professional people are competent in their area of expertise.

Trusting Stance
1. I usually trust people until they give me a reason not to trust them.
2. I generally give people the benefit of the doubt when I first meet them.
3. My typical approach is to trust new acquaintances until they prove I should not trust them.
**Institution-Based Trust**

*Situational Normality-General*
1. I feel good about how things go when I do purchasing or other activities on the Internet.
2. I am comfortable making purchases on the Internet.

*Situational Normality-Benevolence*
1. I feel that most Internet vendors would act in a customers' best interest.
2. If a customer required help, most Internet vendors would do their best to help.
3. Most Internet vendors are interested in customer well-being, not just their own wellbeing.

*Situational Normality-Integrity*
1. I am comfortable relying on Internet vendors to meet their obligations.
2. I feel fine doing business on the Internet since Internet vendors generally fulfill their agreements.
3. I always feel confident that I can rely on Internet vendors to do their part when I interact with them.

*Situational Normality-Competence*
1. In general, most Internet vendors are competent at serving their customers.
2. Most Internet vendors do a capable job at meeting customer needs.
3. I feel that most Internet vendors are good at what they do.

**Structural Assurance**
1. The Internet has enough safeguards to make me feel comfortable using it to transact personal business.
2. I feel assured that legal and technological structures adequately protect me from problems on the Internet.
3. I feel confident that encryption and other technological advances on the Internet make it safe for me to do business there.
4. In general, the Internet is now a robust and safe environment in which to transact business.

**Trusting Beliefs**

*Benevolence*
1. I believe that LegalAdvice.com would act in my best interest.
2. If I required help, LegalAdvice.com would do its best to help me.
3. LegalAdvice.com is interested in my well-being, not just its own.

*Integrity*
1. LegalAdvice.com is truthful in its dealings with me.
2. I would characterize LegalAdvice.com as honest.
3. LegalAdvice.com would keep its commitments.
4. LegalAdvice.com is sincere and genuine.

*Competence*
1. LegalAdvice.com is competent and effective in providing legal advice.
2. LegalAdvice.com performs its role of giving legal advice very well.
3. Overall, LegalAdvice.com is a capable and proficient Internet legal advice provider.
4. In general, LegalAdvice.com is very knowledgeable about the law.

**Trusting Intentions**

*Willingness to Depend*
1. When an important legal issue or problem arises, I would feel comfortable depending on the information provided by LegalAdvice.com.
2. I can always rely on LegalAdvice.com in a tough legal situation.
3. I feel that I could count on LegalAdvice.com to help with a crucial legal problem.
4. Faced with a difficult legal situation that required me to hire a lawyer *(for a fee)*, I would use the firm backing LegalAdvice.com.

*Subjective Probability of Depending*
1. If I had a challenging legal problem, I would want to use LegalAdvice.com again.*

*Follow Advice*
2. I would feel comfortable acting on the landlord/tenant information given to me by LegalAdvice.com.
3. I would not hesitate to use the landlord/tenant information LegalAdvice.com supplied me.
4. I would confidently act on the legal advice I was given by LegalAdvice.com.
5. I would feel secure in using the landlord/tenant information from LegalAdvice.com.
6. Based on the advice I just read, I would serve notice, wait, go ahead and get the repair done, and then deduct the cost of the repair from my rent.

Suppose you wanted more specific information about landlord/tenant relationships and you could consult (one time only) by telephone with one of the LegalAdvice.com lawyers for 15–30 minutes *(free of charge)*. For this service, please answer the following:
1. I would be willing to provide information like my name, address, and phone number to LegalAdvice.com.
2. I would be willing to provide my social security number to LegalAdvice.com.
3. I would be willing to share the specifics of my legal issue with LegalAdvice.com.

Suppose the LegalAdvice.com site was *not* free, but charged to access information on the site. Answer the following questions:
1. Faced with a difficult legal situation, I would be willing to pay to access information on the LegalAdvice.com Web site.
2. I would be willing to provide credit card information on the LegalAdvice.com Web site.
3. Given a tough legal issue, I would be willing to pay for a 30-minute phone consultation with a LegalAdvice.com lawyer.

**Personal Innovativeness**
1. I like to explore new Web sites.
2. When I hear about a new Web site, I often find an excuse to go visit it.
3. Among my peers, I am usually the first to try out new Internet sites.
4. In general, I am not interested in trying out new Web sites.
5. When I have some free time, I often explore new Web sites.

**General Web Experience**
On average, how much time per week do you spend on each of the following Web activities? (Scale: None, 0–30 minutes, 30–60 minutes, 1–2 hours, 2–4 hours, 4–8 hours, 8+ hours)
1. Reading newspapers on the Web?
2. Reading and/or posting messages to news groups?
3. Accessing information on the Web about products and services you may buy?
4. Shopping (i.e. actually purchasing something) on the Web?

**Perceived Site Quality**
1. Overall, this site worked very well technically.
2. Visually, this site resembled other sites I think highly of.
3. This site was simple to navigate.
4. On this site, it was easy to find the information I wanted.
5. This site clearly showed how I can contact or communicate with LegalAdvice.com.

---

**NAP (2008) - Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment**

Right to Privacy (Public Agenda Foundation and CBS/New York Times Surveys)
“Do you believe that the right to privacy is currently under serious threat, is it basically safe, or has it already been lost?”
- Basically safe
- Currently under serious threat
- Has already been lost
- Don’t know

“How much do you worry that computers and technology are being used to invade your privacy?”
- A lot
- Some

Here are some increased powers of investigation that law enforcement agencies might use when dealing with people suspected of terrorist activity, which would also affect our civil liberties. For each, please say if you would favor or oppose it? ("Favor")
- Stronger document and physical security checks for travellers
- Stronger document and physical security checks for access to government and private office buildings
- Expanded undercover activities to penetrate groups under suspicion
- Use of facial recognition technology to scan for suspected terrorists at various locations and public events
- Issuance of a secure ID technique for persons to access government and business computer systems, to avoid disruptions
- Closer monitoring of banking and credit card transactions, to trace funding sources
- Adoption of a national ID system for all U.S. citizens
- Expanded camera surveillance on streets and in public places
- Law enforcement monitoring of Internet discussions in chat rooms and other forums
- Expanded government monitoring of cell phones and e-mail, to intercept communications

Would you favor or oppose the following measures to curb terrorism?" ("Favor")
- Requiring that all citizens carry a national identity card at all times to show to a police officer on request
- Allowing airport personnel to do extra checks on passengers who appear to be of Middle-Eastern descent
- Allowing the U.S. government to monitor your personal telephone calls and e-mails
- Allowing the U.S. government to monitor your credit card purchases
**University of Huddersfield 2012 - Evaluating measures to improve personal security and the value of their benefits**

Q15. During the past 6 months, have you had cause to worry about your personal security whilst at this station?
(Yes/No)

Q16. Thinking about the last time you felt concerned, how worried did you feel (not very worried; a little bit worried; quite worried; very worried)

Q17. During the past 12 months, have concerns about personal security stopped you from travelling from this station or to adapt your journey?
(Yes/No)

Q18. How much of a problem are the following at this station (a very big problem; a fairly big problem; not a very big problem; not a problem at all; don't know)
   a) Rubbish or litter lying around
   b) Vandalism and graffiti
   c) People using or dealing drugs
   d) People being drunk or rowdy
   e) People being harassed or intimidated
   f) Car crime (theft or damage)


A. 25-30 deaths in a single Underground accident is worse than 25-30 deaths in separate Underground accidents.

B. The experts probably have a pretty good idea about the causes of small-scale Underground accidents and the number of people likely to be killed in them over the next 25 years, but they have much less idea about the chances of large-scale Underground accidents and the number of people likely to be killed in those kinds of accidents over the next 25 years.

C. Victims of large-scale Underground accidents are typically not to blame for them, whereas small-scale Underground accidents are likely to be at least partly the victim's own fault.

D. You can be pretty sure that if you spend more money trying to prevent small-scale accidents then fewer will occur; whereas, however much you spend trying to prevent large-scale accidents, it probably won't make much difference: in some cases, they might not happen anyway, and in other cases, some freak set of circumstances may still cause them to occur.

E. The thought of being killed in an Underground accident is worse than the thought of being killed in a road accident.

F. London Underground is providing a public service and therefore has a duty to protect the public’s safety, whereas road users have a greater responsibility to look after their own safety.

G. When I travel by Underground, it's usually because there's no real alternative, and I therefore have little choice but to accept whatever risks are involved; whereas when I travel by car, it's usually because I choose to do so, and I therefore voluntarily accept whatever risks are involved.

H. When I'm travelling by car, I have much more control over my own safety than I do when I'm travelling on the Underground.

**Cheng 2010 - Exploring passenger anxiety associated with train travel**

Measurement items of passengers’ riding anxiety

Question

Do you agree that the following episodes make you anxious during your travel by train? (5-point scale—5 for “strongly disagree,” 4 for “disagree,” 3 for “neutral,” 2 for “agree,” and 1 for “strongly agree”)

When considering the convenience of transport to the railway station

When I need to transfer via another train before arriving at my destination

When I take the train by myself Time of a day

When I take a night train

When the train is delayed

When possible attack could occur at the station, on the platform, or inside the coach

When strangers sit next to me on the train

When I cannot quickly find my coach on the platform

When there is not enough waiting seats on the train or platform
Poor provision of timetable information (outdated, difficult to get)
When gap between the train and platform is large
When the train is crowded
Noise in the train


Concern for Information Privacy
Here are some statements about personal information. From the standpoint of personal privacy, please indicate the extent to which you, as an individual, agree or disagree with each statement by circling the appropriate number (1 = strongly disagree, 7 = strongly agree).

Collection
C1. It usually bothers me when health care entities ask me for personal information.
C2. When health care entities ask me for personal information, I sometimes think twice before providing it.
C3. It bothers me to give personal information to so many health care entities.
C4. I’m concerned that health care entities are collecting too much personal information about me.

Errors
E1. All the personal information in computer database should be double-checked for accuracy—no matter how much this costs.
E2. Health care entities should take more steps to make sure that the personal information in their files is accurate.
E3. Health care entities should have better procedures to correct errors in personal information.
E4. Health care entities should devote more time and effort to verifying the accuracy of the personal information in their databases.

Unauthorized Access (Improper Access)
UA1. Health care entities should devote more time and efforts to preventing unauthorized access to personal information.
UA2. Computer databases that contain personal information should be protected from unauthorized access no matter how much it costs.
UA3. Health care entities should take more steps to make sure that unauthorized people cannot access personal information in their computers.

Secondary Use
SU1. Health care entities should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.
SU2. When people give personal information to a company for some reason, the company should never use the information for any other reason.
SU3. Health care entities should never sell the personal information in their computer databases to other health care entities.
SU4. Health care entities should never share personal information with other health care entities unless it has been authorized by the patient who provided the information.

Hwang et al (2012) - The Differing Privacy Concerns Regarding Exchanging Electronic Medical Records of Internet Users in Taiwan

<table>
<thead>
<tr>
<th>Indicators for concerns regarding health information exchange</th>
<th>Item</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dimension</strong></td>
<td></td>
</tr>
<tr>
<td>Collection</td>
<td></td>
</tr>
<tr>
<td>It bothers me when medical facilities ask me for personal information.</td>
<td></td>
</tr>
<tr>
<td>I sometimes think for a while when medical facilities ask me to provide personal information.</td>
<td></td>
</tr>
<tr>
<td>It bothers me to give personal information to so many medical facilities.</td>
<td></td>
</tr>
<tr>
<td>It bothers me that medical facilities collect too much personal information.</td>
<td></td>
</tr>
<tr>
<td>Unauthorized Access</td>
<td></td>
</tr>
<tr>
<td>Medical facilities should devote more time and efforts to preventing the unauthorized access of patients’ personal information.</td>
<td></td>
</tr>
<tr>
<td>Medical facilities should prevent unauthorized people from accessing patients’ personal information without considering the cost.</td>
<td></td>
</tr>
<tr>
<td>Medical facilities should take more measures to ensure that unauthorized people can not use their computer to access patients’ personal information.</td>
<td></td>
</tr>
</tbody>
</table>
**Secondary Use**

Medical facilities should never use patients’ personal information for purposes other than medical care, unless it has been authorized by the patient.
Medical facilities should not use the personal information provided by patients for any purpose other than those required for medical care.
Medical facilities should never sell patients’ personal information to other institutions.
Medical facilities should not share patients’ personal information with other institutions unless it has been authorized by the patient.
Medical facilities should repeatedly check the accuracy of patients’ personal information without considering cost.
Medical facilities should use more procedures to ensure the accuracy of patients’ personal information.
Medical facilities should have a more comprehensive procedure to correct for errors in patients’ personal information.
Medical facilities should devote more time and manpower to verify the accuracy of patients’ personal information.


For each of the following statements, please indicate the likelihood of engaging in each activity. Provide a rating from 1 to 5, using the following scale:

1 = Extremely unlikely, 2 = Not sure, 3 = Extremely likely

1. ______ Admitting that your tastes are different from those of your friends. (S)
2. ______ Arguing with a friend who has a very different opinion on an issue. (S)
3. ______ Asking your boss for a raise. (S)
4. ______ Betting a day’s income at the horse races. (F)
5. ______ Buying an illegal drug for your own use. (E)
6. ______ Chasing a tornado by car to take photos that you can sell to the press. (R)
7. ______ Cheating a fair amount on your income tax. (E)
8. ______ Cheating on an exam. (E)
9. ______ Co-signing a new car loan for a friend. (F)
10. ______ Dating someone that you are working with. (S)
11. ______ Deciding to share an apartment with someone you don’t know well. (S)
12. ______ Disagreeing with your father on a major issue. (S)
13. ______ Driving home after you had three drinks in the last two hours. (E)
14. ______ Eating ‘expired’ food products that still ‘look okay’. (H)
15. ______ Exploring an unknown city or section of town. (R)
16. ______ Forging somebody’s signature. (E)
17. ______ Frequent binge drinking. (H)
18. ______ Going camping in the wild. (R)
19. ______ Going down a ski run that is too hard or closed. (R)
20. ______ Going on a safari in Kenya. (R)
21. ______ Going on a two-week vacation in a foreign country without booking accommodations ahead. (R)
22. ______ Going whitewater rafting at high water in the spring. (R)
23. ______ Ignoring some persistent physical pain by not going to the doctor. (H)
24. ______ Illegally copying a piece of software. (E)
25. ______ Taking a medical drug that has a high likelihood of negative side effects. (H)
26. ______ Traveling on a commercial airplane. (R)
27. ______ Plagiarizing a term paper. (E)
28. ______ Engaging in unprotected sex. (H)
29. ______ Investing 10% of your annual income in a blue chip stock. (F)
30. ______ Investing 10% of your annual income in a very speculative stock. (F)
31. ______ Investing 10% of your annual income in government bonds (treasury bills). (F)
32. _____ Investing in a business that has a good chance of failing. (F)
33. _____ Lending a friend an amount of money equivalent to one month’s income. (F)
34. _____ Moving to a new city. (S)
35. _____ Never using sunscreen when you sunbathe. (H)
36. _____ Never wearing a seatbelt. (H)
37. _____ Not having a smoke alarm in or outside of your bedroom. (H)
38. _____ Openly disagreeing with your boss in front of your coworkers. (S)
39. _____ Periodically engaging in a dangerous sport (e.g. mountain climbing or sky diving). (R)
40. _____ Regularly riding your bicycle without a helmet. (H)
41. _____ Shoplifting a small item (e.g. a lipstick or a pen). (E)
42. _____ Smoking a pack of cigarettes per day. (H)
43. _____ Speaking your mind about an unpopular issue at a social occasion. (S)
44. _____ Spending money impulsively without thinking about the consequences. (F)
45. _____ Stealing an additional TV cable connection. (E)
46. _____ Taking a day’s income to play the slot-machines at a casino. (F)
47. _____ Taking a job where you get paid exclusively on a commission basis. (F)
48. _____ Trying bungee jumping. (R)
49. _____ Using office supplies for your personal business. (E)
50. _____ Wearing unconventional clothes. (S)