Project acronym:	PRISMS
Project title:	The PRIvacy and Security MirrorS: "Towards a European framework for integrated decision making"
Project number:	285399
Programme:	Seventh Framework Programme for research and technological development
Objective:	SEC-2011.6.5-2: The relationship between Human privacy and security
Contract type:	Collaborative project
Start date of project:	01 February 2012
Duration:	42 months

Deliverable D8.1:
Validating the hypotheses: Interviews with privacy and security experts

Editor:	Michael Friedewald, Fraunhofer ISI, David Barnard-Wills, Trilateral Research & Consulting
Dissemination level:	Public
Deliverable type:	Report
Version:	0
Submission date:	

Contents

1 KEY SUGGESTIONS FOR PRISMS SURVEY BASED UPON EXPERT VALIDATION

David Barnard-Wills (Trilateral Research & Consulting)

1.1 INTRODUCTION

In order to validate and check the work conducted by the PRISMS project to this point, and in preparation for the focus groups and survey to be conducted in WP 9, we presented the collated hypotheses and working assumptions generated by the preceding work packages to ten privacy and security experts suggested by the PRISMS partners. We conducted interviews with these experts with the intent of understanding: if we are heading in the right direction (or not); if there is anything missing, or that we need to take into account; expert's experience of empirical research in the areas of privacy, security, trust, public perceptions and acceptance of security technologies; as well as any thoughts on the process of turning hypotheses into research questions. This report collates the findings and comments from those interviews.

This report contains the key points distilled from all the interviews. An internal version of this report for use within the PRISMS project contained full detailed notes on the interviews as well as an annex with the hypotheses that were shared with these experts by the project.

The interviews raised a number of points for consideration for the PRISMS project, and for the creation and conduct of the survey instrument. As several points were addressed by multiple participants, they have been collated here thematically.

The discussions were generally positive, with participants supportive of the aims of the project. The discussions were therefore focused upon how the project could refine its hypotheses in order to better meet its objectives, and how to ensure that the survey produced informative findings.

1.2 SPECIFIC AND GROUNDED QUESTIONS

Several experts drew attention to the importance of creating specific hypotheses with a clear sense of what exactly we wished to investigate, rather than broad hypotheses, that were not driving the project forward. Setting specific hypotheses to be explicitly tested and explored would aid us in generating specific questions. We were warned not to focus upon "trivial" hypotheses.

Similarly, we were advised to maintained grounded questions, based upon a context, or a real world dilemma, rather than engaging in the abstract. Understandings of privacy were seen as highly context dependent. Grounded questions also potential avoid some of the sensitising and social desirability effects of asking direct questions about privacy and security.

We were advised to separate hypotheses that were our foundational working assumptions (supported by the literature) from hypotheses that were to be actively tested in the survey design. The project proposal and Description of Work should serve as a guide to this.

1.3 THE PERIL OF DEMOGRAPHICS

There were several comments on the importance of demographic variables and statistics. There was broad support for the expectation of variance in various attitudes towards privacy and security across cultures, and across ages, genders and other demographic variables. However some experts expressed concern that a study that was too focused upon demographic variables for its explanatory models would result in a relatively descriptive set of results, which would be productive for producing interesting and insightful accounts of the processes of acceptance and attitude formation. Demographics are relatively easy questions to ask, but we should be cautious about expecting too many clear correlations, and then drawing generalisations based upon demographic information. We are likely to see as much as if not more variation in attitudes with countries as between countries.

A number of other issues also emerged in relation to demographics: unclear indicators, settled demographics against current situations, the difference between privacy attitudes and other cultural beliefs, generational diversity, and non-national clusters of attitudes. These are explored in the following sub-sections.

1.3.1 Unclear indicators

Issues were raised regarding some of the terminology in the hypotheses that generalised countries. For example, H25 "Individualistic countries tend to give up privacy more easily". It was unclear what "individualistic countries" meant. Similarly for H24 "In those parts of Europe where interpersonal trust is low, citizens are willing to give up privacy for a potential increase of security". Is our intention to operationalize these descriptions using a separate metric from another research project? A suggested source was the world values project: http://www.worldvaluessurvey.org/wvs/articles/folder_published/article_base_46

It was also suggested that given the somewhat unique position of the UK, it might be worth separating the UK out from "Western Europe" (in hypotheses such as H58). Southern Europe was conspicuous in its absence from the current hypotheses. Is there any material from the previous work packages or literature, which would suggest relevant hypotheses about attitudes to privacy and security in Southern Europe?

1.3.2 Settled demographics versus current situation

One demographic avenue that emerged was the potential to examine if attitudes to surveillance and security cross borders. The experience of immigrants was highlighted due to the frequent focus of surveillance and security technologies upon these groups. This also provides an opportunity to attempt to understand the extent to which attitudes towards surveillance are determined by country of origin, country of residence, or experience of surveillance. Do immigrants have attitudes towards surveillance and security that more closely mirror their host country than their country of origin? Do immigrant experiences of surveillance and security practices reduce their acceptance of these measures, as compared with non-immigrant populations?

Is our sample methodology able to accommodate questions in this vein? If the expected number of immigrant participants in each sample is low, then we may not get statistically significant differences.

1.3.3 Are privacy attitudes different to other cultural beliefs?

Related to the previous point, it was discussed to what extent attitudes towards privacy were different to other cultural beliefs, particularly in relation to immigrant populations. We might hypothesise that in general, cultural beliefs of immigrant populations tend towards alignment with the host country over time. However, given that immigrants (and minorities) tend to disproportionally encounter surveillance and security practices, might privacy be more highly valued than amongst the general population?

It was suggested that different "stereotypes" of citizens would like have very different propensities towards security and privacy we that we risk averaging this out by just looking at age, gender and religion. A range of potential beliefs that might influence attitudes towards security and privacy were suggested:

- Belief in technological neutrality
- Belief in (social/individual) control over technology.
- Belief that more data means more knowledge
- Experience with practices/technology

These beliefs are quite likely to be associated with differing attitudes to privacy and security. We do not currently have hypotheses associated with these beliefs. It may be appropriate to design survey questions to attempt to assess these beliefs, perhaps in the format of:

To what extent to do you agree with the following statements?
"Technology can be used for both good and bad purposes"
"Technology is the best option for solving social problems"
"I feel comfortable using modern technology"

1.3.4 Generational diversity?

Generational differences in privacy attitudes were of interest to several experts. Methodologically, this raised the issue of ensuring sufficient access to younger members of the population. This is a question for IPSOS – is their sampling method dependent upon fixed landlines, which many younger Europeans will not have access to, or do they have methods to ensure a generationally representative sample?

1.3.5 Clusters of concerns and attitudes

Our analysis must be able to identify regional clusters of privacy attitudes beyond the simple boundaries of Western/Eastern Europe.

1.4 TIPPING POINTS/DECISION BOUNDARIES

Of particular interest to several experts was understanding the changes and variations in context that would cause people to *change* their opinion on the acceptability or otherwise of a surveillance or security practice. This was counter to the assumption that demographics were primary determinants of attitude.

It was suggested that the vignettes would be a suitable place to investigate these differences through a series of similar vignettes that varied particular conditions, to see if these variations made a difference to the opinion of the participant.

For example: The vignette might first present a security practice, such as a body scanner in an airport, and ask the participant to comment on the acceptability of this arrangement. The participant is then provided with additional details or variations upon the scenario and asked to comment on the acceptability under these conditions. Variations might include being told that the scanner is operated by a private company rather than a government, or that any data from the scan is deleted immediately after use, or that a privacy impact assessment has been conducted prior to installing the technology. These variations are intended to drill down upon the factors that cause changes in attitudes.

Suggested variations included: police vs. private security firm, presence or absence of access controls or other security measures, online or offline use, the purpose of the security technology (preventing terrorism or profit protection), access to data stored on a home computer versus access to data stored in the cloud.

Alternatively, a series of questions could present a policy problem (for example organised crime, or terrorism) and then present a series of increasingly (or decreasingly) intrusive surveillance technologies, asking the participant if each technology in turn would be a proportionate response to the policy problem. The order of increase or decrease could be varied to reduce the influence of the list.

1.4.1 Questions based around policy responses

It was also suggested that we should align questions with current policy discourse around privacy protection measures (data protection law, privacy impact assessments, codes of practice, privacy by design, privacy by default) and attempt to determine the extent to which the presence or absence of these measures impacts upon attitudes. To the extent that Data Protection discourse is based around allowing collecting and processing of data provided that some conditions are met, do these conditions actually affect acceptability of practices for the population? The policy options could also be variables in the vignettes.

We currently do not have hypotheses related to how law and regulatory efforts affect attitudes to privacy and surveillance. Attitudes on this issued were divided amongst experts, with some thinking that law was influential, whilst others believing that privacy law was not particularly relevant to everyday decisions made by the public. We could potentially assess awareness of major legal instruments, or confidence in existing law.

1.5 SUPPORTING THE DECISION SUPPORT SYSTEM

It was suggested that given the aim of PRISMS to produce a decision support system (DSS), that the current hypotheses seemed to be lacking direct reference to this, and that we might seek to anticipate some of the demands and requirements of a DSS at this stage.

Involvement of the WP11 team in question formulation for the survey would therefore be advisable. If this is not possible, then some sense of the potential requirements of a DSS would be beneficial.

Alternatively, it might be a deliberate strategy to conduct a stand-alone survey as a form of knowledge generation, which is only then translated into a decision support framework.

1.6 MEDIA EFFECTS

The current hypotheses do not go into great detail about media influences on perceptions and attitudes towards security and privacy. Several experts identified the media as the key source of information on privacy and security, and as having a particular way of framing these issues.

Currently, H29 "Not only online communication habits but also offline communication experience, including participating in social events, exchange of news and information, the nature of information shared with others, and the expectations of what should and what should not be divulged about the respondent's private life in the various social circles, show correlations with the respondents' views on privacy and related subject areas" has some relation to media effects. H45 and H46 suggest that the attention the media pays to security/privacy is disproportionate, but we should separate these out into clear "not enough attention", and "too much attention."

Media effects may be an area we need to explore more. It is a complex field, with its own literature, however, we may be able to ask questions about the source of participants information on privacy and security, to determine the extent to which they are exposed to media messages on these issues. As well as the amount of attention to security and privacy, in the media, we may also ask if the respondent is satisfied with the tone of media coverage of these issues.

1.6.1 Imaginaries and available narratives

Given the assumption that available narratives (either originating with media or policy discourse) are highly influential on attitudes to privacy and security, it was suggested that we could attempt to understand the available narratives that participants use to make sense of privacy and surveillance, and which key events (related to H41 and H42) participants are aware of.

The use of Social Representation techniques was suggested (see interview notes with Sarah Spiekermann). In this approach, participants are asked to give a number of terms that they associate with a concept (e.g., "security", or "Google", or even "Google & Privacy") to understanding the associated ideas and concepts. Is such a technique possible within a survey instrument?

We could also attempt to understand the extent to which attitudes in particular countries correlate with the policies adopted by their governments.

A final form of available narrative is the particular history of a given country and if differences in attitudes towards privacy and security in different countries can be associated with their individual national history.

1.7 ENCOUNTERS AND EXPERIENCE

It was suggested in some discussion that personal experience of surveillance, privacy intrusions and security technologies (especially negative experience) would be strongly associated with negative attitudes towards the practices and technologies. Currently the hypotheses do not make significant reference to the experiences of the participant.

One element of this which was highlighted was the level of social media use of the participant, and that this might influence perceptions of online and offline privacy.

Experience of discrimination was also identified as potentially having an effect upon attitudes to privacy and security.

1.8 PRIVACY AS A SOCIAL GOOD

Several experts suggested that the current list of hypotheses appear to focus upon an individualistic model of privacy – as something that individuals possess and might be willing to give up in certain circumstances. These experts highlighted both the collective social value of privacy, and the related nature of privacy (that the privacy of one member of a group affects the privacy of other members of that group).

This could suggest questions to explore the extent to which the participant agrees with or supports, or is even aware of the social model of privacy. A hypothesis might be framed as:

"People who believe privacy is a social good, rather than an individual good, are less likely to find a potentially privacy invasive practice acceptable than those who do not."

Similarly, questions about fear of crime should distinguish between perception of individual risk of crime or exposure to harm, and the threat posed to society by crime more generally. People may feel that they personally are not at risk from crime, or from invasions of their privacy, but still believe that these are issues for society more broadly, and our survey design should be nuanced enough to accommodate these positions.

1.9 CRITICISMS OF THE TRADE-OFF MODEL

The aim of the survey is to determine whether people evaluate the introduction of security technologies in terms of a trade-off. We discussed the model of trade-offs between privacy and security with each of the experts, including the extent to which this was a suitable model for understanding the relationship between privacy and security; the extent to which this model was used to talk about the relationship between the two by the public, the media, and political actors; and the extent to which this was a suitable model for how people made decisions.

Criticisms of the trade-off model:

- Trade-off model is too abstract, distanced from day-to-day decision-making.
- Trade-off is a rhetorical move that automatically privileges security over privacy.
- Trade-off is lazy, unthinking media framing.
- Trade-off model assumes rational decision-making that is unsupported by evidence.

- People do not make a privacy calculus
- Poor evidence for panoptic effects – behaviour change arising from surveillance.
- Any proposed "trade off" happens prior to the individual moment of decision. The individual is presented with a fait accompli and must decide to oppose or resist an established practice.
- Impossible to "monetise" either side of the trade-off
- Many situations in which privacy is necessary for security or security for privacy.
- Trade-off model perhaps more useful for understanding political decisions and support for them as opposed to decisions to engage or avoid surveillance practices.
- Assumes that security means state security.

The trade-off model was further complicated by the suggestion that it should include trade-offs between privacy and convenience or practicality, and that these were more likely to be salient to everyday decision making. Much research in information security suggests that people are often willing trade off security for convenience.

1.9.1 Trading off whose privacy?

Related to the above criticisms, several contributors suggested that in many circumstances individuals were not asked to trade off their own privacy for security, but rather to support a situation in which the privacy of others was likely to be infringed. We should therefore develop a set of questions based around examining the extent to which people's acceptance of security and surveillance is affect by the stated or intended target of those measures.

It was suggested that even where an individual is likely to be the subject of surveillance as part of a population, the potential negative effects of that surveillance might be unevenly distributed. As such we may need to find a way to capture how much an individual feels that a surveillance practice might affect them.

1.10 WHAT IS TO BE PROTECTED/SECURED?

Several experts commented on the concept of security, and the extent to which the language of security immediately privileges a framework of meaning based around national security, and all the associated imagery, and appeals to the "responsible citizen" contributing to collective security. It was suggested that one approach to avoid this would be to avoiding using the language of security, but rather develop a metric based upon asking [not directly as a survey question]:

> What are individuals' basic needs?
> What are they afraid of?
> What risks are they exposed to?

There was also interest if the "broadened" concepts of security developed in Critical Security Studies, which push security beyond that of the nation state, or the concept of Human Security, had any purchase or recognition with the public. One approach may be to present a participant with a number of domains and ask them which they include with the concept of security.

1.11 A SURVEY METHODOLOGY WHICH IS AGNOSTIC TO PRIVACY AND SECURITY?

Experts generally agreed that both privacy and security were highly complex concepts, which has many different ways of understanding, both in the academic and practitioner fields, and likely amongst the general public. This raises the issue of handling this conceptual complexity within the survey design. Experts expressed concern that in many previous surveys, they could not be if the participants understood the concept of security or privacy, and if the researchers and the subjects were operating with anything approaching similar conceptions of those concepts.

There may be a tension between the survey design that would best capture the concepts of privacy and security which an individual respondent possesses, and a survey design which is better suited to using privacy and security as more fixed concepts, but then able to understand the extent to which the importance of those concepts varies alongside other variables.

Is it possible to design a questionnaire design, which works if we are agnostic about how a participant understands security or privacy? Some questions might try to determine what a participant includes in those concepts, and then later questions ask about relationships between security, privacy, convenience, trust etc., but in the analysis can we then relate the two together?

So for example:
People who included financial wellbeing and health in their concept of security were more likely to give up privacy for security than people who excluded those factors

1.12 LINKED SURVEILLANCE PRACTICES

Respondents suggested the need to incorporate hypotheses and questions related to the linking up and coming together of disparate surveillance and security systems and the extent of public awareness or knowledge, and then acceptance of this. We should be careful (in the vignettes for example) to avoid presenting security and surveillance technologies as isolated and unique.

1.13 VIGNETTE DESIGN

There was significant support for the use of vignettes on the part of the interviewed experts, as a way of grounding discussion of privacy and security and identifying the small variables that would change attitudes to surveillance and privacy. Vignettes could also be treated as choice experiments.

There was some concern about H21-23, which relate to vignettes, being at a different level of analysis to others.

It was seen as important not to isolate technologies from the organisations that are making use of them, because trust in the institutions is likely very important. This suggests that the context explored by the vignettes should include the user of the security or surveillance technology.

Vignettes could also be used to ask participants to put themselves in the position of others and see if they believed that would alter their perceptions of privacy and security.

1.13.1 Suitable contexts and technologies for vignettes

Some experts suggested that we avoid typically security-focused technologies and contexts (such as border checks and airports) in the vignettes, instead using more every-day example (buying a book online, smart metering in the home) because the security/privacy discourse is not so dominant in these contexts, and norms have not yet been established.

1.14 ISSUES WITH INDIVIDUAL HYPOTHESES

- Are H25 (Individualistic countries tend to give up privacy more easily) and H55 (Non-individualistic countries care about privacy in traditional terms and care less about individual privacy than individualistic countries) compatible?
- Andrew Charlesworth provided feedback upon almost every hypothesis; see the particular interview for more detail.
- Is higher education acting as a proxy for some other value (e.g. income? Is this legitimate).

1.15 METHODOLOGICAL ISSUES

- Need to use stage of question generation to carefully filter out the bias that can emerge from participants' not understanding terminology in hypotheses.
- Ask for people's behaviours rather than their intentions (what would they do in the context of a vignette.