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 9.1: Findings from qualitative focus groups

Editors:	Gideon Skinner, Daniel Cameron, Will Harrison (Ipsos MORI)
Reviewer:	Michael Friedewald (Fraunhofer ISI)
Dissemination level:	Restricted to a group specified by the consortium
Deliverable type:	Report
Version:	1.0
Due date:	30 June 2013
Submission date:	29 October 2013

About the PRISMS project

The PRISMS project analyses the traditional trade-off model between privacy and security and devise a more evidence-based perspective for reconciling privacy and security, trust and concern. It examines how technologies aimed at enhancing security are subjecting citizens to an increasing amount of surveillance and, in many cases, causing infringements of privacy and fundamental rights. It conducts both a multidisciplinary inquiry into the concepts of privacy and security and their relationships and an EU-wide survey to determine whether people evaluate the introduction of security technologies in terms of a trade-off. As a result, the project determines the factors that affect public assessment of the security and privacy implications of a given security technology. The project uses these results to devise a decision support system providing users (those who deploy and operate security systems) insight into the pros and cons, constraints and limits of specific security investments compared to alternatives taking into account a wider society context.

Terms of use

This document was developed within the PRISMS project (see http://prismsproject.eu), co-funded by the European Commission within the Seventh Framework Programme (FP7), by a consortium, consisting of the following partners:

- Fraunhofer Institute for Systems and Innovation Research (Fraunhofer ISI), co-ordinator,
- Trilateral Research & Consulting LLP,
- Dutch Organization for Applied Scientific Research (TNO),
- Vrije Universiteit Brussel (VUB),
- University of Edinburgh (UEdin),
- Eőtvős Károly Policy Institute (EKINT),
- Hogeschool Zuyd and
- Market & Opinion Research International Limited (Ipsos-MORI)

Document history

Version	Date	Changes
1.0	29 October 2013	

Version 1 | Internal Use Only

PRISMS – WP 9.1

Findings from qualitative focus groups

28th October 2013

Ipsos MORI
Social Research Institute

Methodology

- This qualitative research was designed to inform questionnaire design for the quantitative phase of the PRISMS study
- Discussion groups were carried out in 8 countries: Belgium, Portugal, Denmark, Estonia, Hungary, Romania, Germany, UK
- Participants were recruited to reflect the adult population in each country, with two groups (usually aged under and aged over 40) conducted per country
- Each group was presented with four vignettes (in a different order in each group) and asked questions to reveal their perceptions and values
  - The same eight vignettes were covered in Belgium, Portugal, Estonia, Hungary, Romania, Germany, UK, with at least four being covered in each group
  - In Denmark, three new scenarios where tested in both groups, following discussion of the emerging findings from fieldwork in the other countries
- The discussion guide also explored more general perceptions and attitudes on privacy and security, trust and concern

Key findings

Vignettes tested in Belgium, Portugal, Estonia, Hungary, Romania, Germany, UK

Scenario 1 – Air travel

- Across countries, most felt this situation – while difficult for individuals – was acceptable given the security risks
- The safety of all the passengers was considered more important than the inconvenience to some
- The scenario seemed realistic and in line with their expectations about how these checks would be done
- “Pat down” option not seen as sufficiently secure by most
- Participants suggested a number of alternatives to reduce inconvenience for people with medial conditions:
  - Portugal, Germany, UK: describing medical condition to one or two members of security staff
  - Hungary: security procedure carried out in a separate room
  - Germany: everyone gets scanned occasionally to reduce the risk of a two-class society
  - Belgium: disclose your medical situation in a more private way e.g. on the chip of your identity card, special passes

Wording tested:

Hannah often travels by air for work. She has a colostomy bag, which is detected by most airport body scanners. It sometimes makes her feel uncomfortable having to explain her medical condition to airport security staff when she flies.

Scenario 1 – Air travel – Comparisons by country

Germany	Portugal	Belgium	Estonia	Hungary	Romania	UK
Little acceptance Concerns about nudity and sense of shame this brings Abuses of power in in-proper training of staff are concerns Preference for everyone to be scanned occasionally to reduce risk of two-class society	Passengers with medical conditions should not constantly be made to explain themselves But medical conditions should not exclude people from the same checks Preferable to inform one or two staff about their medical condition	Scenario is very likely and recognisable Acceptable to disclose medical conditions Low empathy towards people in this situation as security is important	Generally felt situation was justified Though some sympathy was felt for Hannah (especially if in a group) felt that no exceptions can be made for people like her	Acceptance and understanding Male respondents: passenger should accept the situation. Female respondents: Airport staff should ensure they are given more privacy	Seen as an acceptable scenario Safety comes first Acceptable to disclose medial conditions, as long as this is the rule and it protects them	Viewed as necessary to ensure security Sympathy for those individuals affected, but no appetite to change the rules If alternatives that are still as secure are possible then these would be welcomed

Scenario 1 – Air travel

"I think it is ok. I want to have a safe flight and reach my destination alive."
Female, under 40, Germany

"People with a medical condition shouldn't be constantly made to explain what's the matter with them"
Female, under 40, Portugal

"If the situation is like this, you have to learn to live with it and there is nothing you can do about it. In terms of security you cannot make an exception for one person that you will close your eyes for a moment."
Male, under 40, Estonia

"They can also put it on the chip of your passport."
Female, over 40, Belgium

"It's hard for her but I don't know what else you can do."
Female, under 40, UK

Scenario 2 – Thumb prints

Wording tested:

Brian is set to enrol in a new system that means he has to use his thumb print to access his unemployment benefits. The government agency that handles the benefits system has explained that they use thumb prints to fight identity fraud and that they will not store his thumb print, just a mathematical representation of it. However, Brian is unsure what this means in practice.

- Balance of opinion supportive but views somewhat polarised
  - Some like the idea as an effective way to fight fraud
  - Others worried about storage, access and other uses
- Seems a plausible scenario, irrespective of acceptability
- Some feel the system would be too complicated or expensive just to access benefits – is it really needed?
- Lack of understanding of ‘mathematical representation’
- Trust in government mixed:
  - Hungary: not convinced data would be safe and government could share with private company
  - Estonia: trust their fingerprints to public sector but not to private companies
  - Portugal: fingerprints have been widely used for many years as a method to identify citizens – so no problem
  - Germany: fingerprints associated with crime and some feel that private companies have stronger firewalls to protect data

Scenario 2 – Thumb prints – Comparisons by country

Germany	Portugal	Belgium	Estonia	Hungary	Romania	UK
Mistrust about how the data will be used – fears of data being abused Need for clarification and transparency Seen as more acceptable for those born outside country / asylum seekers Associations with crime – doesn’t fit with German values	General acceptance as a positive way to reduce crime Believable – already used by companies for checking in/out of work – widely used in Portugal No concerns about storage and use of data by private companies – as long as done in informed and voluntary way	Concept seen as too abstract and unfamiliar No major concerns with government collecting and storing fingerprints – greater mistrust of private companies	Fingerprints already used on biometric passports – inevitable that the technology will be used elsewhere Seen as a reliable system Do not want such systems to expand into the private sphere Trust in government but not private companies	Positive initial reaction – reliable form of identification Feeling that government would do the best job in handling the data, but still not convinced it would be in safe hands No differences seen between private companies or government handling the data	Associations with crime amongst older respondents Younger respondents more accepting – sign of modernity Unfair – would only apply to unemployed Would ultimately accept – Romania seen as an obedient nation	Acceptable if the case can be made that this technology is worth the money – already enough ways of checking ID? Important that government has confidence when paying benefits Few concerns in this context, but would be more if used for other types of public services

Scenario 2 – Thumb prints

"It makes it more difficult for fraud to happen in these areas"
Male, under 40, Portugal

"A too expensive system to make it only for unemployment benefit. It will be definitely used elsewhere as well because there is no sense in making it only for this thing. Then it is inevitably connected to some other spheres of life as well.
Female, under 40, Estonia

"It doesn't matter…our personal data is stored in many places…when you are on-line all your data can be available…"
Male, over 40, Hungary

'I don't find it alright to be asked this much for the unemployment benefits for which I have proofing documents."
Female, over 40, Romania

"I would have more difficulties with a private company, nowadays they pass on all your data."
Male, over 40, Belgium

Scenario 3 – Smart meters

- Wide range of views on this scenario – from enthusiasm to ambivalence to significant concerns
- Potential cost reductions attractive to some (e.g. Germany, UK and Romania) based on the assumption they could choose whether to have one or not
- But personal benefits not always obvious given many have no concerns about current experience – therefore no reason to share this information
- Lack of trust in private companies across all countries – why would they want to collect energy consumption data
  - Estonia, Germany: worries that this information will be used by other companies to target advertisements
  - Belgium: power company knowing when they were not home created a feeling of insecurity
  - Romania: not concerned as they do not perceive this information as confidential – and happy to receive offers

Wording tested:

A power company has decided to offer smart meters to consumers. These enable consumers to use energy more efficiently. Smart meters are installed by engineers from the energy companies and allow consumers to see how much energy they are using in near real-time using an interactive display unit. However, smart meters record more personal data (such as how much electricity is used and when it is used) than conventional meters (which only measure the total amount of electricity used).

Scenario 3 – Smart meters – Comparisons by country

Germany	Portugal	Belgium	Estonia	Hungary	Romania	UK
Positive initial reaction – benefits to individual consumer Suspicions around private companies wanting to make profit from the data Need for reassurance and concerns about expansion, for example targeting advertising for low energy appliances	Ambivalent response – benefit to consumers, but also companies may benefit from the information Majority wiling to try the technology, but main concern is around what companies will gain from the data Need for balance between gains of consumer and companies	Thought this was an unlikely scenario – Belgian law would protect them against the use of this technology Concerns around what data would be used for No perceived benefits Privacy concerns – e.g. knowing when a consumer is not at home	Familiar – two tariff meters already used in Estonia Sceptical about the purpose – will the information just be used for advertising Concerns around security – belief that such systems will never be secure Useful for the provider, but no use for the consumer	General lack of trust in energy companies Information gained by companies would be too much Males would use smart meters, females feel they are unreliable	Highly positive reaction Understand and agree with the principles Main concerns around financial implications, not the meters themselves Accept the idea of power companies using the info to target advertising Accept trade off between privacy and security	Many supportive of the idea as a way to reduce costs and improve energy efficiency But some instinctively opposed to a private company knowing this information Benefits for consumers not obvious – already feel in control of their energy use

Scenario 3 – Smart meters

"If it saves me money then I'm all for it."
Male, over 40, UK

"I am just wondering why they do this. Do they want to send me adverts when they see that I am using an old fridge?"
Female under 40, Germany

"It is a good way to control yourself when it comes to using energy and saving money is always nice."
Male, under 40, Germany

"If I want to understand my personal consumption, I can always check my meter myself! "
Male, over 40, Belgium

"We will be definitely told how great and good this will be for us as consumers but no one will start to tell you about all this that what kind of conclusions can be made from this."
Female, under 40, Estonia

Scenario 4 – Internet monitoring (terrorism)

Wording tested:

Hassim is a student who is very interested in understanding why some fellow Muslims become terrorists. He often researches terrorism on the internet and frequently discusses it on online forums. Hassim's parents have recently read about security agencies which monitor webpages related to terrorism in order to detect potential terrorist threats. They ask their son to stop doing internet research about terrorism.

- This scenario generated good discussions in all countries and reminded some participants of the recent stories about internet monitoring in the US
- For almost all, this type of monitoring was considered acceptable or desirable – participants assumed their governments would be doing so to deal with terrorism
- Participants could see all three perspectives:
  - **Parental concern is legitimate** – some said they would do the same in similar circumstances
  - **Monitoring this type of behaviour is legitimate** – provided it is done by government in a controlled way
  - **Researching terrorism is legitimate** – although this divided opinion – those who are genuinely interested in researching this topic must do so in a transparent way and be willing to answer to government if questions are asked
- By contrast, this type of monitoring was deemed completely unacceptable in Germany – Hassim not considered a legitimate target

Scenario 4 – Internet monitoring – Comparisons by country

Germany	Portugal	Belgium	Estonia	Hungary	Romania	UK
No acceptance Highly provocative Seen as very unfair and intrusive – huge impact on privacy and does not reflect German values Undermines presumed innocence as a basic value in the German legal system	Seen as very believable Agree with request by parents to stop Ambivalent opinion – protects from terrorism but invades privacy Legitimate to monitor – not because individual is Muslim, but because of viewing sites linked to terrorism	Very likely scenario Support if done by the government Uncomfortable with giving up privacy, but accept doing so for security Hassim seen as a legitimate target	Little knowledge about the Muslim faith apart from negative stereotypes Felt Hassim had a unhealthy curiosity – needs to be cautious Parents are right to intervene See internet monitoring as inevitable	Hard to comprehend concept – religious extremism not something that affects them Hassim considered a legitimate target for monitoring Internet seen to be subject of constant monitoring anyway Agree with behaviour of parents	Find the idea acceptable But considered unlikely to happen in Romania Acceptable for Hassim to be monitored – safety more important	Assumed people like Hassim would be monitored Agreed that he should have the right to visit these websites for academic study, but also that he should expect to explain Empathised with parents – some said they would act in a similar way with their child

Scenario 4 – Internet monitoring (terrorism)

“He’s absolutely entitled to do this kind of research but he should expect to have to answer questions if he does.”
Female, over 40, UK

“This is far away from our constitution. It does not reflect German values at all.”
Male, under 40, Germany

“Maybe monitoring disturbs me, but I know that it is for my safety!”
Female, over 40, Hungary

“This is discriminating. This is an abuse of small people for political reasons. Poor Hassim.”
Female, under 40, Germany

“It’s sad that it has come this far.”
Male, over 40, Belgium

“I agree with the parents… I would do the same thing.”
Male , over 40, Portugal

Scenario 5 – Music sharing

- In general, participants saw this type of activity as a minor crime – many had shared files like this themselves
- Even so, most had no problem with action being taken to tackle copyright infringements
- However, monitoring being carried out by internet service providers – rather than through legal channels – was a concern for most participants
  - ISPs were not trusted to do this – should only be government (i.e. police) that have powers to monitor usage and take action
  - Internet access is seen as too important to be left in the control of private companies
  - Only exceptions was Hungary where there were fewer concerns about ISPs taking action
- There was also confusion about what their individual rights would be in this situation – e.g. if they were members of the website but had not been involved in illegal sharing

Wording tested:

James shares home-made music files with his friends on a small file sharing website. However, some friends have recently begun to upload content that may infringe on copyright restrictions. Their internet service providers have been monitoring their activities for months and are about to cut off their internet service to all the website members following previous written warnings.

Scenario 5 – Music sharing – Comparisons by country

Germany	Portugal	Belgium	Estonia	Hungary	Romania	UK
Familiar scenario Prefer law enforcement agencies to take the lead, rather than the ISP Mistrust towards surveillance technologies Unjust to close site to all users Uncertainty if ISP have legal authority to close the site	Very familiar scenario Downplay of importance of this type of activity More appropriate if done by official law enforcement agency Invasion of privacy is carried out by private company	Sceptical views towards ISP Unlikely scenario for Belgium Not the ISPs' job to monitor web pages Difficult balance – not a major crime, resources should be focused on serious crimes	Sympathy for James Copyrights seen as meaningless so not a major crime Users should be fined rather than having service cut off Sanctions should only apply to those who upload files, not download them	Realistic – believe ISPs have contractual obligation to carry out such monitoring General acceptance – do not feel it will catch major criminals Unfair to target average consumers No major concerns about ISPs monitoring usage	Welcome the activity – would lead to reductions in copyright infringements Should be carried out by a authorised entity Serious concerns about ISPs monitoring and using the data – police would be in much better position to do this	Considered a fairly low-level offence But accepted that action is legitimate Confusion about how ISPs would know Concerns about the implications (i.e. losing internet connection) if someone is not aware their friends are sharing files illegally

Scenario 5 – Music sharing

"We cannot do anything against it…we are monitored by everywhere, even in the street."
Female, under 40, Hungary

"How can they cut the internet service for all members? He did not do anything wrong. That's not possible."
Female, over 40, Germany

"Something like that should only be possible with a court order."
Male, under 40, Belgium

"In the same way [the ISP] has no authority to monitor, it also does not have authority to suspend the service."
Female, over 40, Portugal

Scenario 6 – ANPR

- Improving road safety seen as an important priority across countries – a tangible benefit that saves lives
- Not considered likely in some countries (e.g. Hungary, Romania) because of existing infrastructure
- Many support the idea because those who do not violate traffic rules “would have nothing to fear”
  - More divided views in Germany and Belgium: perceived as a trade off between giving up privacy and increasing safety
- Some concerns about how exactly the system would work:
  - Quality of image: contrasting views between those who would only want it to identify the vehicle (e.g. Belgium) and those who would want certainty by using HD images (e.g. Hungary)
  - Access to data: who will be able to use the data?
  - Storage of data: how long will it be held for?
- Differing views on whether the police or local government should implement the system – based on levels of trust

Wording tested:

A local council is considering expanding the use of Automatic Number Plate Recognition (ANPR) systems that automatically identify speeding vehicles by their number plate. Future systems would also detect other road safety violations such as passengers not wearing seatbelts, cars carrying dangerously large items, or drivers using mobile phones.

Scenario 6 – ANPRs– Comparisons by country

Germany	Portugal	Belgium	Estonia	Hungary	Romania	UK
Recognition of the benefits e.g. for personal security Picked up on the negatives, e.g. infringements on privacy, data not being protected, security of data Permanent control and lack of transparency mentioned as big concerns	Regarded as favourable – will make drivers more compliant with road safety Would act as a deterrent Most accept the situation providing it is managed by official authorities	High ‘big brother is watching you’ initial reaction Likely scenario – cameras used all the time anyway, for example in shopping centres Division in opinion between acceptable to improve road safety to how far it will go and violations of privacy	Already the reality on national roads Unlikely at the local government level – don’t have the funds for this Majority agree that it’s a good idea Not regarded as a breach of privacy	Positive initial reaction – cite high number of road accidents Do not think the system would work from a functional point of view No objection to the principle itself, greater concerns around the reliability of the current system	Welcome the idea if it makes roads safer Unlikely to happen due to high costs Supported – acceptable to reduce privacy in order to increase safety No concerns about the system – need to consult with residents beforehand No mentions of privacy concerns	Strong support for anything that reduces road deaths Those who obey the rule should have no problems Some concerns about other uses of the data, and how exactly it would work in practice

Scenario 6 – ANPR

“How does that system work? Will they permanently watch us via this system? That would be crossing frontiers!”
Male, over 40, Germany

“I don’t know what the problem is – if you follow the rules there’s nothing to worry about. If not you deserve to be caught.”
Female, under 40, UK

“I favour the use of video surveillance in the cities because of safety concerns.”
Female, over 40, Portugal

“I think it’s scary that they know when and where we go, but I can understand.”
Female, under 40, Belgium

Scenario 7 – Internet monitoring (health)

Wording tested:

Last winter Lauren received a letter from her doctor in which they recommended she had a flu vaccination. This letter was sent because government monitoring of internet searches and communication suggested that a certain type of aggressive flu pandemic was very likely to occur.

- Many participants were concerned about the government monitoring general internet searches
- This seemed to be a result of confusion about what exactly the monitoring would involve:
  - Is this a serious enough issue to justify monitoring?
  - Is the information about searches reliable?
  - Is this more effective than doctors deciding who needs a vaccine?
  - How would doctors be told who to write to?
  - Is this just marketing for a pharmaceutical company?
- Confusion partly linked to the phrase “government monitoring of internet searches” and how it was translated
  - Rather than using aggregate, anonymised data, participants assumed this meant government monitoring their searches
  - Some expected that this kind of thing already happened, but still opposed it (e.g. Romania)

Scenario 7 – Internet monitoring – Comparisons by country

Germany	Portugal	Belgium	Estonia	Hungary	Romania	UK
Total no-go scenario Seen as very strong infringement of privacy Undermines German constitution Fear of abuse of data - sale to 3rd parties	Raises issues about reliability of information on websites and how easily this can be manipulated No objection to government monitoring if in the interest of national security Privacy of secondary importance to national security	Would make government very patronising Very unlikely and questions about the credibility of the information Opposition - violation of privacy	Welcome the idea if it can help predict things in advance Lack of resources to implement the system in Estonia Letter sent by family doctor, seen as more acceptable - opposite if sent by pharmaceutical company	Seen as realistic - not surprising as felt all internet use was monitored anyway Clearly and unanimously opposed to the government monitoring the internet Not seen as an efficient system	Expensive, not plausible, not important Likely scenario - already a myth of government following citizens online Concern was related to the information being used as a marketing tool Trust in the government with monitoring, but still not seen as necessary	Caused confusion – how would the government know this information? Some cautious support on discussing the idea in more detail but lack of trust use would be limited Assume there are other ways of predicting the need for health interventions

Scenario 7 – Internet monitoring (health)

"It must be good as a tool, but looking at it from our side, well, it's in most of the cases disturbing… Would my searches also mean that I automatically agree that these searches are being monitored?"
Female, under 40, Hungary

"What does that mean? How does that work? Usually physicians give general feedback and this is how they gain the information."
Female, over 40, Germany

"This may be a lobby for pharmaceutical industry to make money."
Male, under 40, Portugal

Scenario 8 – Religion ID cards

- Viewed as completely unacceptable in almost all countries
  - Less concern in the UK because government trusted on this topic, but some worries about the potential for misuse in future
- Most thought it could not happen in their country, and would strongly oppose the introduction of this kind of measure
  - And use of Jewish name heightens concerns
- A number of objections raised by participants:
  - Religion is a private matter and no one should feel obliged to share this with government
  - Religion can change over time
  - Linking this to other data on an ID card particularly worrying
  - No way of storing data is completely secure, so there are always risks even if the government is trusted generally
  - The information could be misused by radical organisations – now or in the future
  - There are no obvious benefits – alternative ways to consult religious groups are available

Wording tested:

Chaim received a request from the government to register his religious background on his identity card so that they can involve citizens from a variety of religions in local decisions about schools and the construction of religious buildings. The government promises to ensure that this data will only be accessed by them in order to assess his religion and will never be stored in other databases or transferred.

Scenario 8 – Religion ID cards – Comparisons by country

Germany	Portugal	Belgium	Estonia	Hungary	Romania	UK
Immediate reluctance – no acceptance at all Religion is a private decision and is not relevant for the state Fear data will be forwarded to the police	Very sensitive topic. Firmly opposed Could be root to prejudice and discrimination Local factor raises concerns even more – raises likelihood of segregation Government holding the data does not provide any reassurance	Completely unacceptable Feel public opinion would be strong and revolt against this Lack of trust in government to store data	Unlikely to happen in Estonia Laws state the religious affiliation is sensitive	Unanimous rejection of this in principle Not seen to be feasible or acceptable	Revolted with such a measure Not perceived as relevant – no perceived benefits Unlikely to happen in Romania	Some concern but not strong rejection – assuming it is voluntary A few could see potential benefits for public service delivery Government trusted to hold religious data, but some worries about the potential for misuse in future

Scenario 8 – Religion ID cards

"This goes too far. I can say I'm Islamic while I'm not. How will they control this?"
Female, under 40, Belgium

"If there is a database there is always someone who can access it."
Male, under 40, Portugal

"The problem is that the government pays small salary to IT managers in its sector…so the less experienced and talented experts work there"
Male, under 40, Hungary

"We already had that 70 years ago. Especially we need to be careful with that."
Female, over 40, Germany

Recommendations for scenarios

Scenario	Comprehension?	Suitable for survey?
1. Air travel	▪ Explain "colostomy bag"	Yes
2. Thumb prints	▪ Unfamiliar technology ▪ Some calls for further details – e.g. explaining "mathematical representation"	Yes
3. Smart meters	▪ No issues	Yes
4. Internet (terrorism)	▪ No issues	Yes
5. Music sharing	▪ Some confusion about how the ISP would be able to monitor usage	Yes
6. ANPR	▪ No issues	Yes
7. Internet (health)	▪ Causes confusion – not clear enough how monitoring would work	Not in current form
8. Religion ID cards	▪ Use of Jewish name heightens concerns	Possibly – provokes strong reactions

Key findings

Vignettes tested in Denmark

Scenario 9 – Internet advertising

- Many believe search engines, commercial websites and social media are already doing this
  - For the purpose of personalized advertising (Facebook is a frequently mentioned example)
  - Although not aware of ISPs directly monitoring internet behaviour
- Receiving personalized advertising was positively perceived by some
- As advertising is already there and impossible to avoid, it is better to look at something of interest.
- The two different versions of the scenario did not prompt different reactions
- Raised the least controversy of any of the scenarios tested in Denmark

Wording tested:

Version 1: Your internet service provider wants to sell information about your internet use to advertisers so they can use it to create offers, deals and advertising targeted at you. This would include the searches you conduct and the websites you visit. Your provider's terms and conditions say the information they sell will be anonymous.

Version 2: An internet service provider wants to sell information about their customer's' internet use to advertisers, so they can use it to create better advertising targeted at these customers. The provider's terms and conditions say this information will be anonymous.

Scenario 10 – DNA samples

- This scenario provoked mixed reactions
  - DNA was acknowledged as being useful in solving and preventing crimes
  - But personal nature of DNA meant participants were uncomfortable with the impact on their privacy of the data being shared
- Consent for DNA to potentially be shared with the police was seen as crucial
- Selling this information for profit was considered unethical and unacceptable – and this extended to other health and biological information
- They had some reservations over what would happen to their information in the future, and were also cautious about how legislation might change

Wording tested:

Version 1: John voluntarily provided a sample of his DNA to a company that carries out medical research. He then learns that the research company has been asked to share their DNA samples with the police for use in criminal investigations. John has not committed a crime, but still feels unsure about the police accessing his DNA. DNA samples can be used to understand potential health problems but also to identify people and to make inferences about who they are related to.

Version 2: John voluntarily provided a sample of his DNA to a company that carries out medical research. He then learns that the research company has offered to sell their DNA samples to the police for use in investigating crime and terrorism. John has not committed a crime, but still feels unsure about the police accessing his DNA. DNA samples can be used to understand potential health problems but also to identify people and to make inferences about who they are related to.

Scenario 11 – Crowd monitoring

- Monitoring crowds by means of police (in both uniform and plain clothes), helicopters, and drones considered largely uncontroversial
- More mixed views on tapping phones
  - Most agreed that reasonable suspicion was necessary in order to justify telephone tapping
- There is a difference between participating in a demonstration and a football game
  - Exercising democratic rights vs. entertainment
  - There is a greater concern about the risk of being wrongfully monitored or arrested based on a misunderstanding at a demonstration
  - Monitoring a football match is considered more appropriate and even necessary – violence often occurs and it should be easier to identify trouble makers

Wording tested:

Version 1: Marc is an active member of an environmental group that is campaigning to block the construction of a new road. The group organises a demonstration near the national parliament. The police monitor the crowd at the demonstration in various ways: by using uniform police and plain clothes police, by using helicopters and drones, and by tapping phones. By linking the information they collect to details about individuals on their social media profiles, the police hope to track and identify suspicious persons, to collect information on potential activists willing to cross the line between peaceful and violent activism and to have an additional way of controlling the crowd.

Version 2: Claire is a football fan who regularly attends home matches when his national team play. The police monitor the crowd at these matches in various ways by using uniform police and plain clothes police, by using helicopters and drones, and by tapping phones. By linking the information they collect to details about individuals on their social media profiles, the police hope to track and identify individuals who cause trouble before, during or after matches.

Overall views in Denmark

"I worry about my bank account details. If your internet traffic is being tracked, so are your bank account details."

Man, under 40, Denmark

"Violence at football matches for me is a security issue. You get the wrong people in the wrong groupings. That happens at demonstrations as well. "

Male, under 40, Denmark

"I don't want to be monitored at home, they can do that all they want in other places, but not at home."

Female, under 40, Denmark

"For me, the greatest threat is Google being able to piece together my profile – I don't feel safe knowing that they have so much information."

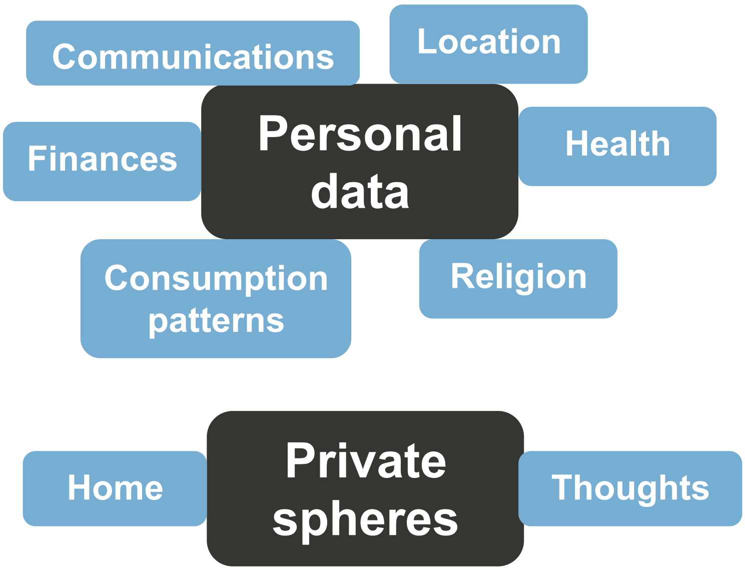
Male, over 40, Denmark

Key findings

Privacy and security discussions

Privacy

- Privacy considered important in the abstract
- ‘Personal data’ the usual starting point with lots of examples discussed
  - Online privacy certainly important but not the only consideration
- Some also prioritised protecting private spheres
- But privacy of movement in public not considered as important
  - For many this seemed unrealistic given level of surveillance
  - And unimportant if nothing to hide
- Reflected a broader assumption that privacy is difficult to maintain if you want to be part of modern society



> *“I think privacy in public spaces is not possible anymore. There are cameras everywhere.”*
> **Male, over 40, Germany**

Types of privacy – terminology generally clear

Difficult to achieve

1. The right to protect a person’s data from other individuals and organisations; giving people control over that data and its use
2. The right to keep body functions and body characteristics (such as genetic codes and biometrics) private
3. The right to privacy in public and private spaces, including regarding sensitive issues such as sexual preferences and habits, political activities and religious practices
4. The right to keep people’s communications private from, for example, telephone tapping interception or access to e-mail messages
5. The right to move about in public spaces without being identified, tracked or monitored
6. The right to think whatever people like and not have to share those thoughts or feelings with others
7. People’s right to associate or meet with whoever they wish, without being monitored

Not realistic

Practical meaning?

Not realistic

🟩 Most important

🟧 Important but difficult

🟥 Less important

Responsibility for privacy

- In most countries, primary responsibility for protecting privacy thought to lie with individuals
- But also see a strong role for the state in developing the correct framework and policing and enforcing standards
  - Different levels of trust in government to do this effectively
- Organisations that hold data also responsible for doing so securely
  - Applies to both the public and private sectors

> *"You can control a lot of these things yourself. You can consciously say: 'I'm not throwing my life on facebook or internet.'"*
>
> **Male, under 40, Belgium**

> *"If I have issued some information or I have a device which issues some information, then this person from whom I have received some service is definitely also responsible. Regardless whether this is the state or not."*
>
> **Male, under 40, Estonia**

Types of security

- Security again considered important in the abstract
- Physical and financial security considered vital
- Spontaneous discussions did not generate all the different categories
  - Internet access a separate category?
- Other types considered important but feel less immediate – perhaps because the currently feel secure in these areas
  - Cultural security
  - Political security
- Some things seen as outside anyone's immediate control
  - Natural resources
  - Sudden emergencies

1. The right to physical security, for example protection from burglary
2. The protection of political rights
3. Security of future income
4. The protection of values and morals of cultural importance
5. Protection of, ensured access to and safe use of natural resources
6. Protection from sudden emergencies such as pandemics
7. Safe access to the internet

🟩 **Most immediate**

🟧 **Hard to control**

🟥 **Less immediate**

Responsibility for security

- Some aspects are the responsibility of individuals
  - Reasonable steps to protect themselves and their property
- But overall balance of responsibility more towards government authorities for security
  - Police
  - Counter-terrorism
  - Military
- This is an issue for some as they do not trust the police to protect them
- Broader understanding of security means a role for others (e.g. NGOs)

"Their measures often have the reverse effect: they do it for security, but no one feels secure anymore."
Female, under 40, Belgium

"I have written very many reports during my life that this or that has been stolen from me. I always get an answer from there that the matter has expired, there is no public interest and so forth."
Male, under 40, Estonia

" We rely on government – the police and the army and so on – for our security, ultimately. There are things you can do but we need outside help."
Male, over 40. UK

Key findings

Surveillance technologies

Surveillance technologies – Portugal snapshot

- Participants are willing to accept that the increase in sophistication and equipment development will translate into more accurate and effective surveillance practices
- The use of camera surveillance in public spaces is considered a desirable practice and as one that is already widely discussed by the population
- The use of techniques to monitor internet traffic is a practice admitted under certain circumstances – assuming the reasons are clear
- The use of devices that collect information such as smart meters points to an area that is new and surprising for some participants (especially those over 40)
  - For the first time, people are being asked to willingly share a certain type/level of information from a private place (his/her home) in exchange for specific benefits
- The use of biometric technologies or body scanners is considered desirable but must be used in very specific situations. Participants don't have much contact with these technologies, but they recognize that they are very useful in the context of the situations described. The extent to which they are used in Portugal is not known.

Surveillance technologies – Romania snapshot

- The amount of technologies used nowadays seems right
  - Less would not make them feel secure while more would make them feel restrained
- For them security comes first and, as long as the surveillance brings them the wanted feeling of being secure, they are open to more technology in future
- The older age group are even glad the surveillance practices nowadays seem to be lighter than the ones experienced during Communism
- For the younger target, the surveillance technologies are perceived as a sign of modernity and civilization, thus acceptable, as long as they have a good purpose, the security of people

Surveillance technologies – Belgium snapshot

There were differences between the two age groups:

- The group over 40 believed that the current level of surveillance technologies was fine
  - They did not seem to give it much thought and were willing to give up their privacy with the aim of increasing security
  - Only at home they opposed to the surveillance technologies, more specifically surveillance cameras: at home you must have some privacy
- The group under 40 would like to have less surveillance technologies
  - They get the feeling of not having a free choice when it comes to surveillance and this was essential for this group
  - They are not willing to give up more privacy in order to increase security, as they have always lived in a world that is more secure
- All participants agreed that they should first be informed about the surveillance technologies before they are used

Surveillance technologies – Hungary snapshot

- The level of trust in decision makers is low, and the need for a ombudsman or supervising organisation to implement surveillance technologies was mentioned
- Participants had no clear idea about who could make decisions about surveillance practices being introduced in the name of security
- The use of surveillance cameras seen as reliable and acceptable, and the use of biometric technologies also considered a safe way of identifying individuals (even though people are relatively unfamiliar with this technology)
- Internet monitoring view as inherent to internet usage, and could have positive implications with regard to security (for example monitoring terrorists)
  - Though concerns were raised about who would be able to get hold of their data, and what it would be used for

Surveillance technologies – Estonia snapshot

- General lack of trust in the government and low expectations – the state is considered to be quite weak, with resources for the police and security forces scarce
- Most types of surveillance technologies considered to be necessary, with over 40s more likely accept the types of technologies discussed
- Traffic cameras were seen to be efficient, while internet monitoring was seen as likely to happen frequently, both by public authorities, as well as by private companies (e.g. to analyse consumer behaviour)
- Potential security risks with smart devices were identified, while limitations with surveillance cameras were discussed in that footage is difficult to retrieve, for example when needed in legal cases
- Participants argued that less privacy leads to greater security and visa versa
  - In their view, the more urbanised a society is, the less privacy and security

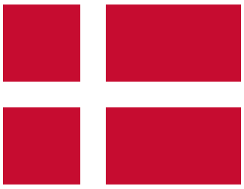
Surveillance technologies – Germany snapshot

- German constitution and presumed innocence seen as basic values in the legal system – has a strong influence on views towards privacy
- German state seen to be reliable and delivering security – mistrust is greater towards private companies who handle personal data
- Internet surveillance technologies seen as the greatest threat to privacy
  - No personal benefit seen that justifies a reduction of privacy rights
  - Likely to be subject to abuse and out of individual's control
- Surveillance cameras and ANPR increase physical security, and seen as more acceptable
  - Transparency important, whether run by the state or private companies
- Devices that offer monetary benefits(e.g. smart meters) considered more acceptable
- Given mistrust about how data will be handled and used, they would welcome an official body to controls and guide surveillance technologies

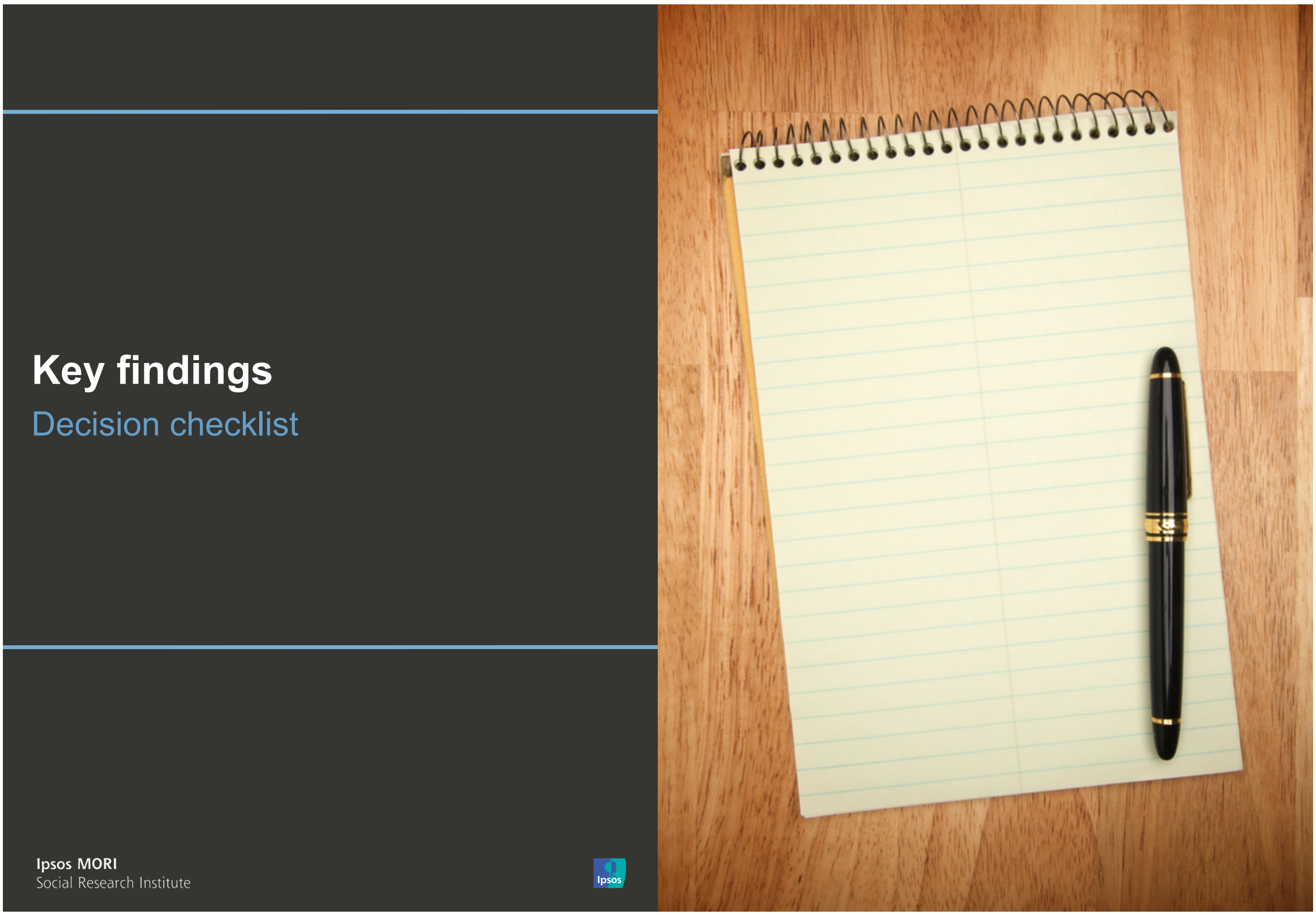
Surveillance technologies – UK snapshot

- Research conducted in a relatively affluent, semi-rural area of England where participants said they felt secure
  - Emphasis on maintaining this security
  - Little experience of any downsides of surveillance technology
- Reasonable trust in the state to deliver given high levels of perceived security – and considerable security worries about the country generally
- Therefore appetite for greater surveillance in future, provided this helps further increase feelings of security
- All technologies discussed considered potentially useful, as long as they are implemented appropriately
- Few concerns about impact on privacy – not something most had given any thought to in their own lives
  - Acceptance that surveillance is an inevitable part of life, both on the internet and as soon as individuals go out of their homes

Surveillance technologies – Denmark snapshot



- Most were not worried about the current level of surveillance
  - Relatively open to increasing the level of surveillance in public spaces
  - In particular, camera surveillance was positively perceived as this adds to a sense of security in public spaces
- Respondents were more cautious about surveillance of their “identity”, e.g. bank account details, CPR (civil registration number), and DNA
  - In the case of DNA, perceptions depend on the purpose – using DNA in a criminal investigation is (more) acceptable than for more trivial matters
  - There needs to be a balance between suspicion and prevention of crime – the ‘less’ serious the crime, the stronger (and more accurate) the suspicion needs to be
- State, police, and local authorities are considered more trustworthy than private companies and other third parties when it comes to surveillance



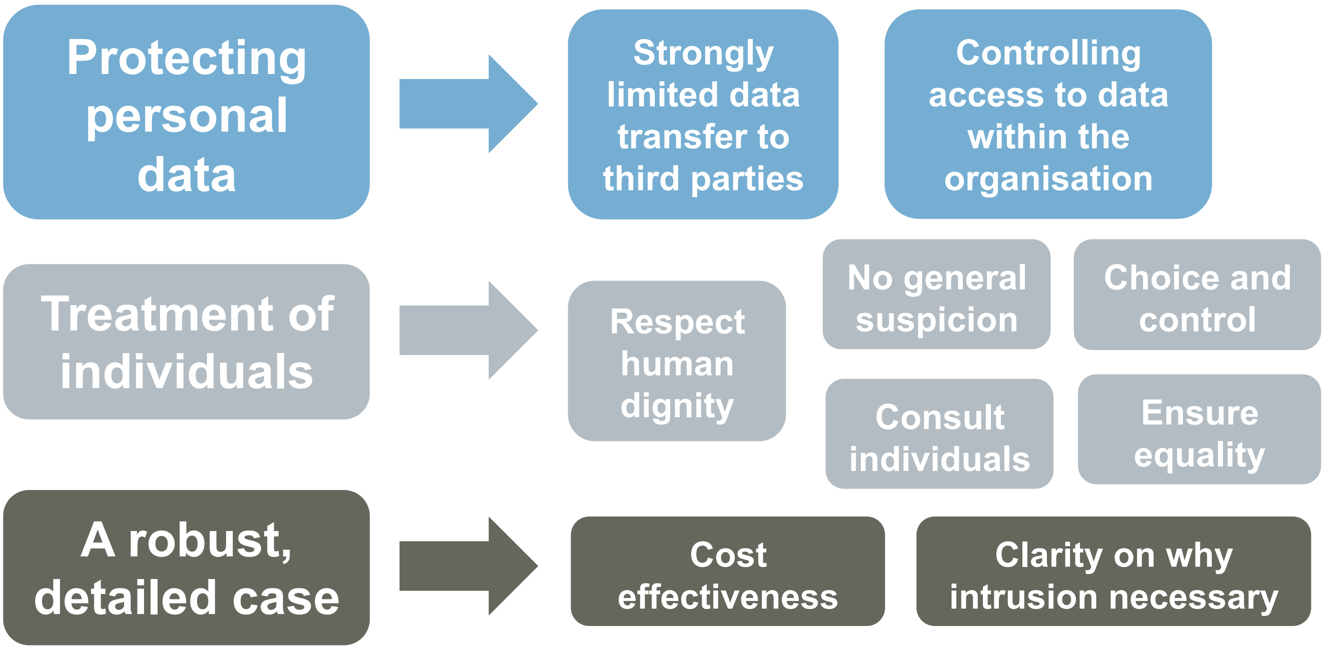
Key findings

Decision checklist

Ipsos MORI
Social Research Institute

Suggestions for surveillance technology checklist

- Participants struggled to come up with ideas for a surveillance technology checklist because they lacked familiarity – but some consistent themes emerged:



Protecting personal data → Strongly limited data transfer to third parties; Controlling access to data within the organisation

Treatment of individuals → Respect human dignity; No general suspicion; Choice and control; Consult individuals; Ensure equality

A robust, detailed case → Cost effectiveness; Clarity on why intrusion necessary

gideon.skinner@ipsos.com

daniel.cameron@ipsos.com

will.harrison@ipsos.com

Ipsos MORI
Social Research Institute

Co-ordinator:
Dr. Michael Friedewald
Fraunhofer Institute for Systems and Innovation Research ISI
Breslauer Straße 48 | 76139 Karlsruhe | Germany
Phone: +49 721 6809-146 | Fax +49 721 6809-315
michael.friedewald@isi.fraunhofer.de

Fraunhofer
ISI