"Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe"

Project acronym: **SurPRISE**

Collaborative Project

Grant Agreement No.: 285492

FP7 Call Topic: SEC-2011.6.5-2: The Relationship Between Human Privacy And Security

Start of project: February 2012

Duration: 36 Months

Final publishable summary report

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

This document was developed by the SurPRISE project (http://www.surprise-project.eu), co-funded within the Seventh Framework Program (FP7). SurPRISE re-examines the relationship between security and privacy. SurPRISE will provide new insights into the relation between surveillance, privacy and security, taking into account the European citizens' perspective as a central element. It will also explore options for less privacy infringing security technologies and for non-surveillance oriented security solutions, aiming at better informed debates of security policies.

The SurPRISE project is conducted by a consortium consisting of the following partners:

Institut für Technikfolgen-Abschätzung / Österreichische Akademie der Wissenschaften Coordinator, Austria	ITA/OEAW
Agencia de Protección de Datos de la Comunidad de Madrid*, Spain	APDCM
Instituto de Politicas y Bienes Publicos/ Agencia Estatal Consejo Superior de Investigaciones Científicas, Spain	CSIC
Teknologirådet - The Danish Board of Technology Foundation, Denmark	DBT
European University Institute, Italy	EUI
Verein für Rechts-und Kriminalsoziologie, Austria	IRKS
Median Opinion and Market Research Limited Company, Hungary	Median
Teknologirådet - The Norwegian Board of Technology, Norway	NBT
The Open University, United Kingdom	OU
TA-SWISS / Akademien der Wissenschaften Schweiz, Switzerland	TA-SWISS
Unabhängiges Landeszentrum für Datenschutz, Germany	ULD

*APDCM, the Agencia de Protección de Datos de la Comunidad de Madrid (Data Protection Agency of the Community of Madrid) participated as consortium partner in the SurPRISE project till 31st of December 2012. As a consequence of austerity policies in Spain APDCM was terminated at the end of 2012.

Table of Contents

Executive Summary

The EU FP7 Security Research project SurPRISE was launched to re-examine the relationship between security and privacy. This relation is commonly positioned as a 'trade-off', and accordingly infringements of privacy are sometimes seen as acceptable or even required costs of enhanced security. This common understanding of the security-privacy relationship has informed and influenced security policies and measures across the EU. However, an emergent body of scientific work and public scepticism question the validity of the security-privacy trade-off. In response to these developments, SurPRISE investigates the relation between surveillance, privacy and security from a scientific as well as citizen's perspective. A major aim of SurPRISE was to contribute with its results to the shaping of security technologies and measures as effective, non-privacy-infringing and socially legitimate security devices in line with human rights and European values.

SurPRISE contributed to this objective in a number of ways. Main results of the research conducted are:

- The comparison of the most important security challenges, as perceived by citizens and by experts, with security policies on the European and national level shows a considerable mismatch; where's concerns are mainly of economic and social nature, policies are focused on fighting crime and terrorism by surveillance technologies.
- The development and empirical testing of a model of criteria and factors influencing acceptability of surveillance oriented security technologies (SOSTs) showed that the trade-off approach is by far oversimplifying the existing complex relationships. This approach is therefore not suitable to inform policy-making.
- The scanning of technical possibilities to make SOSTs less privacy infringing, of available legal measures to regulate and limit the implementation and use of SOSTs, and of security measures not based on surveillance technologies revealed a range of less privacy infringing or alternative approaches.
- As preparation of the participatory events, involving about 2000 citizens in nine European countries in large-scale citizen summits and in smaller scale citizen meetings, information brochures on the privacy-security topic in general and on specific surveillance technologies were produced in eight languages; movie clips on smart CCTV, Deep Packet Inspection and smartphone location tracking are also available in eight languages.
- The citizen summits, full day events with alternating phases of providing information, debates among citizens in the small groups, and anonymous electronic voting provided extremely valuable qualitative and quantitative data on the topic:
  - new insights on the evaluation of SOSTs by citizens and the reasoning for acceptance or rejection of specific measures and technologies
  - a set of policy recommendations, reflecting the recommendations provided by the citizens at the participatory events
  - information and practical experiences used for the development of a decision support system (DSS) for the involvement of citizens in future security related decision-making in form of small-scale citizen meetings.
- The development of a web tool supporting the workflow of citizen meetings which was successful tested in five countries, providing in-depth information on additional aspects and on two more SOSTs (drones and biometrics).

The organisation of a two days joint international conference organised by the SurPRISE, PRISMS and PACT project is a highlight of the dissemination activities.

1 Project context and objectives

The years since the turn of the millennium have been characterised by dramatic changes in both, the objectives and the means of security policies. The proclaimed war on terror after 9/11 2001 is a clear landmark of this development, although it denotes rather an acceleration of longer-term tendencies than a real turning point. These tendencies comprise political and societal developments of securitisation as well as technical progress in information technologies, creating unprecedented possibilities of data collection and surveillance. The attacks from 9/11 and subsequent acts of terrorism were exploited to make actual use of the surveillance capabilities offered by technology, obviously to a literally unlimited extent as the revelations made by Snowden on global surveillance programs conducted by the NSA showed.

In this context, a core objective of SurPRISE was to re-examine the relationship between security and privacy. This relation is commonly positioned as a 'trade-off', and accordingly infringements of privacy are regarded as an acceptable or necessary cost of enhanced security. This common understanding of the security-privacy relationship, both at state and citizen level, has informed and influenced policymakers, legislative developments and best practice guidelines concerning security developments across the EU, and led to the growing focus on pre-emption and proactive measures, resulting in ever more increasing focus on improving surveillance capabilities.

However, an emergent body of scientific work and public scepticism question the validity of the security-privacy trade-off. In response to these developments, SurPRISE investigated the relation between surveillance, privacy and security from a scientific as well as citizen's perspective. Major aims of SurPRISE were to identify criteria and factors, which contribute to the shaping of security technologies and measures as acceptable, effective, non-privacy-infringing and socially legitimate security devices in line with human rights and European values, and to develop policy recommendations based on recommendations provided by about 2000 citizens from nine European countries. The involvement of citizens constituted an essential element of the identification of criteria and factors and of the formulation of policy recommendations. Two types of participatory events were organised and conducted by SurPRISE, large-scale "Citizen Summits" and small-scale "Citizen Meetings". Citizen Summits involved on average about 200 citizens per country; Citizen Summits were full day events, with alternating phases of receiving information, discussing the topics and emerging issues in small groups, electronic voting and formulating recommendations to policymakers. Citizen Meetings allow the involvement of citizens in decision-making in small-scale participatory events. Citizen Meetings are a decision support system developed by SurPRISE. This method of participatory involvement was tested in five countries with about 200 participants; the results were integrated into the analytical work and the development of policy recommendations.

SurPRISE fulfilled nine main objectives:

1. Map key security challenges and related security policies and technologies. Focusing on SOSTs with an identifiable impact on privacy and other ethical and legal values of European citizens, security challenges and related responses were identified.

2. Identify factors influencing acceptability and acceptance of these security technologies. An extensive literature review was undertaken to understand the emergence of, and then to deconstruct, a privacy-security trade off. Viable alternatives influencing the acceptability and acceptance of security solutions, which emerged from this detailed reading, were identified for testing.

3. Develop models and hypothesis about relations between these factors, beyond the simplified trade-off model between privacy and security. Using a detailed reading of material produced in earlier objectives, the nature and direction of relationships between new factors which influence citizens' acceptance and acceptability of security solutions were hypothesized, and a questionnaire purporting to investigate these relationships was designed and validated.

4. Identify technical design and legal/regulatory options and non-technical alternatives. Through an extensive literature review of the relevant legal and technical fields, state of the art reports examined

whether legally backed security interventions necessarily result in technological developments, implying intensive surveillance and privacy infringements. Available alternatives were identified and elaborated.

5. Elaborate information material for selected cases for empirical testing. A limited number of security challenges and solutions identified under objective 1 were explored and translated into information material, including short films, which communicated the challenges and the available alternatives to a citizens' audience.

6. Perform a large scale participatory empirical testing of models. On average about 200 citizens participated in Citizen Summit Events in each of nine European countries to discuss and provide their views. They answered questionnaires, comprising a broad range of factors, examining and explaining the acceptability and acceptance of surveillance technologies beyond the security-privacy trade off. The arguments raised by citizens in the deliberative discussion were integrated in the analysis.

7. Synthesize empirical findings with theoretical models and practical options to shape security policies. Data were analysed into a series of country reports and a synthesis report. Findings and draft recommendations were discussed at an expert and stakeholder workshop with policy makers, NGOs, law enforcement and data protection authorities and so on.

8. Transform results into smaller scale participatory methods to involve citizens in decision making on security technologies and measures. The SurPRISE decision support system was then tested in citizen meetings in five participating countries.

9. Disseminate its findings widely throughout Europe and beyond. SurPRISE used a broad range of multimedia and traditional channels to disseminate its findings to academic, policymaker and practitioner audiences.

2 Main scientific and technical results

Core objectives of SurPRISE were to re-examine the relationship between security and privacy – a relation that is commonly positioned as a 'trade-off', accordingly infringements of privacy are seen as acceptable or necessary costs of enhanced security – and to identify criteria and factors, which contribute to the shaping of security technologies and measures as effective, non-privacy-infringing and socially legitimate security means in line with human rights and European values.

The work of SurPRISE was organised in eight[1] technical work packages. WP1 supported research activities by developing and establishing common project methodologies. WP2 developed a theoretical framing of criteria and factors influencing the acceptance and acceptability of security technologies, which was evaluated and tested in the empirical work done later in the project. Following this theoretical framing, WP3 identified and elaborated on options to shape security measures, to comply with ethical and privacy requirements from a technical, legal and social perspective. Combining the results of WP2 and WP3, WP4 developed an empirical model, which was applied and tested in large-scale participatory activities. WP4 also provided supporting material for the involvement of citizens, including comprehensive information brochures to allow for informed debates and video clips to present a range of conflicting opinions from experts. WP5 organised and conducted large-scale participatory technology assessment events in nine European countries. These "Citizen Summits" involved on average about 200 citizens per country. These citizen summits were full day events, with alternating phases wherein participants received information, discussed the topics and emerging issues in small groups of six to eight persons and voted electronically as individuals on general aspects of the relation between surveillance and security and on specific surveillance technologies. As concluding activity each of the small groups of citizens was asked to develop and formulate recommendations to policymakers. In WP6, the qualitative and quantitative data from the citizen summits were analysed in depth, and synthesised to form conclusions and develop recommendations, combining expert knowledge and citizens perspectives. The methodological approach and results from the citizen summits were also used in WP7 to develop a decision support system, allowing the involvement of citizens in decision-making on security measures and technologies in small-scale participatory events. This approach, called "Citizen Meetings", was also tested in five countries and the results were integrated into the analytical work and the development of policy recommendations.

The following figure sketches the main steps undertaken to derive the results presented here, indicating the main parties responsible for the outcome of each task, the SurPRISE project team, external experts and stakeholders and specifically addressing the role of the citizens participating in the summits and meetings organised by the project.

[1] WP 1 Methodology and design, WP 2 Framing the assessment, WP 3 Exploring the challenges, WP 4 Questionnaire and information material, WP 5 Participatory data gathering, WP 6 Analysis and Synthesis, WP 7 Decision support testing, WP 8 Dissemination and implementation

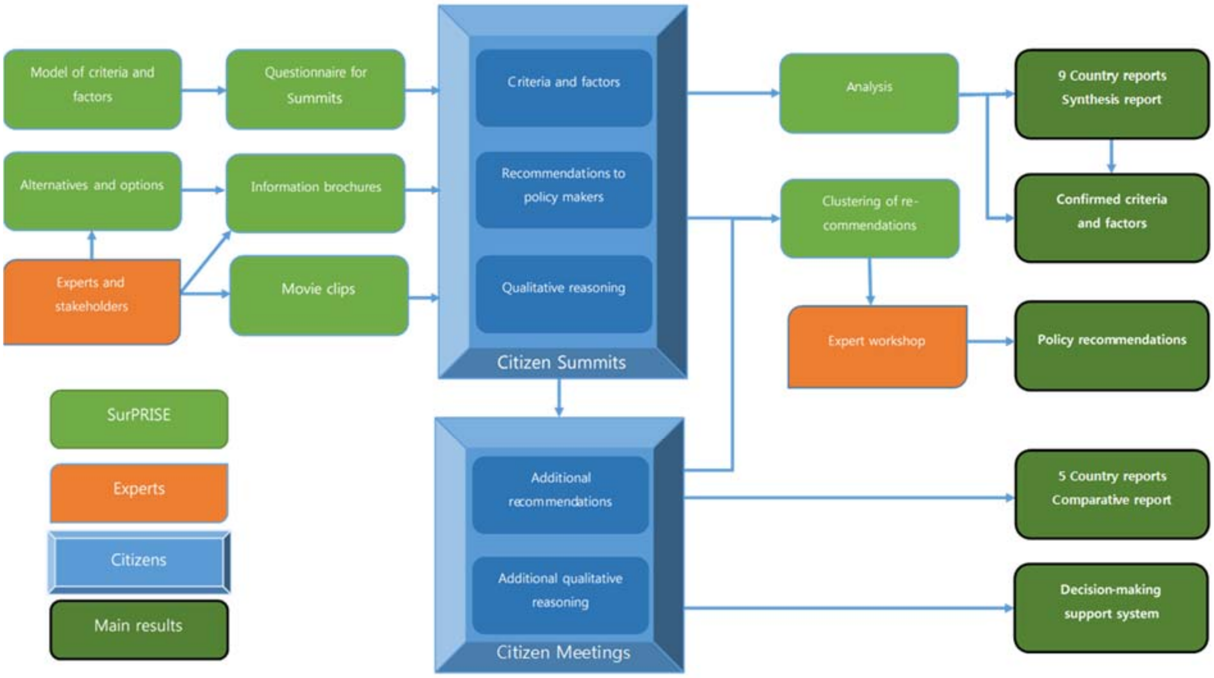

Model of criteria and factors
Questionnaire for Summits
Alternatives and options
Information brochures
Experts and stakeholders
Movie clips
Criteria and factors
Recommendations to policy makers
Qualitative reasoning
Citizen Summits
Additional recommendations
Additional qualitative reasoning
Citizen Meetings
Analysis
Clustering of re-commendations
Expert workshop
9 Country reports Synthesis report
Confirmed criteria and factors
Policy recommendations
5 Country reports Comparative report
Decision-making support system
SurPRISE
Experts
Citizens
Main results

Figure 1: Overview of tasks and responsibilities

2.1 WP 2 Framing the assessment

One of the initial task of this work package was the selection and description of surveillance-oriented security technologies (SOSTs) that built the foundation for the further exploration of the interrelations between privacy, security and surveillance within the SurPRISE project; in particular in the participatory setting to gather citizens' assessments of this interplay. The following SOSTs were chosen, presenting a wide range of technologies and of privacy spheres concerned:

- Cyber surveillance, as it is a sort of meta-SOST and entails a magnitude of privacy impacts also in relation to the other SOSTS. A focus is on data retention and DPI as prominent examples.
- (Smart) CCTV, as surveillance cameras are most familiar and smart CCTV triggers a variety of additional privacy impacts
- Location tracking, due to the rapid progress of smart phones and mobile computing referring to concepts such as ambient intelligence, augmented reality, etc.
- Biometrics due to its high relevance for law enforcement and emergence in many security-related actions
- (Behavioural) profiling, as it also represents a sort of crossover SOST that is increasingly employed in a variety of contexts such as passenger screening.
- Drones as peculiar form of a SOST that is expected to become an issue of wide societal concern

The report "Key factors and criteria affecting public acceptance and acceptability of Surveillance-Orientated Security Technologies" (D2.4), provides a central contribution to the achievement of SurPRISE overall project objectives by offering a detailed recognition of those parameters likely to affect the way in which security measures are assessed by lay people. By gathering insights from relevant studies in the security and technology assessment fields, this report outlines how contextual elements, such as perceived trustworthiness of institutions and operators managing SOSTs, specific features of the technology under study, such as the level of perceived intrusiveness or effectiveness of a given SOST, as well as personal concerns, such as privacy concerns, and individual opinions about the necessity of relying on technological solutions to solve security problems, may affect the probability of considering a given security measure acceptable by citizens.

The results are based on the empirical testing of the theoretical model outlined in the following figure.

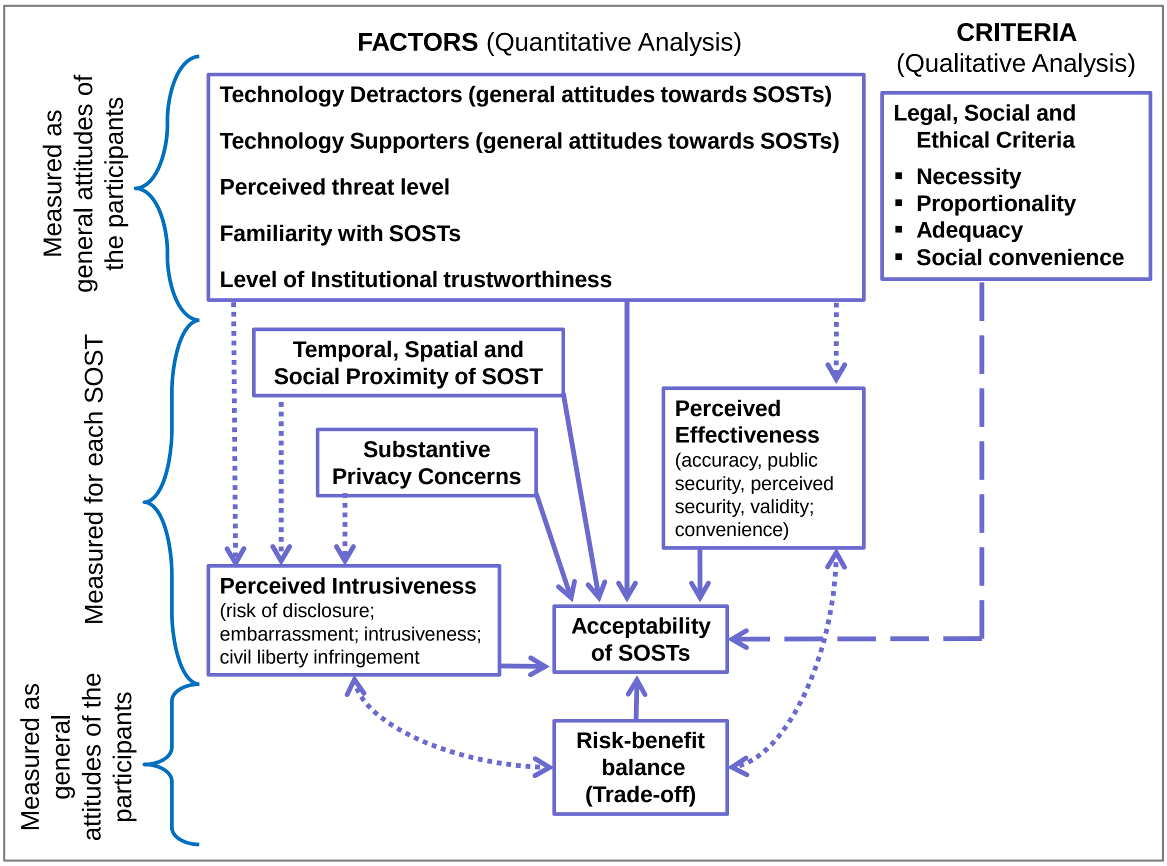

FACTORS (Quantitative Analysis)
CRITERIA (Qualitative Analysis)
Measured as general attitudes of the participants
Technology Detractors (general attitudes towards SOSTs)
Technology Supporters (general attitudes towards SOSTs)
Perceived threat level
Familiarity with SOSTs
Level of Institutional trustworthiness
Legal, Social and Ethical Criteria
▪ Necessity
▪ Proportionality
▪ Adequacy
▪ Social convenience
Measured for each SOST
Temporal, Spatial and Social Proximity of SOST
Substantive Privacy Concerns
Perceived Effectiveness (accuracy, public security, perceived security, validity; convenience)
Perceived Intrusiveness (risk of disclosure; embarrassment; intrusiveness; civil liberty infringement
Acceptability of SOSTs
Measured as general attitudes of the participants
Risk-benefit balance (Trade-off)

Figure 2: Theoretical Model

In the following lists the main findings on factors and criteria influencing the acceptability of SOSTs are briefly summarised.[2] They contain information of highest importance and relevance for policy makers, security agencies, security industry and citizens alike. In the context of SurPRISE, factors represent those elements that influence people's opinions, but that people usually do not explicitly state or that they recognize only partially. Criteria are argumentations consciously used by citizens to explain their position vis-à-vis the acceptability of SOSTs.

Institutional trustworthiness is a key factor determining the acceptability of SOSTs, and it shows that, besides what citizens may think or know about security technologies, the degree of trust that security agencies and political institutions enjoy is a crucial element that citizens do take into account when assessing the acceptability of security technologies. Interestingly, the perceived level of threat has a limited effect on the acceptability of SOSTs, whilst social proximity has a strong impact on acceptability, confirming that security technologies that operate blanket surveillance are considered significantly less acceptable than security technologies carefully focusing on specific targets. Both effectiveness and intrusiveness emerge as highly relevant factors in explaining the level of acceptability of SOSTs. Moreover, whilst much of the security technology discourses insists that security technologies need to be intrusive to be effective, citizens argue that the more a technology is considered intrusive, the less it might be

[2] See D2.4 - Key factors affecting public acceptance and acceptability of SOSTs for a full description of the theoretical foundations of this model, of the complex hypotheses and relationships mapped in the model, of the methods applied in the empirical testing, and of the detailed results of the empirical analyses.

considered to be effective. This results question the general idea that SOSTs need to be intrusive to be effective, and, consequently, radically questions the trade-off approach.

1. **General attitudes towards technology**. A generally positive attitude towards the ability of technology to enhance security makes SOSTs more acceptable. Conversely, a generally critical or sceptical view makes SOSTs less acceptable.
2. **Institutional trustworthiness**. Trust in security agencies makes the use of a given SOST more acceptable. The opposite is also true: the use of a more acceptable SOST (CCTVs or SLT, in this case) helps security agencies to be perceived as more trustworthy.
3. **Social Proximity.** SOSTs targeting specific groups or profiles, usually presented as “suspects” or “criminals” are eventually more acceptable than SOSTs (smart CCTVs and SLT) that operate on blanket surveillance (DPI).
4. **Perceived intrusiveness** has a negative influence on acceptability. The more a SOST is perceived as intrusive, the less it is considered acceptable.
5. **Perceived effectiveness** has a positive influence on acceptability. The more a SOST is perceived as effective, the more it is considered acceptable.
6. **Substantive privacy concern.** A higher concern for both information and physical privacy makes SOSTs less acceptable.
7. **Age**. Age is positively correlated with acceptability of SOSTs. Older participants are more likely to accept SOSTs than younger ones.

Table 1: Factors influencing acceptability of SOSTs (statistically significant)

1. **Perceived level of threat**. Contrary to expectations, a more intense perception of security threat would NOT make SOSTs more acceptable. Concerns for online security, though, do have a positive effect on acceptability: the more participants are worried about their safety online, the more willing they were to accept SOSTs.
2. **Spatial proximity**. The proximity of SOSTs located and/or operating close to the physical and virtual spaces usually frequented by the participants did not influence the acceptability of SOSTs. However, we found that it has an effect on Substantive Privacy Concerns, which decreases the likelihood of considering SOST acceptable.
3. **Temporal proximity.** The prospective of SOSTs being very influential in the future did not influence the acceptability of them. However, we found that it has an effect on SOST Perceived Intrusiveness and Substantive Privacy Concerns, which, in turn, decrease the likelihood of considering a SOST acceptable.
4. **Familiarity with SOSTs.** Contrary to expectations, a deeper familiarity with SOSTs does not influence the acceptability of them.
5. **Security/privacy balance**. Considering technologies as both intrusive and effective do not make these technologies, in general, more acceptable. This relation has been confirmed only in the case of DPI.
6. **Education.** The educational level does not influence acceptability of SOSTs.
7. **Income.** The income level does not influence acceptability of SOSTs.

Table 2: Factors influencing acceptability of SOSTs (statistically not significant)

SurPRISE identified a number of criteria influencing the acceptability of surveillance technologies.

SOSTs are regarded as more acceptable if:

- operating within a European regulatory framework and under the control of a European regulatory body.
- operating in a context where transparency about the procedures, information about both data protection rights and principles and about the purposes and the scopes of security actions as well as accountability of security operators is ensured at all times.
- operated only by public authorities and only for public benefits. The participation of private actors in security operations, such as when security agencies acquire banking data or Facebook data or when security functions are outsourced to private operators, therefore, must be strictly regulated.
- their benefits largely outweigh their costs, especially in comparison to other non-technological, less intrusive, alternatives.
- their operation can be regulated through an opt-in approach. Whenever this is not possible, their operation need to be communicated to targeted individuals.
- they allow monitored individuals to access, modify and delete data about themselves.
- they target less sensitive data and spaces, whenever possible, according to criteria and purposes know to the public.
- they do not operate blanket surveillance. After reasonable evidences are gathered, they address specific targets, in specific times and spaces and for specific purposes. Whilst their purposes may change, these changes need to be explicitly discussed and publicly approved.
- they incorporate Privacy-by-Design protocols and mechanisms.
- they work and operate in combination with non-technological measures and social strategies addressing the social and economic causes of insecurity. SOSTs are not alternatives but complementary to human resources and social policies.

These criteria are also addressed by the recommendations developed by and included in the description of WP6 below. They should be integrated in decision making on SOSTS as an additional checklist and initial opening of the evaluation process.

2.2 WP 3 Exploring the challenges

WP3 – “Exploring the challenges” reviewed and explored challenges and options for technological, legal, political, and societal developments on privacy and security. In this section the key findings from the different perspectives of law, technology and social science are summarized and a number of policy implications are presented for discussion.[3]

Key findings

- The rights to privacy and data protection express crucial societal values. Privacy refers to the sphere of a person’s life in which he or she can freely express his or her identity. As such, it puts normative limits to technological advances (notably in the field of ICTs) and related practices that enhance human possibilities but interfere with autonomy and freedom (of home, body and correspondence).

- Such values informed the legislative development of the right to privacy, from article 12 of the Universal Declaration of Human Rights of 1948, to articles 7 and 8 of the European Charter of Fundamental Rights, including a full acknowledgment of the right to personal data protection. The formulations of the right to privacy attest to its universal relevance. “Privacy” appears as an umbrella term encompassing several different dimensions, a versatile understanding upheld and fostered by Courts. Data protection appears as a more “procedural right” safeguarded by the mechanisms put in place by the legal instruments. Both rights, though, are defined as relative, in the meaning that they

[3] By IRKS, EUI, ULD

can be interfered with by means of permissible limitations, which must respect a number of criteria that have been interpreted and clarified through case law.

- The established meaning of the fundamental rights to privacy and data protection allowing for permissible limitations implies that, in principle, there is no opposition between their protection and the achievement of individual or public security, understood as a legitimate aim. In practice, however, after the terrorist attacks of 9/11, law enforcement activities driven by the collection of personal information have expanded, leading to the increased use of SOSTs.[4]

- The research conducted challenges the security vs. privacy approach, and proposes an analytical alternative: the core/periphery approach (based on a reinterpretation of Robert Alexy's theory of rights). The theory can be applied to explain how any fundamental right would have an inviolable core (often more than one such core) or "essence" sealed in a rule, and a periphery surrounding that core and subject to permissible limitations. Three different criteria have been preliminarily suggested as candidates to determine the scope of the core of the right to privacy: sensitive data as privileged content, information produced in the course of confidential personal relationships, and methods of intrusion. The inviolability of the essential core of any human right – in this case the right to privacy – is one of the steps in an analytically rigorous test for the permissibility of restrictions.

- The test for permissible limitations incorporating the core/periphery theory could provide a tool for evaluating the acceptability of SOSTs and SOSSs, whenever an interference with the right to privacy is the outcome.

- Surveillance-oriented security technologies often do not stand the test of functionality outside controlled laboratory settings. There is often an imbalance between intrusiveness and the security gain to be achieved by SOSTs.

- Technological solutions to enhance privacy (mainly privacy by design) are difficult to implement for most surveillance technologies.

- SOSTs do entail a social definition of normal and deviant (or unusual, suspicious) behaviour. Since the underlying algorithms come with the inherent assumption of zero-tolerance, such definitions can create a substantial number of false positives when the technology is implemented.

- All SOSTs are prone to function creep and also abuse and may easily be used outside the narrowly defined realm justifying their implementation in the first place. It is difficult to control such proliferation once a given technology is put in place.

- Alternative concepts to enhance security typically target root causes of societal problems. Technological solutions focus on a narrow understanding of security and ignore the wider societal context.

- Security is a multi-dimensional concept and has to be understood in a comprehensive sense. Reducing security discourse to a narrow understanding of identifying potential perpetrators by means of pervasive surveillance ignores aspects of perceived security.

[4] The ensuing policies in the field of AFSJ, such as the Council Framework Decision 2008/977/JHA and the Data Retention Directive, framed the relationship between privacy (together with data protection) and security predominantly in terms of the need to "strike a balance", i.e. to weigh against each other security interests and privacy (and data protection) rights. Yet, such rhetoric de facto often results in introducing excessive limitations to these rights, questioning their significance in our society.

- Technology use in contemporary societies creates security problems and problems of privacy and data-protection at the same time.

- Falling back on alternative societal solutions to reduce security risks in modern societies is difficult since these alternatives often involve elements rooted in traditional social forms of community life which cannot be revitalized at will. Furthermore communitarian approaches to security tend to entail a limitation on individualistic life styles typical for modern societies.

Policy suggestions from a legal perspective

- Fast technological and technical innovations constantly put under test our understanding of the fundamental rights to privacy and data protection, sometimes to the effect of making the mechanisms of protection that we devised obsolete. A deterministic approach whereby the full enjoyment of the rights is inevitably sacrificed vis-à-vis technological innovation and its many applications is not compatible with a democratic society. We suggest:

- Promoting a political reflection as to how to harmonize the enjoyment of human rights with the technological innovation and its application in the field of Justice and Home Affairs.

- Including in these reflections a commitment to the idea that the essence of any fundamental right is inviolable (the core/periphery approach) and that in issues that do not fall within the essence (core), a proper proportionality assessment is required, including through demonstrating that the benefits actually delivered are greater than the intrusion into privacy and data protection.

- This requires introducing technology assessment at the earliest stage of policies in the AFSJ. As it is understood that law enforcement agencies will avail themselves of technologies, the discussions of which technologies are permissible (and acceptable) should be fully included in the decision-making processes.

- Such a process requires the involvement of data protection agencies, technology experts and civil society organizations.

- Excluding citizens from the decision-making process as to what technologies are permissible could affect the right to good governance. Citizens at the national level need to be fully involved in the process. National governments should address the democratic deficit in this field.

Policy suggestions from a technological perspective

- Policy-makers have to make important choices on the implementation of SOSTs. In order to do this in a rational way, compatible with principles of privacy and data-protection, they should be able to answer the following questions, using the proficiency of independent experts from the relevant fields of privacy impact and technology assessment. These criteria or questions also connect to the test of permissible limitations.

- How does a given technology work exactly?

- Which individuals or groups are affected primarily and in what way?

- What are the benefits for enhancing security this technology provides?

- Can the security gains be measured independently?

- Which risks are known or anticipated when implementing a given technology?

- Can Privacy by Design approaches be applied and are non-technological alternatives available to address the problem at hand?

- Do the criteria for technology impact assessment applied strike a balance between security and privacy?

- Does the technology stand the test of criteria from a legal point of view:

- Necessity, suitability, and proportionality? How are these criteria operationalized into technological requirements of design?

Policy suggestions from a social perspective

- Narrowly defined security problems should be deconstructed into more general problems of social justice and inequality. This can open the horizon for alternative solutions addressing root causes of security threats.

- Strengthening available societal resources can have preventive effects in the long run and increase social resilience, i.e. making societies more robust in the face of different types of threats.

- Security should not be perceived as the exclusive domain of law enforcement and intelligence experts. Security has to be taken back from the experts to the general public. Involving citizens and civil society organisations in an informed public debate about security can create a better and more comprehensive understanding of the different aspects of (perceived) security.

- Policy discourse on security issues should not fall prey to securitization. The broader the perspective adopted when analysing policy options the better the chances to develop a sustainable solution for security problems.

- Security should always be understood as a public good, a discursive object and an individual psychological state at the same time, taking into account the interrelation between these different kinds of security.

- Policy makers should refrain from strategies claiming the elimination of security risks but rather strive for balanced risk awareness as desirable public attitude.

2.3 WP 4 Questionnaire and information material

WP 4 was responsible for transferring the theoretical model into an empirically testable questionnaire and for the preparation of all information material required for the participatory involvement of citizens.

Here an extract of the questionnaire is depicted for illustration; the questionnaire used is composed of about hundred questions in total, comprising demographic questions, general attitudes, SOSTs specific attitudes and the evaluation of the event itself.

GENERAL ATTITUDES OF THE PARTICIPANTS (BEFORE FILMS)

I. Now we are going to ask you about how safe you feel in your daily life. The question appears in the form of a statement. You can choose between 5 different responses:

If you strongly agree with the statement, click 1
If you agree with the statement, click 2
If you neither agree nor disagree with the statement, click 3
If you disagree with the statement, click 4
If you strongly disagree with the statement, click 5

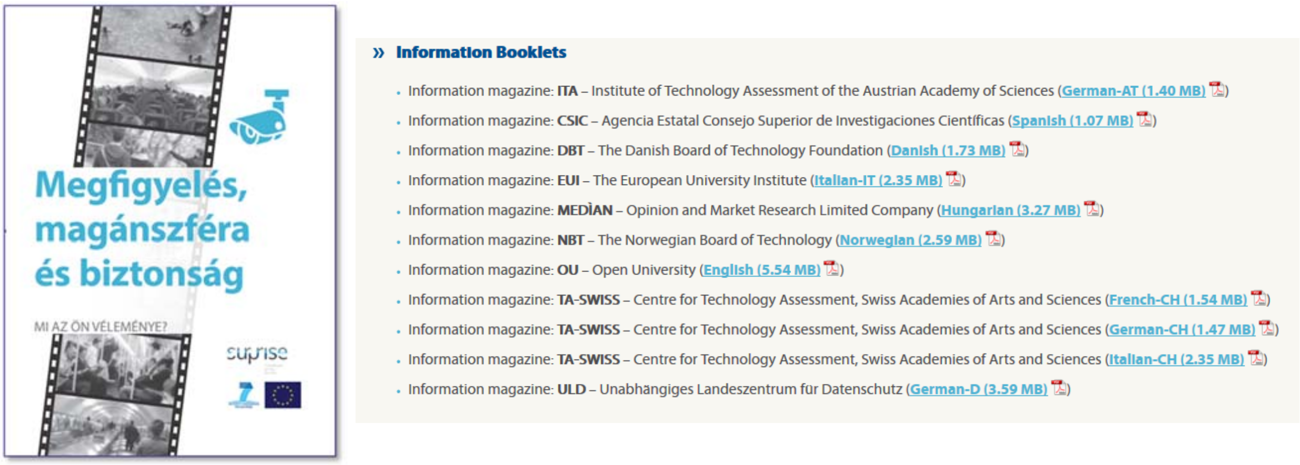
1. I generally feel safe in my daily life.
2. I worry about security when I am online.
3. I feel that this country is a safe place in which to live.

II. Now we'd like to ask you about your knowledge of these issues before you came along to this event, and before you read our magazine. There are four possible responses.

4. Before reading the SurPRISE information booklet how would you rate your knowledge of security technologies?

Click 1 for 'I was very knowledgeable about security technologies'
Click 2 for 'I knew something about security technologies'
Click 3 for 'I knew very little about security technologies'
Click 4 for 'I knew nothing about security technologies'

In order to support an informed debate among the participating citizens, an information booklet of about 40 pages was distributed in advance to the participants. The booklets contain an introduction to surveillance, privacy and security, describe the discussed security technologies (why they were developed, how they are used, which security improvements they promise and which issues they raise), and the discussion of non-technical alternatives. The booklet was translated into eight languages for use in all of the European countries involved in the project.



» **Information Booklets**

- Information magazine: **ITA** – Institute of Technology Assessment of the Austrian Academy of Sciences (German-AT (1.40 MB))
- Information magazine: **CSIC** – Agencia Estatal Consejo Superior de Investigaciones Científicas (Spanish (1.07 MB))
- Information magazine: **DBT** – The Danish Board of Technology Foundation (Danish (1.73 MB))
- Information magazine: **EUI** – The European University Institute (Italian-IT (2.35 MB))
- Information magazine: **MEDÌAN** – Opinion and Market Research Limited Company (Hungarian (3.27 MB))
- Information magazine: **NBT** – The Norwegian Board of Technology (Norwegian (2.59 MB))
- Information magazine: **OU** – Open University (English (5.54 MB))
- Information magazine: **TA-SWISS** – Centre for Technology Assessment, Swiss Academies of Arts and Sciences (French-CH (1.54 MB))
- Information magazine: **TA-SWISS** – Centre for Technology Assessment, Swiss Academies of Arts and Sciences (German-CH (1.47 MB))
- Information magazine: **TA-SWISS** – Centre for Technology Assessment, Swiss Academies of Arts and Sciences (Italian-CH (2.35 MB))
- Information magazine: **ULD** – Unabhängiges Landeszentrum für Datenschutz (German-D (3.59 MB))

Figure 3: Information booklets

Three of the selected SOSTs were presented and debated at the large-scale citizen summits. For each SOST a movie clip of about seven minutes length was produced. Experts from different backgrounds, representing different stakes and interests, were interviewed to explain the technologies and to discuss the pro and cons. The movie clips were also translated and subtitled in all languages (in Denmark and Norway the English versions were used and just subtitles in the national languages provided).

Figure 4: Movie clips for the discussed SOSTs

2.4 WP 5 Participatory data gathering

WP 5 was responsible for the organisation of the large scale participatory events, also used for the empirical testing of the model developed in WP 2. On average about 200 citizens participated in Citizen Summits in each of the nine involved European countries to discuss and provide their view. At these events the participating citizens also answered questionnaires, comprising a broad range of factors, examining and explaining the acceptability and acceptance of surveillance technologies beyond the security-privacy trade off. The arguments raised by citizens in the deliberative discussion were integrated in the analysis. The participants were also asked to formulate and write down their own ideas and recommendations to policymakers.

Figure 5: Setting at the citizen summits

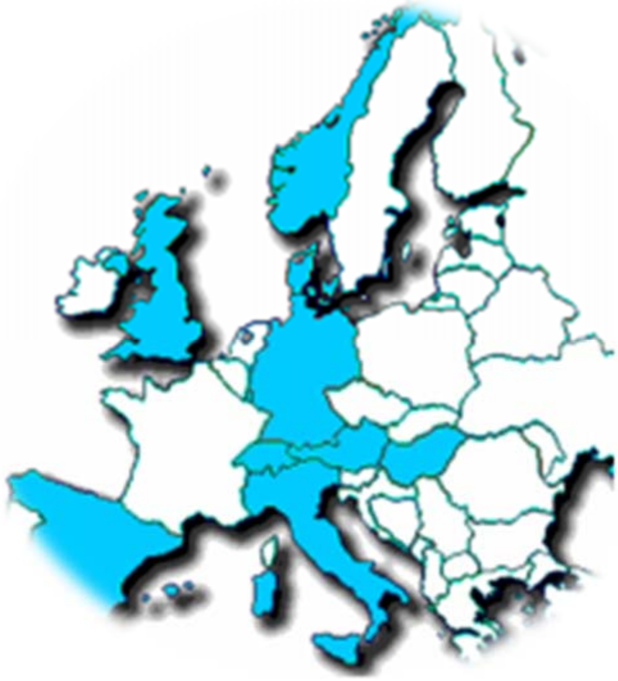


Figure 6: Countries in which the citizen summits were conducted

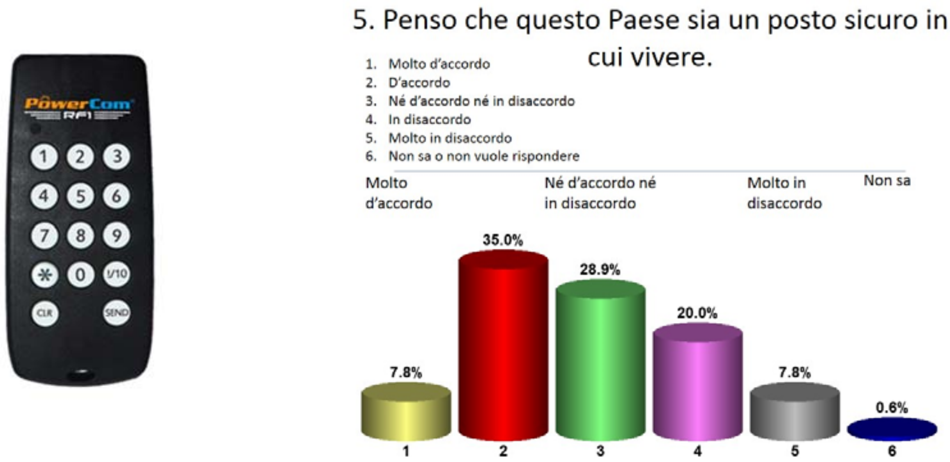


Figure 7: Clickers for anonymous electronic voting; the results for each question were presented immediately after voting

2.5 WP 6 Analysis and Synthesis

WP6 was responsible for the analyses of the quantitative and qualitative data for the participating countries and for the synthesis of the country reports. The following figures provide examples of the kind of comparative data generated at the citizen summits.

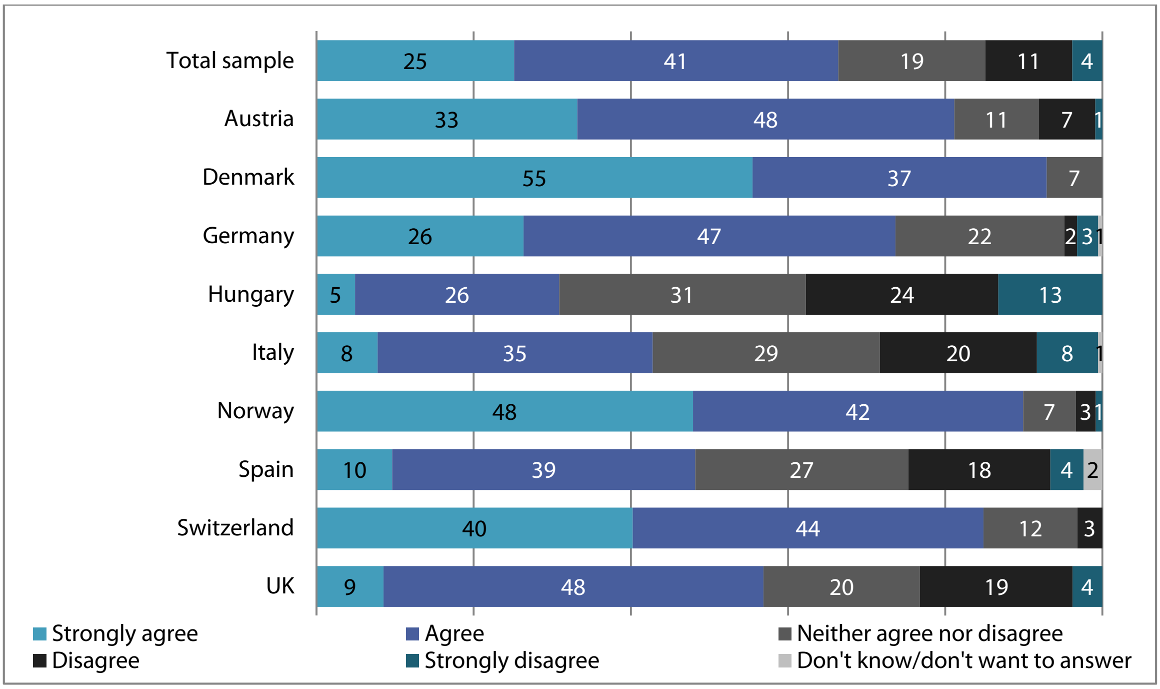


Figure 8: "I feel that this country is a safe place in which to live" (percentages)

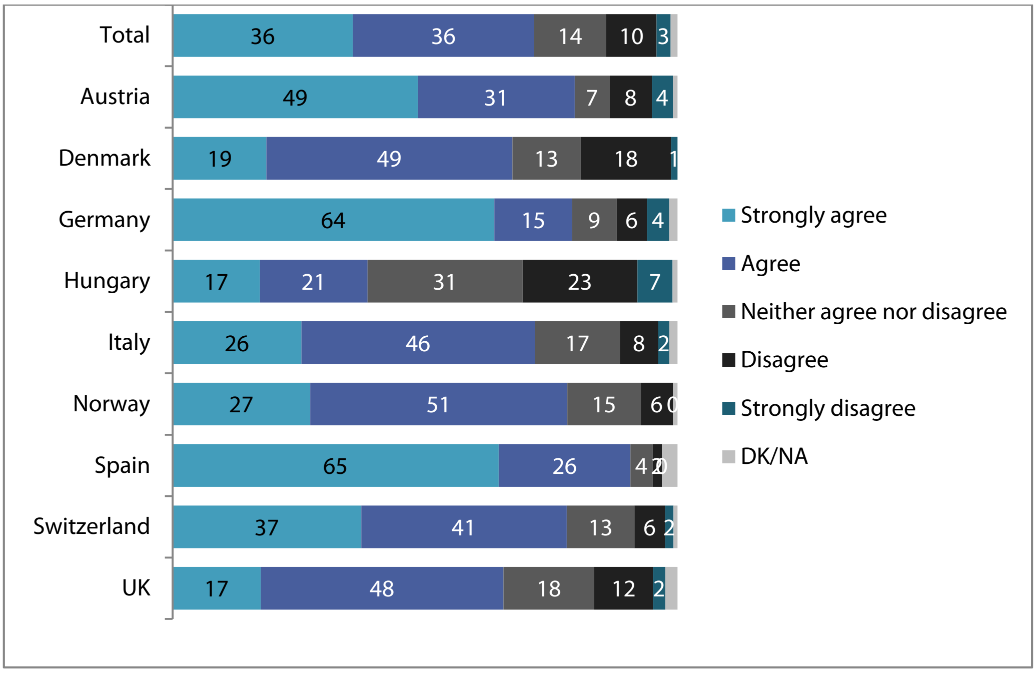


Figure 9: "I am concerned that the use of surveillance-oriented security technologies is eroding ***privacy in general***" (percentages)

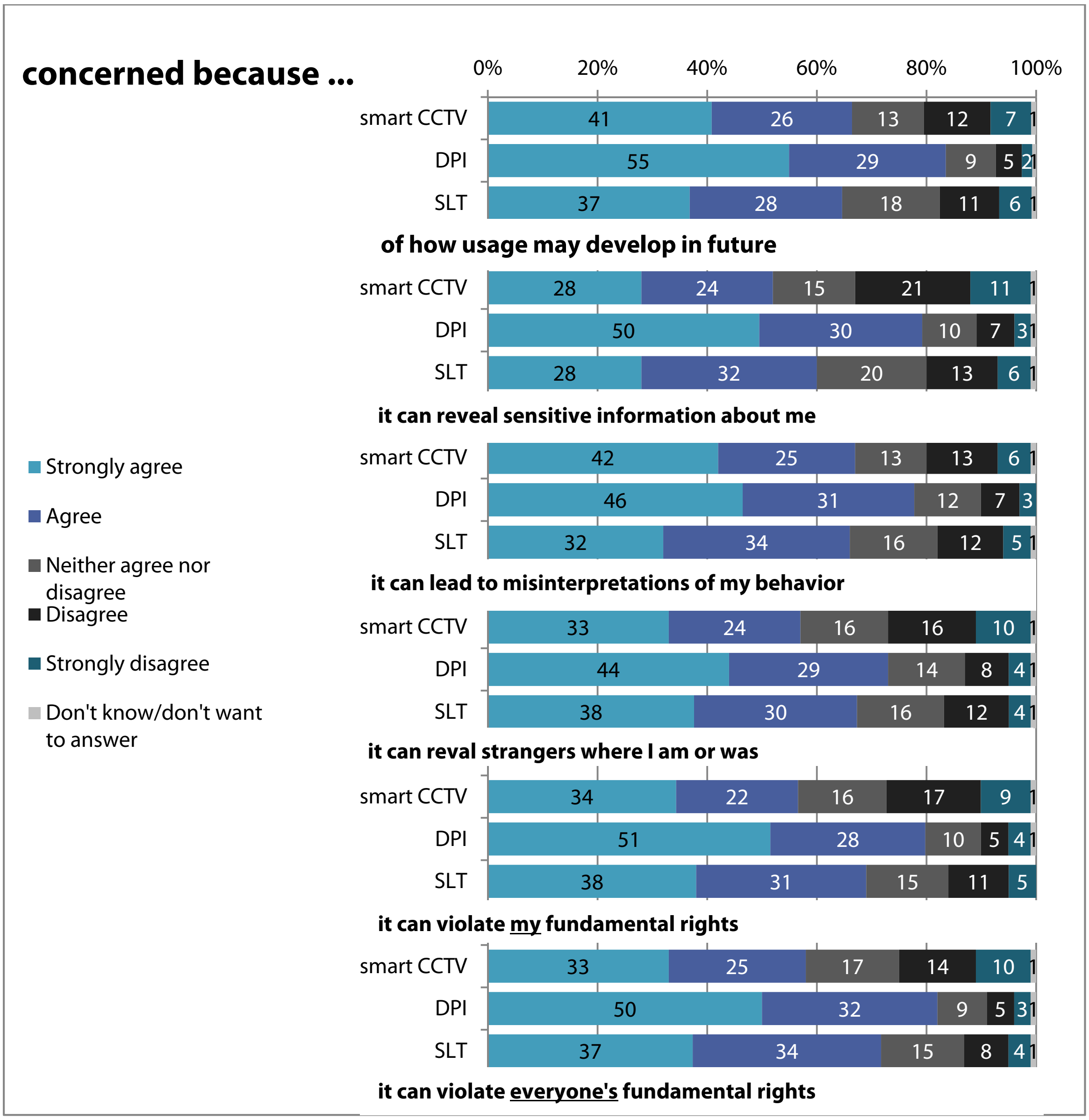


Figure 10: Major concerns regarding particular SOSTs

WP6 was also responsible for the elaboration of policy recommendations. The results of the involvement of about 2000 citizens from nine European countries in participatory assessment activities of SOSTs conducted by the SurPRISE project, confirm the scepticism against the trade-off approach in general and, in particular, as a suitable guideline for decision-making related to security policy. The participants of the Citizen Summits and Citizen Meetings predominantly requested strict limitations and regulations with regard to the use of surveillance technologies.

The development of the recommendations encompassed several steps. An essential contribution came from citizens participating in the Citizen Summits and Meetings. Their recommendations were integrated in and enriched by academic research and expertise within and external to SurPRISE:

The legal framework on data processing must meet the challenges of technological advances

The current data protection legal framework needs to be adapted and modernised to meet the specific challenges of the most recent tools and techniques of (big) data processing performing data crawling, matching, linkage and analysis functions. In particular, the impending major reform of the EU-level data protection legal framework should set rules that explicitly target the functions (or effects) of such tools in the course of private and public activities including law enforcement, to preserve protection levels independently from technological progress.

These rules should be specified and operationalised in form of technical annexes. The annexes should be regularly updated and, if required, be extended to allow the law to keep in line also with future technological advancements.

Enforcing data protection in Europe

The impending revision of the data protection legal framework on the EU-level and amendments of national law should provide for mechanisms to effectively enforce data subjects' rights, also when tackling national and public security.

To this effect, an integrated strategy should be adopted at the national and European level (where applicable also on the local level) that takes into account the interaction between the private and the public sectors. At the local/national level, real control over data processing should be enabled, e.g., with mandatory ex post notification of data processing in law enforcement, the failure of which is subject to sanctions. Data protection authorities should be given harmonised powers of investigation and sanctioning, backed by sufficient human and financial resources. At the European level, collective lawsuits for mass-scale violations and the infliction of deterring sanctions should be enabled.

Protect personal data in transit, notably on the Internet

Technical and legal solutions need to be adopted to protect data in transit, notably on the internet, and in particular data travelling outside the European Union and the Schengen area.

Technical means to protect the privacy of transferred data should be explored and implemented. The conclusion of legally binding treaties with other countries, like the United States of America, is strongly recommended. Such treaties would protect data subjects in the context of both commercial activities and operations conducted for the pursuit of public and national security. The transfer of data, especially for law enforcement purposes, to jurisdictions that do not offer an equivalent protection with regard to data processing, should be the exception and be duly accounted for.

A common policy should be developed and rules should be uniformly applied and enforced throughout the European Union and the Schengen area.

Strengthen agencies providing supervision, guidance and control

For the processing of personal data, particularly in the field of police and justice, harmonised guidelines on a high level of protection are necessary. This especially applies to the respective control instances as well as to their control standards. Where data protection authorities exist in the EU member states which are already concerned with such tasks, they should be strengthened. Independent, competent and empowered data protection authorities should ensure meaningful supervision, guidance and control regarding the protection of personal data and the privacy of the individual. They should be enabled to include representatives of different knowledge areas and societal domains into their personnel structure.

With the background of already existing local, national and European supervisory authorities, it is recommended that these authorities are organised in such a way that governance is provided by them close to the European citizens and with effective means of enforcement even in cases of cross-border data transmissions.

An effective supervision and control of personal data processing by private (and internationally operating) companies is needed. These companies are oftentimes obliged to cooperate with security agencies. As for the security agencies themselves, a clear concept for the competences of data protection supervisory authorities and their jurisdiction over intelligence agencies is required.

All data protection supervisory authorities should be made better known to the citizens.

Implement proper safeguards

Untargeted mass surveillance circumvents existing legal safeguards. Any restriction of fundamental rights resulting from the use of surveillance technologies and derived personal data must be based on a stringent case-by-case examination of their permissibility, such as that foreseen by articles 52.1 and 52.3 of the Charter of Fundamental Rights of the European Union. Such examination must ensure that:

a) any restriction of fundamental rights has a proper legal basis;

b) these restrictions are compatible with a democratic society;

c) any exercise of discretion by (administrative) authorities is foreseeable and constrained;

d) these restrictions are reasonable, necessary and proportionate in achieving an identified and pressing aim;

e) they do not violate the core dimensions of privacy (as progressively identified).

Such a test should be performed prior to the adoption of a tool or derived data, they should encompass the implementation and use and they should be subject to ex post reviews by independent judicial authorities.

Limit the scope of data collection

Enable a more effective preservation of citizen's right to privacy by meaningful enforcement of the principles of purpose limitation and proportionality. This encompasses a genuine consideration of non- or less intrusive alternatives prior to the deployment of broad dragnet surveillance measures for security purposes. Develop, foster, and prioritise measures (including SOSTs) with a narrower scope of data collection, storage and use whenever they are suitable instead of focusing on forms of untargeted mass surveillance.

Increase accountability and prevent abuse

European states need to promote and pursue a sincere political reflection as to how to design and deploy technology for security purposes in compliance with fundamental rights. Stronger accountability and liability for misuse and abuse must be established in both the public as well as the private sector. Measures include:

- introducing and enforcing effective and deterrent sanctions;
- making misuses publicly known;
- supporting whistleblowing schemes;
- storing data securely, and never reselling or transferring them; and
- limiting automated decision-making based on the collected data (algorithms-based decisions) so that they assist humans, rather than replace them.

Organisational and technical measures should be implemented to prevent abuse and to make abuses detectable to supervisory agencies.

Regulate and limit the role of private and non-governmental actors in the provision of public and national security

Security should remain the responsibility of state actors. It should be clarified to which extent and in which way the private sector and non-governmental actors currently contribute to the pursuit of security and to which degree these contributions are necessary. Outsourcing security and cooperating with private actors (including data requests) should be made known and subjected to public scrutiny. Suitable and legitimate cooperation between such actors and the state must be strictly regulated. Breaches of the law should be strictly sanctioned.

Security functions may only be outsourced if the contributions of private actors are equally or better than public standards in both terms, compliance with fundamental rights and quality of services.

The ownership and control of data should always remain under European legislation, security related data must not be mixed with other private data. The limitation concerns also the transfer of data from public authorities to private entities, it must be not allowed to sell data to private actors, neither for security nor for commercial purposes.

Establish a privacy-orientated competitive market

Policy makers should provide regulatory acts and incentives to establish a European market where privacy constitutes a competitive advantage. To this effect two sets of measures should be adopted. First, incentives in the form of regulation should be implemented, e.g., obligatory Privacy by Design for public procurement. Second, asymmetric or missing information of citizens concerning means of data collection, storage and use should be corrected, e.g., by mandatory information of users of "free services" about the basis of business models of such offers.

Implement and improve transparency

Member states need to increase their efforts to implement and improve the transparency of policy decisions, of the work of security authorities as well as of corporations and companies, in particular if the privacy of the citizens is affected. Transparency must be supported actively as current arrangements are insufficient and must comprise more than existing rights to know. Different communication channels should be used to reach as many parts of the population as possible.

Information about data access rights is not enough, transparency must include information about who is doing what and why to get more active insight.

Transparency does relate to policy making, the Constitution and laws on the one hand, and also to the practices of data collection, storage, processing, linkage, and (re)transmission on the other hand.

At least three levels of transparency are to be envisaged:

- transparency about policy (legislation transparency),
- transparency about security authorities (operational transparency),
- corporate transparency (corporate and social responsibility).

Citizens should be given the right to access on a low-threshold level sufficient information on how surveillance systems operate, information on which and where surveillance systems have been implemented and information on how they can exercise their civic rights (e.g., in order to gain information about what kind of data about them is stored and processed where and by whom).

Mandatory standards based on (independently evaluated) best practices according to operational transparency as well as corporate and social responsibility should be implemented.

Improve training and education of security authorities

There is a need for more training and education for the personnel of security authorities and stakeholders in various surveillance practices to improve their work in order to act in compliance with privacy and other fundamental rights. Stakeholders in surveillance practices refer to all parties who are involved in conducting surveillance practices such as governmental organisations, service providers (public and private), staff of (surveillance) technology producers and vendors, or consultancies advising security authorities.

Only authorised, trained and ethically aware personnel should be allowed to handle SOSTs and the derived data.

Raise awareness on security and privacy

Governments should support all actors in the field of education to reach citizens and educate the population on how new information technologies, and in particular SOSTs work, and how citizens can protect their privacy and manage their digital data. Appropriate strategies should be developed and implemented for different knowledge levels, ages and social backgrounds.

Foster participation in decision making

Citizens need to be fully involved in the process of policy-making, at least at the local and national level. National and regional governments should open the debate on surveillance orientated security technologies to the public and find appropriate solutions for involving citizens directly in decision making. This may entail several approaches, such as enhanced information through media, citizen consultations, participative TA (see Establish technology assessment and on-going evaluation), or referenda. This involvement should come along with prior provision of objective information about facts which are related to the topics of the public discourse.

Establish technology assessment and on-going evaluation

A Technology Assessment (TA) should be conducted from the earliest stage of developing security technologies. A vital part of technology assessment is looking for and evaluating different alternative solutions, be it technical, organizational or legal. Applied TA methods should provide a transparent and participative assessment of alternatives. TA is therefore more comprehensive than a Privacy Impact Assessment (PIA) only. The discussions of which technologies are permissible (and acceptable) should be mandatory and fully included in the procurement and decision-making processes.

An evaluation of surveillance-orientated security technologies should also embrace implementation and deployment. Therefore, it needs to be regularly repeated during use by an impartial and competent entity. This evaluation should support and extend the case-by-case examination of their permissibility addressed in the recommendation, Implement proper safeguards. It should operationalise the permissibility test by covering the following aspects: suitability, effectiveness, cost, robustness, ethical and societal impact, privacy impact assessment, means of intended deployment, and the existence of potential alternatives.

Request mandatory Privacy by Design and Privacy by Default

The integration, maintenance, and further development of Privacy by Design and Privacy by Default principles should become a mandatory requirement for the development and implementation of surveillance orientated security technologies. Implementing PbD may occur in various ways, such as reducing the amount of data initially collected, obfuscation of sensitive information, preventing unauthorized access or misuse for other purposes. Furthermore, it must be ensured that the realisation of PbD is effective, comprehensible, evaluable, and that it goes along with an effective Privacy Impact Assessment in advance.

Focus on root causes of insecurity

Economic and social policies should become an integral element of security strategies at the level of the European Union and its member states. Reducing economic inequalities and addressing the general problems of lacking social justice are of essential importance for other key dimensions of security. It is an indispensable contribution to the prevention of violent radicalisation, and also a precautionary measure against poverty related crime, terrorism and the loss of political and societal cohesion in Europe. National and European policy-makers in the area of security policy should be aware of these intertwined factors and urgently foster measures to improve the economic and social situation.

Details, backgrounds and suggestions for implementing all these recommendations can be found in the Policy Paper (D6.13) on the project's website: http://surprise-project.eu/dissemination/research-results/

2.6 WP 7 Decision support testing

A major task of WP7 was to develop and to test the SurPRISE Decision Support System (see the next chapter on potential impact, the main dissemination activities and the exploitation of results for details) in small-scale participatory activities. The SurPRISE DSS was developed in order to guide the process and record the data of small-scale events (citizen meetings), it was used in the small-scale events conducted in five countries by the SurPRISE consortium. Apart from testing the system and the supporting web tool, the citizen meeting contributed to in-depth insights on the attitudes and lines of argumentation of citizens. In addition to the three SOSTs discussed at the Citizen Summits, smart CCTV, deep packet inspection (DPI) and smartphone location tracking (SLT), the small-scale events considered five SOSTs, the above three as well as drones and biometrics.

The "image" of the five technologies discussed in a greater depth by participants during the citizen meetings can be summarised as follows:

Deep packet inspection (DPI)

- Difficult to grasp
- Useful in maintaining the digital infrastructure
- Has some national security advantages (for intelligence and crime prevention)
- Can be used for targeted surveillance of suspects of serious crimes
- Highly intrusive when used for mass surveillance (a danger to freedom of expression and to democratic freedom; data could be manipulated, modified, or interpreted out of context)
- It may be a useful tool if it is handled with legal and judicial authorization
- Acceptability is context related, and depends on how "just" the government is and if fair and effective regulations are in place

Biometric identification

- New, not really known technology in its early stage of development
- Useful in investigations
- Ensures security of e.g. work place or while travelling
- Reliable and safe
- Not intrusive to privacy
- Concerns are related to the development and storage of biometric databases

(Smart) CCTV

- Smart functions are not known
- Preventive with regards to petty crime
- Can help to detect crime retrospectively
- Improves public security and the feeling of safety by its deterrent effect
- Not very intrusive; it does not target individuals (but smart cameras do)
- The most accepted technology

Smartphone location tracking (SLT)

- It is primarily seen as convenience technology
- Only useful in investigating or preventing crime to a limited extent
- Improves the sense of personal security, but primarily because of the permanent availability of convenience services
- Rather intrusive (danger to democratic freedom, lack of control on the consequences drawn from location data)
- Distrust towards the service providers is evident and has a negative impact on trust towards security authorities that use SLT
- Trade-off appears between convenience and privacy

Drones

- Not known as SOST
- Modern technology (represents development)
- Associated military use might generate distrust
- Improves national and personal safety only if used in specific situations, such as:
  - accidents, disasters, terrorist attacks, fire – to provide an overview;
  - for search and rescue to avoid putting people into hazardous situations;
  - after a serious crime has been committed (for following criminals);
  - in dangerous situations to increase public safety (e.g. mass events)
- Very intrusive if used for prevention in general (they can monitor private areas that belong to the core of privacy)
- Dangerous technology in itself (they can crash, terrorists can use them)
- Drones should not be permitted for use by the general public, or should be regulated in much the same way as gun ownership

Figure 11: Perceptions of particular SOSTs

3 The potential impact, the main dissemination activities and the exploitation of results

3.1 Potential impact

SurPRISE addressed the need for going beyond conventional studies which consider the relationship between privacy and security as a zero-sum game. These studies not only fail to address the complexity of the relationship between privacy and security, they also neglect the social, institutional and cultural factors that influence this relationship and the variety of public responses to the implications of introducing new surveillance-oriented security technologies. They also obscure the existence, and relevance, of alternative approaches, which stem from complex social dynamics and may consider more legitimate effective and appropriate non-technological solutions to security challenges. SurPRISE provided a major contribution to overcome these limitations.

The research design acknowledged the complexity and multi-faceted reality of the relation between security challenges, technological solutions and citizens' responses. It developed an innovative research process, which combines frame analysis with an ethically and legally informed analysis of the societal/institutional context and implications of both technological and non-technological strategies. SurPRISE developed an empirical model, which identifies and combines relevant factors related to acceptance and acceptability of SOSTs, and tested it with the most advanced techniques of participatory data-gathering. The qualitative and quantitative data retrieved are comprising the variety of opinions existing across the countries selected, they provide therefore an excellent ground for a comprehensive and reliable description of existing public demands and requests, and therefore for inspired and farsighted policy recommendations. The results represent a valuable combination of expert based knowledge and public understanding. They provide technology-specific and context-specific implications derived from a comprehensive, open and reflexive assessment process.

SurPRISE elaborated a socially and scientifically robust decision support system, which can assist all kind of users (i.e. from a variety of publics, to policy experts and policy makers, industry representatives and scientific and community stakeholders) to understand, analyze and evaluate any single security option – technological or not – from different angles. This variety of perspectives – including information from legal and institutional contexts, technical information, socially reflexive knowledge and applied ethical reflections – provides a comprehensive evaluation background for assessing the social, economic and scientific appropriateness of developing and implementing technological and non-technological security measures. On the basis of this information, the decision support system allows a preventive assessment of the expected acceptability of any single security option, informed and balanced against its actual social acceptance in the chosen national or international security policy context.

The decision support offered by SurPRISE adds to existing activities in this domain by specifically focusing on the citizens' perspective, let them be heard and their opinion be integrated in the expert and political debate and decision making. The analysis of the citizen summits provided robust knowledge of citizen attitudes, evaluations and lines of reasoning, contributing to potential any decision making process on security research, technologies, measures and policies as well as providing assistance for the interpretation of data gained by polls and surveys. The small scale participatory method developed and tested by SurPRISE offers to integrate this efficient approach of citizen participation into future decision making endeavors, allowing to include the voice of citizens in specific settings, e.g. concerning individual new security technologies or particular environments.

Further potential impacts

- **Strategic impact:** SurPRISE provides a concrete framework to evaluate security solutions and technologies in context. It is of high relevance for taking diplomatic and policy decision related to security issues.
- **Impacts on competitiveness**: SurPRISE will allow security providers and developers to question their design, communication and marketing strategies. By means of critical thinking the project will help companies working in the area to identify those aspects of security solutions which actually provide added value to end-users.
- **Economic justification**: SurPRISE will offer guidelines to understand the drivers of insecurity and the ways to prevent it. This information will allow governments to distribute resources in a more efficient and comprehensible way. Security priorities will be addressed in a more efficacious manner without necessarily rising public investments.
- **Social objectives**: SurPRISE will improve social inclusion because it will highlight potential sources of discrimination, unintended consequences produced by the introduction of security solutions in problematic conditions, and many other aspects that threaten social cohesion inside the EU with respect to security issues.

Relationship with other projects and studies

SurPRISE made extensive use of relevant knowledge produced by on-going or recently concluded security research projects. FP 7 Security research projects were scanned for potential useful exchange of information and collaboration; special attention was paid to Cross-cutting missions projects within area 6 - Security and society. This activity was continued during project lifetime to identify further projects offering potential synergies with SurPRISE, including actively offered exchange of information with projects with (partly) overlapping objectives. Two projects were specifically relevant for SurPRISE: DESSI and SIAM. Part of the partners, including the coordinator, are also partners in DESSI - Decision Support on Security Investment. The coordinator is also member of Advisory Panels of different FP7 Security Research projects and has served as expert to ESRIF; these contacts were used to assist and enforce regular communication and interaction activities with relevant FP7 and national research projects as well as the dissemination and implementation of the decision support developed by SurPRISE. Close cooperation was conducted with the PRISMS and PACT projects, embracing the organization of a final joint international conference to support the dissemination of results to high level experts, stakeholders and policy makers.

3.2 Main dissemination activities

Dissemination activities comprise the following elements:

- Internet dissemination. SurPRISE website, giving information about objectives, methods and results of SurPRISE. The web-site also provides access to the public deliverables of the project and the information material to be used in educational or other contexts.
- Production of two Communication Packages to be used for presenting the process, methods and results of SurPRISE at conferences, seminars, workshops etc. and towards potential users of knowledge and participatory methods of the project. The packages include text based materials as well as audiovisual media
- Stakeholder and user workshops after the first project year and close to the end of the project, giving opportunities for the potential users of the results to discuss approaches, results, conclusions and recommendations .
- A final joint international conference with the PRISMS and PACT projects for the dissemination to high level experts, stakeholders and policy makers.
- Active press contact in order to attract attendance to the novelty of the research approach, in particular the large-scale participatory involvement of citizens, and the political meaning and importance of achieved results, and to communicate the SurPRISE project and the involvement of the EU Commission research into facilitating informed security policy-making.

- Scientific publications and presentations on the methods and results of SurPRISE.
- Information to public and political target groups through the networks of the partners, including towards the STOA Panel (Science and Technology Policy Options Panel) of the European Parliament, towards the members of the EPTA network (European Parliamentary Technology Assessment) and towards national security policy-makers inside EU.
- Interventions and presentations at high level meetings and policy relevant workshops, e.g. of the European Group on Ethics in Science and new Technologies (EGE) and FRONTEX.

3.3 Exploitation of results

A core exploitation activity is the promotion and support of the SurPRISE Decision Support System (DSS) for future uses in a variety of security related decision-making.

The SurPRISE DSS was developed in order to guide the process and record the data of small-scale events, it was successfully tested and used in the citizen meetings conducted in five countries by the SurPRISE consortium.

The SurPRISE DSS offers

- An innovative process for involving citizens in decision-making on security technologies;
- A framework for capturing both qualitative and quantitative data in one tool;
- Flexible content and process;
- User friendly interface;
- Translation module;
- Standardized process, enabling multiple events and comparable results.

The DSS is an innovative methodology and infrastructure for facilitating citizen involvement in processes on security related decision-making. It combines the deliberative participatory methodology of the SurPRISE project with a web-based workshop tool that guides the discussions, and provides a structured web-based framework for capturing the discussions at the tables, and at the same time records quantitative input about how participants vote.

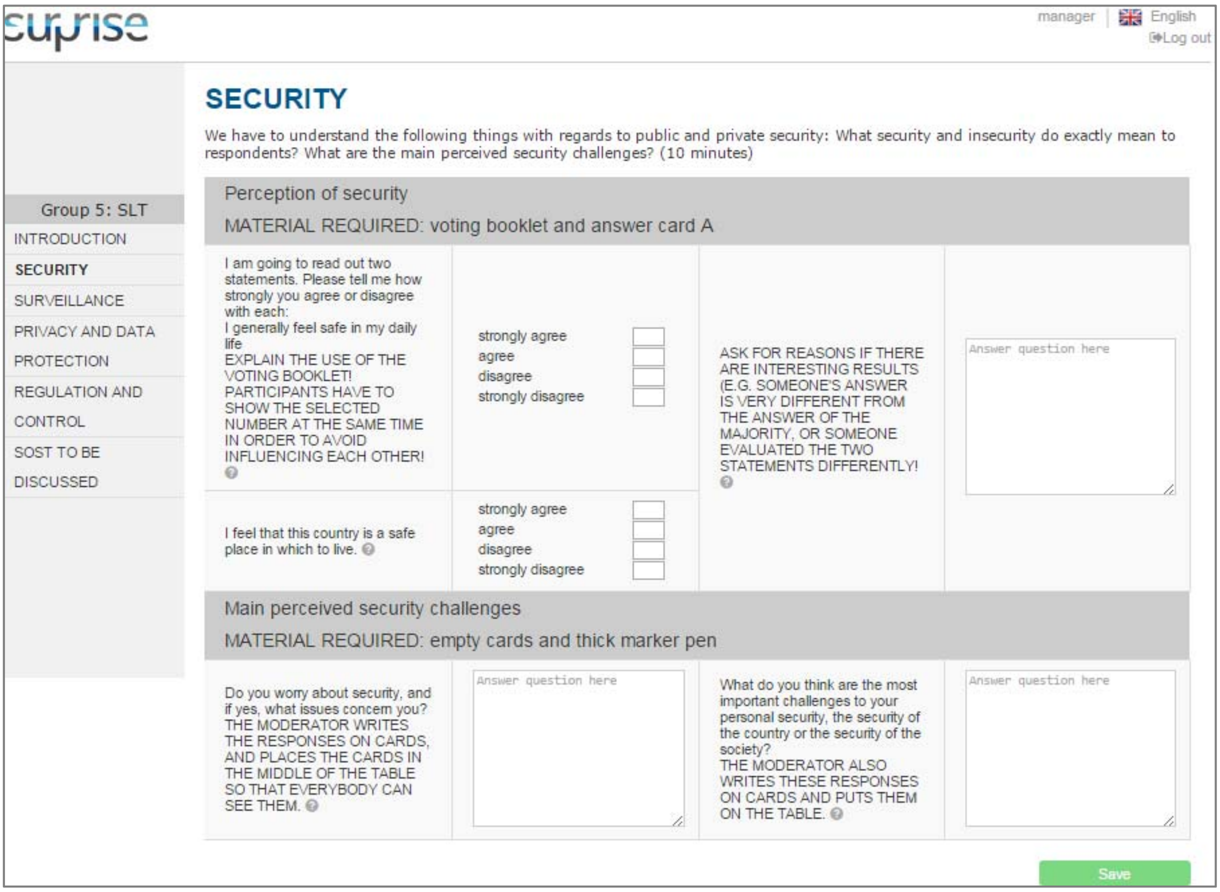
Because of the standardized procedure, the SurPRISE DSS enables users to conduct multiple events with comparable results, even in multiple countries and languages because of the translation module.

The SurPRISE DSS allows ample time for participants to form and express their own opinions and, on an informed basis, in cooperation to develop messages and recommendations for decision-makers. In this way, the SurPRISE DSS provides comprehensive, qualitative insights regarding citizens' attitudes to and evaluations of controversial issues and an opportunity for decision-makers to compare citizen's views with the views of other stakeholder groups. The DSS further provides quantitative data, which, provided sufficient sample size, allows for statistical analysis. The events run by SurPRISE DSS are divided into discussions rounds. An advantage of the tool is, that the results of each discussion round can be displayed immediately to the participants, thus it provides the opportunity of discussing and reflecting on interim judgments as part of the process itself.

Open Source

The SurPRISE DSS is an open source tool which means that it can be used in other deliberative, participatory processes involving security-related decision making. The user-friendly interface means that the tool can be easily customized in terms of content, structure and duration of the process. The simplicity of the user interface reduces the amount of tool-specific training necessary for the operators of the tool, thereby reducing the cost of the overall process; it is not, though, recommended engaging in the process without receiving some training or instruction in the SurPRISE methodology by a member of the consortium.

For more information on the SurPRISE project please visit the project website: www.surprise-project.eu Additional information on the SurPRISE Decision Support System and the other results of the SurPRISE project are available at www.surprise-project.eu/dissemination/research-results/



manager | English
Log out

Group 5: SLT
- INTRODUCTION
- SECURITY
- SURVEILLANCE
- PRIVACY AND DATA PROTECTION
- REGULATION AND CONTROL
- SOST TO BE DISCUSSED

SECURITY

We have to understand the following things with regards to public and private security: What security and insecurity do exactly mean to respondents? What are the main perceived security challenges? (10 minutes)

Perception of security

MATERIAL REQUIRED: voting booklet and answer card A

I am going to read out two statements. Please tell me how strongly you agree or disagree with each: I generally feel safe in my daily life EXPLAIN THE USE OF THE VOTING BOOKLET! PARTICIPANTS HAVE TO SHOW THE SELECTED NUMBER AT THE SAME TIME IN ORDER TO AVOID INFLUENCING EACH OTHER!	strongly agree □ agree □ disagree □ strongly disagree □	ASK FOR REASONS IF THERE ARE INTERESTING RESULTS (E.G. SOMEONE'S ANSWER IS VERY DIFFERENT FROM THE ANSWER OF THE MAJORITY, OR SOMEONE EVALUATED THE TWO STATEMENTS DIFFERENTLY!	Answer question here
I feel that this country is a safe place in which to live.	strongly agree □ agree □ disagree □ strongly disagree □		

Main perceived security challenges

MATERIAL REQUIRED: empty cards and thick marker pen

Do you worry about security, and if yes, what issues concern you? THE MODERATOR WRITES THE RESPONSES ON CARDS, AND PLACES THE CARDS IN THE MIDDLE OF THE TABLE SO THAT EVERYBODY CAN SEE THEM.	Answer question here	What do you think are the most important challenges to your personal security, the security of the country or the security of the society? THE MODERATOR ALSO WRITES THESE RESPONSES ON CARDS AND PUTS THEM ON THE TABLE.	Answer question here

Figure 12: Screenshot of the SurPRISE DSS workshop tool

4 List of Figures

5 List of Tables