"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

D 7.2 – Comparative report - Citizen Meetings

Lead Beneficiary: Medián

Author: Márta Szénay (Medián)

Due Date: October 2014

Submission Date: December 2014

Dissemination Level: Public

Version: 1

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

About SurPRISE

SurPRISE is a three-year Collaborative Research Project under the European Union Framework 7 Security Research Programme, running from 2012-15.

A core objective of SurPRISE is to re-examine the relationship between security and privacy. This relation is commonly positioned as a 'trade-off', accordingly infringements of privacy are sometimes seen as an acceptable 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. However, an emergent body of scientific work and public scepticism questions 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 is to identify criteria and factors, which contribute 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.

The work in the SurPRISE project is organised in eight[1] technical work packages. WP1 supports research activities by developing and establishing common project methodologies. WP2 develops a theoretical framing of criteria and factors influencing the acceptance and acceptability of security technologies, to be evaluated and tested in the empirical work done later in the project. WP3 identifies and elaborates options to shape security measures to comply with ethical and privacy requirements from a technical, legal and social perspective. WP4 combines the output of WP2 and WP3. It translates them into a testable empirical model, applied in large-scale participatory activities. WP4 develops the overall structure of the questionnaire and the supporting information material. WP5 organises and conducts large-scale participatory technology assessment events in nine European countries. These "Citizen Summits" involved on average about 200 citizens per country. Citizen summits are full day events with alternating phases of receiving information, discussing emerging issues in small groups, electronic voting on general aspects of the relation between surveillance and security and on specific surveillance technologies, and of developing recommendations from the citizens to policymakers. WP6 analyses the qualitative and quantitative data in depth and synthesises them to conclusions and recommendations, combining expert knowledge and citizens perspectives. WP7 applies the results and methods of the citizen summits to develop a decision support system, allowing the involvement of citizens in decision-making on security technologies and measures in small-scale participatory events. WP8 is devoted to dissemination to ensure information flows from the project to relevant bodies, interest groups, decision makers and the general public.

This report summarises the outcome of Citizen Meetings, the small-scale participatory events conducted in five countries within work package 7.

[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

Executive Summary

As part of the SurPRISE project, after the first series of participatory events, called "Large-Scale Citizen Summits"[2], five, three-hour long "Small-Scale Citizen Meetings" were organised during the summer of 2014 in Denmark, Hungary, Italy, Norway and Spain. In these five countries, a total of 190 participants gathered to discuss security, privacy and surveillance issues, talk about particular surveillance-oriented technologies, answer questions and formulate messages and recommendations towards decision makers and politicians. The main objectives of this second series of empirical research were to validate and supplement the results of the large-scale citizen summits and to test the web-based research design, called "SurPRISE Decision Support System" (DSS)[3] that facilitated the events.

Perception of security

The hypothesis whereby citizens who are more concerned about their security tend to perceive surveillance-oriented security technologies (SOSTs) as more acceptable, was not justified by the quantitative results of the large-scale empirical research. Two main reasons were detected:

- By exploring what security means for citizens, it was found that SOSTs, or the way they are used, do not often respond to the security challenges perceived by citizens. Moreover, citizens felt that the level of security threats does not justify the extensive, untargeted surveillance used for crime prevention;
- At the same time, a number of citizens fear surveillance, and think that, instead of improving security, SOSTs can decrease the feeling of security.

Security is a complex notion having different dimensions for citizens. On an individual level, **security is a subjective feeling of safety** often expressed by referring to a general absence of fear, worry and concern related to some form of physical, mental or digital attack against them or their loved ones or their property. It is also influenced by existential concerns and social problems. On a country level, citizens differentiate between **public security** that mostly covers petty, everyday crimes threatening the individual, and **national security** covering challenges that impact on society as a whole or a larger segment of it. While the state of public security strongly influences citizens' subjective feeling of safety, the state of national security is difficult to assess for them. Further, citizens rarely feel threatened by actual national security threats. Hence, when the perception of national security is not directly and strongly endangered, it does not have an effect on the subjective feeling of safety. As a consequence, a number of citizens are not ready to sacrifice their privacy for national security.

Privacy concerns and the core of privacy

Similarly to the large-scale results, a great number of participants were concerned that surveillance erodes privacy. They feared that people could lose values such as freedom of speech, anonymity and freedom.

Privacy was often described by participants as a well-defined or designated physical, psychological or digital **space** or **sphere** often surrounded by a real or virtual border, or it was grasped as a **possibility**, a **freedom**, a **capacity,** but first and foremost as a **right** to choose what is exclusively private.

Participants believed **there is a core of privacy deserving special protection**. Most frequently, the home and the family environment were mentioned as the core of privacy, but citizens often included personal connections, thoughts and communications, freedom of behaviour, sensitive data such as data related to political and religious beliefs, sexual orientation, information on health, banking and financial data and data regarding vulnerable individuals. For some, any information allowing another party to reach and harm a person, or cause loss or harassment, belongs to the core of privacy.

---

[2] See the national results in D6.1-D6.9 and the synthesis results in D6.10

[3] See the description of the SurPRISE Decision Support System in D7.3. *SurPRISE decision-support web-tool*

Surveillance and "I have nothing to hide"

In all five countries, opinions on surveillance were influenced partly by a lack of factual knowledge and partly by the presumption that SOSTs can collect any kind of information about an individual.

About half of participants expressed concerns about surveillance, while the other half were less worried. Positions ranged from moderate concerns coupled with a rational, cautious behaviour in order to protect privacy, to views bordering paranoia. Those who claimed not to worry about SOSTs often remarked that knowing about their surveillance sparked unease. Others expressed worries about the future. The reasons behind these concerns stems from uncertainties with regard to privacy protection, regulation and control, and the fear of completely losing control over these technologies and personal data. However, since surveillance cannot often be seen or felt, it generally does not have a direct effect on citizens' everyday life.

Besides the often cited "*I have nothing to hide"* reasoning of those who do not mind compromising their privacy in return for more security, another frequent argument was that *"My data is not interesting to anybody"*. Others expressed a sense of helplessness, saying, *"We are too powerless to do anything about it"*. Other opinions expressed resignation, arguing, "*Everybody knows everything*".

Perceptions of particular SOSTs

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

Security agencies

Participants often distinguished between those who **direct the whole systems** (perceived not in terms of individuals, but as authorities and institutions) and the **field operators**. They were often more concerned that the field operators, who have access to data, abuse information because *"they are humans*", and also because they are not sufficiently controlled or trained, those employed in such positions are not the most suitable and most trustworthy, etc.

The **visibility of field operators** seems to influence the way in which citizens evaluate trustworthiness. Whenever the operators are more "visible", such as in the case of CCTV systems, citizens' (positive or negative) evaluation of trustworthiness focussed on the individuals. Whenever the operators are hidden (e.g. in case of DPI), they tended to evaluate the authorities, and their assessment varied depending on the authorities' general image. Participants often said that they trust security agencies significantly more than (profit-led) private companies. Such **distrust of private actors affected the evaluation** of the behaviour of security agencies when they use SLT.

Security agencies (and other public authorities) are seen as trustworthy when using SOSTs if:

- people have positive personal experience with them;
- no abuses have been associated with such institutions;
- more information is made available about the collection, storage and use of personal information;
- their actions and operation are transparent;
- they do not have unfettered discretion;
- they are controlled;
- the employees of the institution who have access to the data are well trained, do not abuse their power, are not corrupt and are well paid (and therefore are less influenced by corruption).

Regulation, control and legal safeguards

An important element of acceptability lies in how the deployment of technology and data-processing operations are regulated and controlled, as well as what kind of legal safeguards protect citizens against abuses.

The hypothesis formulated following the large-scale research, that **a great number of citizens lack sufficient knowledge** in regard to this field, was confirmed by the small-scale research, supplemented with the observation that even those who believed they knew quite a lot had a superficial, and often incorrect, knowledge. Owing to this fact, it was not surprising that a number of participants felt that while too much effort and resources have been invested in developing these technologies, there was little endeavour to establish appropriate information campaigns on how these technologies work; how they are, and should be regulated and controlled; what the authorities' rights and obligations are; and what citizens' rights and obligations are.

To be sure, the "information hunger" observed during both series of participatory research was partly generated by the fact that the participatory research methodology itself drew attention to the relevance of knowledge, however, the lack of information is evident.

The majority of citizens did not demand a direct say in the regulation of SOSTs, leaving this work to professionals, on the condition that the results should be communicated to the public in a comprehensible language. However, they did succeed in formulating some general important requirements:

- There should be an active, permanent external control over security agencies that use SOSTs by a body or organisation, which should be independent from politics and industrial and commercial interests, to ensure accountability and to avoid unfettered discretion;
- It should be made possible for citizens to control their own personal data collected through SOSTs, upon request;
- The necessity, adequacy and proportionality of use of SOSTs should be assessed;
- Citizens should be informed about lawful data-collection and -processing operations and existing legal safeguards;
- Legal safeguards should also be at hand when private companies use SOSTs.

While citizens required transparent and strict control mechanisms, another opinion also appeared: safeguards cannot be so bureaucratic as to make it difficult for public security authorities to do their job. Moreover, regulation should be SOST-specific, not general. In the case of technologies perceived as less intrusive, such as CCTV, fewer safeguards than with technologies such as DPI may be sufficient.

Trade-off through the citizens' eye

Participants were asked to reflect on the trade-off concept, envisaged as stating that privacy and security are incompatible and one can be increased only at the expense of the other. Opinions were divided on this topic.

Those who accepted the trade-off approach tended to frame it in the SOSTs context, i.e. when evaluating the relationship between privacy and security, they thought exclusively about surveillance technologies. They felt the model is valid, because they thought that surveillance *per se* entails the infringement of privacy. For them, the biggest challenge was finding a balance between the two. However, even those who embraced the model often thought that safeguards must be put in place for any personal data collected.

Those who were unsure held the view that the trade-off between security and privacy is not necessary in several cases, such as when clear and fair rules are in place; when the SOST is not deemed to damage privacy; in particular situations, when it is worthwhile sacrificing privacy; if SOST is used not for prevention but after the event. In addition, they often thought that a trade-off is not necessary in the long run, because, for example, better quality of life could lead to more security without affecting privacy, and it would no longer be necessary to control people to ensure security even if it may be necessary to give up some privacy in the short term.

The main argument of **those who rejected** the trade-off model was that security can be improved by methods that are not based on surveillance technologies. Another explanation was that a society can be secure and at the same time protect citizens' right to privacy. They thought that the development of security technology should take into account both respect for privacy and data-protection legislation.

Some rejected the model by arguing that fear and insecurity is not real but instigated, and public authorities may have an interest in instilling fear in citizens in order to persuade them to waive some of their rights, such as privacy.

Alternatives

An interesting result of the large-scale citizen summit was that, while the acceptability of SOSTs as tools to improve national security was relatively high, a strong majority of participants preferred alternative security solutions. The small-scale citizen meetings tried to solve this contradiction.

The fact that people would like at least to minimize the negative consequences of mass surveillance strongly contributed to the preference for non-surveillance-based security solutions. However, the most likely reason behind the apparent contradiction was that a great number of participants handled the question on two different levels: in the short term and in the long term. They thought that, **in the long term, technological solutions would not improve security**. Rather, the root of the problem should be addressed with education on social, civic and moral responsibility; an increase of solidarity, social cohesion and social wellbeing (including more economic security); and an improvement of the social safety net, fight against poverty and social exclusion, etc.

Such changes, especially because of their timeframe, cannot help to solve immediate security problems. This is why citizens accept the use of SOSTs, although not unconditionally. They think that technological, surveillance-based solutions play a role in improving security in particular situations. In addition, there are technologies, primarily DPI and also biometric identification, which cannot be substituted with solutions like more police, better public lighting, more civil guards, neighbourhood watch schemes or similar measures that were mentioned as possible alternatives in the shorter term.

Those who overlooked alternative solutions often referred to the fear of excessive cost in terms of financial and human resources.

Another attitude concerned the fact that the application of the technology is problematic, rather than the technology itself. The same challenge applies to alternatives, e.g. police patrols on the street could also increase insecurity if implemented incorrectly.

Recommendations

The focus of the small-scale events was to provide the opportunity for citizens to formulate their demands, messages and recommendations for politicians with regards to SOSTs, and to contribute their opinions to a decision-making process. Their most important claims are summarised in brief below (however, the detailed report that follows this executive summary is a richer repository of citizens' requests, suggestions and ideas for decision makers):

- Proportionate and targeted use of SOSTs should be ensured instead of mass surveillance;
- Deployment and use should be strictly regulated and the use should be transparent under intense, independent (also from politics) outside control;
- Information should be provided on surveillance and its control in a comprehensible language;
- Supplementary use of "machines" in addition to humans is acceptable on the short term, but in the long term, the root of the security challenges should be remedied;
- Surveillance should respect privacy and civil liberties, and technology development should also take this into consideration;
- Public discussions and open debates about the use of these technologies are needed;
- People should be educated to use surveillance technologies in a more responsible and cautious manner at school.

Validation

The main results, including the quantitative data of the small-scale research, were identical to the outcome of the large-scale events, and validated the main research results, supplemented them with a few additional aspects, and helped to find explanations to a few apparent contradictions. At the same time, the similarity of the main findings of the two series of participatory events justifies the relevance of the small-scale research design and the SurPRISE Decision Support System that facilitated the five citizen meetings.

1. Introduction

As part of the SurPRISE project, two series of participatory events were organised. These events were public meetings where citizens gathered to have face-to-face discussion about the Surveillance Oriented Security Technologies (SOSTs).

The first series of participatory events, called "Large-Scale Citizen Summits" were organised in nine European countries in the first quarter of 2014 with about 200 participants in each country. In addition, five countries out of these nine, Denmark, Hungary, Italy, Norway and Spain organised a "Small-Scale Citizen Meeting" during the summer of 2014.

The main purpose of the small-scale research was to channel and test the knowledge and experiences developed throughout the project, and to transfer it into a participatory small-scale decision-support system, which helps citizens to articulate their requirements, needs and recommendations for politicians with regards to surveillance technologies. A part of the tasks was to test this decision-support system, which was based on a modified methodology of the large scale research, adjusted to explore citizens' concerns about security challenges and opinions on the given technological answers, in smaller participatory settings, using much less time and expenditure.

Due to its small-scale nature, the focus of the research was not on the collection of quantitative data, but on obtaining more in-depth understanding of citizens' perceptions, attitudes, demands and claims. This second series of empirical research validates and supplements the large-scale results published in nine national reports and a synthesis report of D6.1-D6.10, and intends to inform deliverables D6.13 policy papers and manuals and D2.4, key factors affecting public acceptance and acceptability.

This report is based on the national reports of the five countries published in D7.1.[4] In addition, it presents the results of individual and group ratings, which – owing to the small national sample sizes – can only be statistically interpreted on the level of the total sample of all five countries.

The first chapter summarises the main objectives of the small-scale research. The following three chapters discuss in greater depth how citizens understand the basic concepts of the research: security, privacy and surveillance. Chapter 5 summarises the perception of the five SOSTs discussed, in more details. Chapter 6 summarises opinions on security agencies, and Chapter 7 addresses the topics of regulation, control and legal safeguards concerning the use of SOSTs. Chapter 8 presents the reflections of citizens on the trade-off concept, i.e. that privacy and security are incompatible things: the one can be increased only at the expense of the other. Chapter 9 is about the opinions on non-surveillance-based and/or non-technological, possibilities that can be considered as alternatives to SOSTs. Chapter 10 provides an overview of citizens' messages and recommendations towards European decision makers. The last chapter (Chapter 11) details how participants and table moderators evaluated the event at the end of the meeting.

[4] Marianne Barland, Jacob Skjødt Nilsen, Vincenzo Pavone, Maria Grazia Porcedda, Elvira Santiago, Márta Szénay, Teresa Talò, D7.1 - *Report on decision support testing* (five national reports), 2014. *http://surprise-project.eu/wp-content/uploads/2014/10/SurPRISE_D7.1-Report-on-decision-support-testing.pdf*

2. Objectives and methodology

The main objective of this second series of empirical research, called small-scale citizen meetings, was to validate and supplement the results of the large-scale citizen summits:

- by further investigating factors and criteria influencing citizens' opinions and attitudes towards SOSTs;
- by assessing citizens' perception on two additional technologies, drones and biometrics, which were not included in the large-scale research;
- by examining questions raised in earlier stages of the research in greater depth.

The five citizen meetings were based on a methodology similar to that used for the large-scale events, but adjusted to smaller participatory settings, thus saving time and money. A new and innovative, web-based research design, called "SurPRISE Decision Support System" (DSS)[5], helped to facilitate the meetings and involve citizens into the process of technology evaluation. Moreover, note-takers were able to record the main points of the discussions as well as citizens' recommendations and messages in real time in the DSS.

The total sample of this small-scale research consisted of 190 participants who discussed the raised topics in smaller groups sitting around tables. A total of 26 tables were organised: five in each county except in Italy, where there were six tables[6]. Experienced moderators led the table discussions. Each event lasted three hours, and was divided into two 1.5-hour discussion rounds. After the first, SOST-neutral session, each table discussed a different SOST out of the five included in the assessment: deep packet inspection (DPI), smart CCTV, drones, biometrics and smartphone location tracking (SLT).

The small-scale research was basically a qualitative research, and although questions were also developed for individual or group evaluation, answers can only be statistically interpreted on total sample level owing to the small national sample sizes. When evaluating this data, it is important to remember that the main purpose of the questions was not primarily to gather statistical data but to stimulate the discussions and the group work, and to validate the results of the large-scale research. In addition, the total sample cannot be regarded as a representative sample of the European citizens or even of the five countries involved, despite the fact that the organisation of participants endeavoured to reach a representative mix of citizen. Quotas were set for gender, age and education according to national statistics[7]. Nonetheless, statistics from the close-ended questions provide interesting quantitative background to the qualitative findings.

The detailed research objectives/questions below were formulated on the basis of the model developed in "WP2.2 - Draft report on key factors", the theoretical background analysis completed in "WP3 - Exploring the challenges", as well as the preliminary results of the large-scale citizen summits:

- What does security and insecurity exactly mean to respondents; what are the main perceived security challenges?
- How do citizens connect security issues/threats to surveillance-based security measures?
- How do citizens perceive surveillance in general, and with regard to SOSTs in particular?
- How does surveillance itself affect citizens' everyday life, if at all?
- How do people understand privacy and data protection?
- What is, should it exist, the core of privacy that should be protected the most?
- What do citizens know/believe about the legal framework and control relating to surveillance-based security technologies, and what kind of information/communication do they require?
- What kind of legal safeguards do citizens desire, and how do safeguards contribute to the acceptability of SOSTs?
- How can the connection between trust and the fear of abusing power with regards to security agencies that employ these technologies be better understood?

---

5 See the description of the SurPRISE Decision Support System tool in D7.3. *SurPRISE decision-support web-tool*

6 Owing to the successful organisational work in Italy as well as the unexpectedly low drop-out rate, it was possible to organise an additional, sixth table. Smart CCTV was discussed at this table.

7 See the detailed description of methodology in D1.4. (Emma Christiani Skov,, Jacob Skjødt Nilsen: *Method description decision support test cases*)

- What do people mean by effectiveness as well as intrusiveness in regard to security technologies in general, and the discussed SOST, in particular?
- What is the reasoning behind the acceptance and rejection of the trade-off approach?
- Does the preference for alternative solutions simply represent votes against surveillance, or do citizens have particular ideas and requirements for supplementing the surveillance-based solutions in general, and in regard to the discussed SOSTs in particular?

An information magazine sent to participants in advance of the meeting supported informed discussion. The magazine was a re-edited, adapted and updated version of the one used during the large-scale event supplemented with new chapters on drones, biometrics and alternative solutions.

3. Security

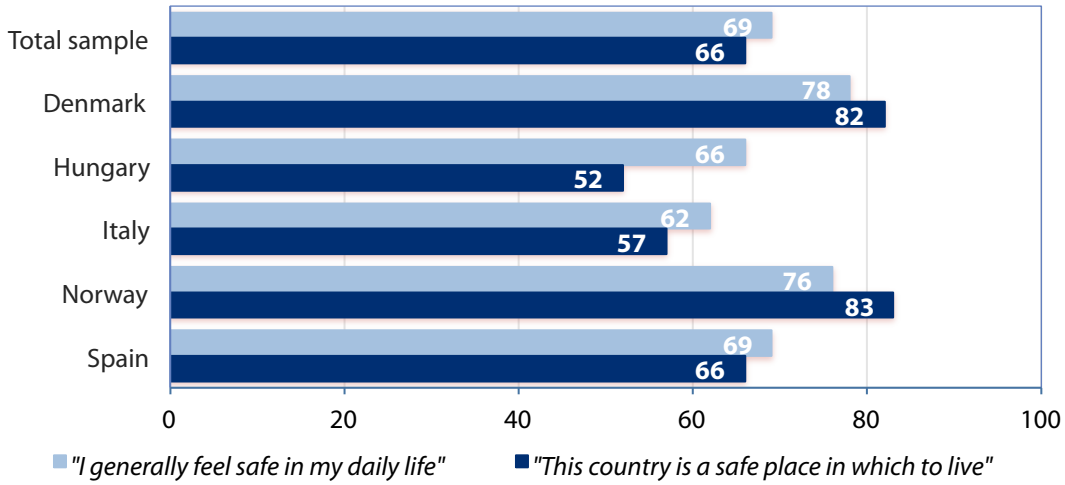
The hypothesis, whereby citizens who are more concerned about their security tend to perceive surveillance-oriented security technologies (SOSTs) as more acceptable did not seem to be justified by the quantitative results of the large-scale empirical research. In addition, rather significant differences were found in the perception of security between the nine countries that participated in the project. Therefore, with the help of the small-scale research, we wanted to better understand how citizens in the different countries of Europe define or interpret security and insecurity, and how they connect it to the new surveillance measures.

3.1 Perception of security and insecurity

Based on individual answers to questions about the perceived level of personal safety and the security of the participants' country, exactly the same national differences could have been observed as in the large-scale research (Figure 1):

- Again Italian participants felt the least safe in their daily life, and Hungarians followed them. Then came Spanish people, while the general feeling of safety was significantly better in Denmark and Norway than in the other three countries.
- When participants evaluated their countries from the point of view of security, the only change in the above order was that Hungarians had the most negative opinion about their country in terms of it being a safe place to live, just as in the large-scale research. Again, the evaluation given by Scandinavian participants was significantly better than that of the other three.
- Another similarity with the large-scale results is that, in the three Central and Southern European countries, the perception of security was better from an individual point of view compared to how people evaluated their own country's security. This was again not the case for the two northern countries, where the security of the country received better evaluation than personal security.

Figure 1
Perception of personal safety and the security of the country
(averages on a 100-point scale[8]; the higher the average the better is the perception of safety/security)



Cultural, political and economic differences evidently are responsible for the national differences in regards to the perception of security both on individual and on country level. However, despite these differences, with both series of data collection (the large- and the small-scale), we found that the majority of the European citizens do not have everyday problems with either their personal security or

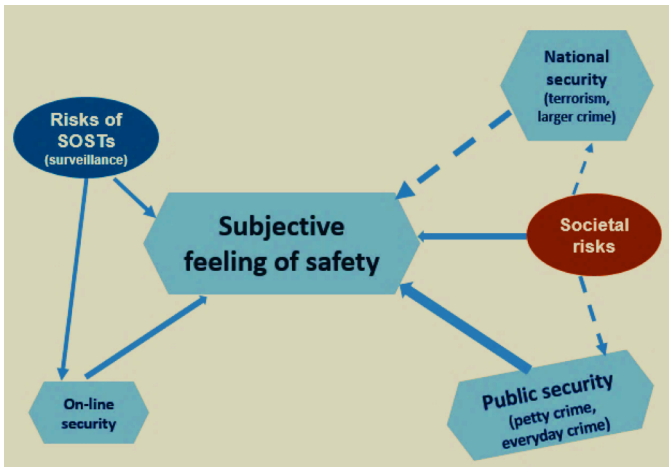
[8] The original four-point scale was projected to a 100-point scale, and then the average scores were counted in order to better visualise the differences in the answers.

with the security of their country. However, this simple statement based on statistical data covers the complexity of the concept of security and its diverse interpretation by citizens. In the small-scale research, we had the opportunity to examine this question in greater depth.

Security is a complex notion having different dimensions for citizens (Figure 2):

- On an individual level, for the large majority, security is a ***subjective feeling of safety*** often expressed by referring to a general absence of fear, worry and concern for some kind of physical, mental or digital attack against them, their loved ones or their property. However, the subjective feeling of safety also influenced by so-called "*societal risks*" that involve fears such as losing one's job, becoming ill, etc. When citizens assess SOSTs, it is natural for them to take into consideration how the particular use of these SOSTs can enhance their subjective feeling of safety.
- On a country level, participants often differentiated between the national security and the general state of public security of the country. ***Public security*** refers mostly to petty crime or everyday crime, such as physical attack against an individual or an individual's property, including burgling someone's house, stealing someone's car or bike from the street, pickpocketing on public transport, etc. The perceived state of public security, based on one's own or others' experiences and media news, strongly impacts the personal feeling of safety. SOSTs are accepted more if their effect on public security is justified in the eyes of citizens.

Figure 2
Perception of security



- ***National security*** is a rather abstract notion for citizens, and covers such challenges as possible military or terrorist attacks against the country, financial manipulation and other serious, international crimes such as drug trafficking and illegal immigration, that is to say, threats that can affect the whole society as a system, or at least a larger segment of it. National security is difficult to assess for citizens. In addition, participants generally think that their country is not endangered by a military or terrorist attack, and consequently rarely feel threatened by actual national security threats. Hence, although at the theoretical level, they regard national security as something that should be protected in any case, they are not ready to sacrifice their privacy for it. This is also the case even for Norway, where the memory of the terrorist attack of 2011 is strong and was mentioned several times during the discussions, and for Denmark, where participants thought that the military involvement of the country in the war against terrorism increases the possibility of a terrorist attack against the country. When the national security is not directly and seriously endangered, the perception of national security does not have an effect on the subjective feeling of safety. The broken line in Figure 2 refers to this "theoretical" connection.
- ***Societal risks*** involve existential concerns (e.g., losing one's job, becoming ill, etc.), worries associated with social problems such as fear for the welfare state, worries about the growing divide between the poor and the rich (e.g., giving rise to subsistence crime), concerns about the state of the social safety net, etc. A number of these societal risks listed by citizens as security challenges have a direct effect on the subjective feeling of safety, but also can have an effect on public and national security, and through this, an indirect effect on the subjective feeling of safety.
- ***On-line security*** appears with regard to the use of the internet, but as internet penetration is growing and the use of the internet becomes part of the life of the great majority of people, on-

line security also has an effect on the subjective feeling of security, although currently this effect is much weaker than that of the state of public security.

- A number of participants spontaneously raised the ***risk of the use of SOSTs*** among security challenges, especially in the Scandinavian countries and in Spain. They think that surveillance-based security solutions also can decrease the feeling of security, especially the perception of on-line security. Many of the participants mentioned the revelation about NSA mass surveillance on a global scale as one of the reasons for these concerns.

Personal experiences, or experiences of other people, play a major role in the perception of security. In Denmark, for example, a number of the participants, especially young people, mentioned that they did not have any experience of unsafe situations, and emphasised that they rarely feel insecure in public areas, even at night or when walking alone. In other countries, citizens listed several worries, such as being accosted returning home late at night, having their home burgled, having their car or bike stolen or having their pockets picked.

People, especially those living with their families, often emphasised that they worried less about themselves but more about the possibility of their children and loved ones being attacked.

Occasionally, the media was blamed as being responsible for increasing the sense of insecurity in people by allowing negative news to dominate content.

Part of the perceived security challenges were the same for citizens living in different countries, but several country-specific differences could be identified and explained by national economic, social, political and cultural characteristics. A crucial difference between the countries involved was how important the subjective feeling of safety was compared to the interests of the total community of the country, and, consequently, how important participants' direct personal interest was when they evaluated a particular SOST. For example, in Hungary, even homeless people were seen as source of danger (e.g. they can spread illnesses).

In contrast, in countries like Norway and Denmark, participants tended to respect the interest of the whole society more, and tended to evaluate the use of SOSTs from a wider societal point of view. They feared the negative effect of surveillance on society more than on themselves.

3.2 The technological answer

The hypothesis, "*the more that citizens are concerned about threats to their security, the more likely they are to find SOSTs acceptable*"[9], was not substantiated by the large-scale research. Based on the discussions of the small-scale research, the main reasons can be summarised as follows:

- SOSTs, or the way they are used, often does not respond to real security needs and the security challenges perceived by the citizens, and
- A number of citizens fear surveillance and think that instead of improving security, SOSTs can decrease the feeling of safety.

Despite this, participants saw a lot of positives in the use of these new technologies, and could mention several examples or situations where surveillance is both appropriate and necessary. However, they objected to unfocused, exaggerated, and disproportionate observation, as well as surveillance that intrudes into a certain segment of their privacy belonging to the so-called "core"[10], such as their personal communication or their intimate sphere. They generally accepted the use of SOSTs if the observation is targeted, has an effect on their subjective feeling of safety, when the technology can actively save lives, and the deployment and use is well regulated, controlled and transparent.

Chapter 6 contains more details with regards to the appropriateness and acceptability of the five particular surveillance technologies that were included in the research.

[9] See D4.1 "List of hypotheses"
[10] See Chapter 4.3 "The inviolable core".

4. Privacy

4.1 Interpretation

Despite the fact that the translation of the English word "privacy" has a slightly different meaning in different languages, the interpretation of privacy was basically similar in the five countries.

Citizens tried to explain what privacy meant for them by using different approaches:

- A **physical, psychological and digital space or sphere**
  - Privacy primarily means some kind of personal space related to intimacy, most frequently the **home**, often described as *"Privacy starts where my home is";*
  - There is another important borderline: within this are the **relationships** with family members and friends (who they are, what the relationship with them is);
  - Some participants drew another borderline around their body, sometimes referred to as their *"**aura**"* or *"shell"*, giving a greater emphasis to their body as part of their privacy; and
  - Citizens who use the internet intensively saw a part of the **digital sphere** as belonging to their private sphere, where they can hide their identity and activity if they choose.
- **A possibility, freedom or capacity** to choose what is exclusively private:
  - what to share with others, whether these others are friends and family, the government, co-workers or private companies;
  - what to disclose;
  - which data is public and which is not;
  - who, if anyone, should have information about and knowledge of their private activities;
  - with whom to share the physical sphere, their thoughts and emotions; and
  - with whom to communicate.
- **A (fundamental) right** (an important element in a democracy):
  - to be anonymous,
  - to be left alone in both physical and digital space;
  - to act and think freely; and
  - to behave according to personal belief.
- Some saw privacy as a **means of maintaining the balance of power** between the state and citizens. They emphasised that information is power, and information can be manipulated against citizens, and it can hurt them.
- **Control** over personal information and to know who collects and stores it;
- **Data protection** is also part of privacy:
  - confidentiality of personal data, especially sensitive data such as communications, habits, religion, political thoughts, sexual orientation and healthcare data**;**
  - largely due to the spread of these new technologies, more and more people have started to include personal and contact data (e.g. phone number, email address, credit card number, passwords) as part of their privacy;
- Something confidential, secret**,** something that a person does not divulge to anyone.

There were participants who thought that **the notion of privacy is in a state of constant change** and that **the private sphere is decreasing** with the increasing use of electronic communication. People seemed reconciled to the fact that, through certain internet activities, a part of their world is becoming irrevocably visible.

Many also expressed a feeling that the **public sphere is moving increasingly into the personal sphere**. As a consequence, participants perceive privacy to be reduced towards a narrower definition and into a narrower space, both spatial and mental.

4.2 Privacy concerns

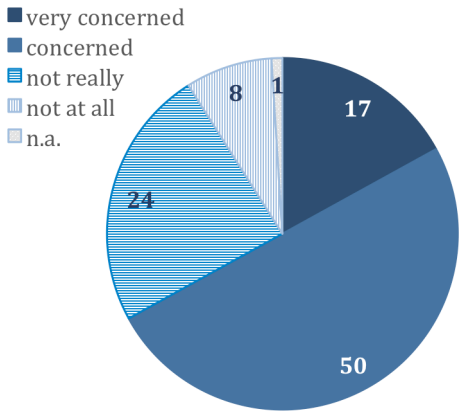
A great number of participants were concerned that surveillance erodes privacy (Figure 3). They feared that people may lose rights such as freedom of speech, anonymity and freedom. Some participants identified our digital society as one of the reasons for this. They thought that when we leave digital traces everywhere, it will become more and more difficult to protect privacy. The revelation of NSA's surveillance practices was worrying for the participants, as they saw this as an example of a state's abuse of power.

The transfer of data between countries was also worrying for some of the participants. Even those who were aware that there are supervisory bodies, feared that these bodies do not have the genuine power or resources to correct wrongdoings.

In less individualistic cultures such as in Denmark, citizens expressed more concern about other people's privacy, stating that while they themselves may not be the target of mass surveillance today or in the future, they still have concerns.

Privacy concerns were very high in the two Scandinavian countries, while they were more moderate in the other three. Many agreed that it is important to be concerned about privacy, but we do not have to exaggerate it. These citizens pointed out that using new technologies involves learning, and it is necessary to acquire sufficient knowledge to be able to use these technologies with caution.

Figure 3
"How much are you concerned, if at all, that the use of SOSTs are eroding your privacy?"
(percentages; individual answers; N=190)



Some of those, who did not worry that their privacy will be compromised, added that this did not mean that surveillance did not disturb them.

There were a few sceptics among participants, who did not worry about privacy because they regarded privacy as a "*non-existent*" "*utopia*".

There were participants, who said that they did not worry today but that they worried about the future development of these technologies. Concerns for the future often appeared during the discussions. Citizens were anxious that legal regulation cannot keep pace with technological development. And they also worried about themselves, the general public, who would not be able to keep pace with such rapid technological development. The participants thought it would be even more difficult to uphold values such as freedom of speech in the future.

When discussing the bodies that use surveillance, some of the participants said that they were not that concerned about the authorities and security agencies, but that they felt greater concern about the surveillance carried out by private and commercial bodies.

4.3 The inviolable core

The following were mentioned as the part of privacy that should be protected the most:

- the home and the family environment (this was mentioned most frequently)
- everything concerning people's intimate sphere
- personal connections
- personal thoughts
- personal communication (oral and written by letter and email, and also communications with doctors/psychiatrist)
- freedom of behaviour
- sensitive data (such as political and religious beliefs, sexual orientation, information on health, and personal identifiers (such as the social security number was mentioned in Norway)
- banking and /or financial data

- for some, all types of data through which a person may be reached or in some way harmed, or all the information with which harm, loss or harassment may be caused to someone
- a few people mentioned data regarding vulnerable individuals (children, people with health problems, foreigners) and felt that children should be especially protected from the negative effects of these technologies

Furthermore, there were participants who stated that the inviolable core of privacy should be such that fundamental rights and the possibility to act freely should be guaranteed.

5. Surveillance

5.1 Awareness of what kind of information is gathered

In all the five countries, participants seemed to have only a vague idea, and lack factual knowledge, about what information is actually gathered by SOSTs. They tended to assume that every aspect of one's personal life is accessible by these surveillance-based technologies. Those who tried to give a more precise answer, often provided examples such as location data, online activities, everyday and consumption habits, and personal connections and political views.

There were participants, who were astonished to learn how much information can be gathered about them partly for national security, and partly for other purposes.

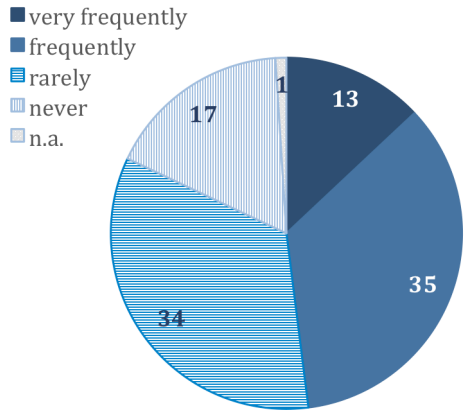
The use of Facebook and the internet provided an analogy that enabled people to better understand that a lot of information about them is stored in several databases. Similarly, they realised how many things can be put together about them from the traces they deliberately leave on the internet, and from data collected by SOSTs.

Some were concerned about new technology enabling collection of information that one previously could prevent, others realised or supposed that this data might also be used in a way they would not like or could not imagine.

5.2 Effect of surveillance on everyday life

Opinions were divided with regards to the effect of surveillance on everyday life. About half of the participants expressed concerns about surveillance, while the other half were less worried (Figure 4). Positions ranged from no or moderate concerns, coupled with rational and cautious behaviour in order to protect privacy, to views bordering paranoia.

Figure 4
"How frequently, if at all, do you worry about the use of SOSTs in your daily life?"
(percentages; individual answers; N=190)



Even those who claimed not to worry about SOSTs remarked that knowing about these surveillance activities sparked **unease**, and a great proportion of those who accepted the use of SOSTs expressed **worries about the future**. The rationale lies in the uncertainties with regard to privacy protection, regulation and control, as well as the fear of completely losing control over these technologies and personal data.

There were citizens who saw surveillance as a **tool in the hands of the authorities against citizens.**

However, since **surveillance can seldom be seen or felt**, it generally does not have a direct effect on citizens' everyday life, and the active avoidance of the surveillance conducted by these technologies only characterises the minority. However, several people had a feeling that they "should" do something, but a general lack of awareness and knowledge made them passive. We have to remark here, that **if there is a trust towards these technologies and their users, citizens expect their privacy not to be infringed even when they are not actively fighting intrusion**.

The following attitudes and arguments were observed in the discussions explaining how citizens accept or try to live with surveillance:

- **Rational behaviour**: acceptance of the fact that surveillance exists, trying to behave rationally, and protecting their privacy as much as they can.

  This behaviour was often not a conscious protection against threats and abuse of their privacy but was a general precaution, which becomes a habit (e.g., not using credit cards on the

internet, using cash instead of a credit card to avoid fraud or to protect consumption habits, stopping use of, or not registering on, social media or carefully selecting what to upload, occasionally leaving the mobile at home, using different service providers for different things, using different browsers for different searches, etc.)

- ***"I have nothing to hide"*** or "*Only criminals or those who have skeletons in the closet have to worry about surveillance*" were frequent reasoning of those who did not mind compromising their privacy in return for greater security.
- **Personal data is not interesting to anybody** *("We are such little things." "They want to observe others not us.")*

  This was a way to rationalize or "explain away" the use of surveillance to the man in the street.
- **Helplessness/ vulnerability**: *"We are too little to do anything against it."*

  This attitude was especially strong in Hungary. Perhaps the main reason for this feeling of helplessness comes from the recent past, when people became accustomed and were socialised by living under strong state surveillance with a weak civil sphere.
- **Resignation**: *"Everybody knows everything."*

  This attitude expressed that we cannot do anything about surveillance, not only because we are not able to represent our interests, but because everything is in vain.
- **Convenience:** People often felt they do nothing against surveillance because this would result in bothersome changes in their everyday life.

6. Perception of five technologies

In the second discussion round, each table discussed a different one of the five SOSTs involved in the technology assessment. In this section of the citizen meeting, open discussions and formulation of common messages and recommendations were given a greater emphasis. The following attributes were discussed in relation to each SOST: positives, negatives, effectiveness, intrusiveness, acceptability[11] security agencies and legal safeguards, the trade-off and alternatives. With the exception of "positives and negatives", at the end of each sub-discussion, participants voted as a group about the question that introduced the phase. Citizens were able to follow what was recorded in the Decision Support System (DSS) [12] that facilitated the event on a second screen, and hence they could read the main points they raised in the open debate, and could control the formulation of their recommendations and messages.

The figures provided in this chapter contain the results of group-ratings, thus show some kind of average opinion of the participants belonging to the same table. As each technology was evaluated only by 5-6 groups, despite of the fact that these evaluations represent the opinion of 30-40 participants, cannot be referred in the analysis as statistical data. They provide interesting illustration of the group work, and often support the main findings based on the discussions behind these ratings.

6.1 Deep packet inspection

Internet surveillance by deep packet inspection proved quite a complex and difficult technology to grasp, but the revelations about NSA surveillance programme have put this on the agenda in all the five countries.

Figure 6
"Does the use of DPI improve the national security and your personal feeling of security?"
(number of groups that selected the answer)

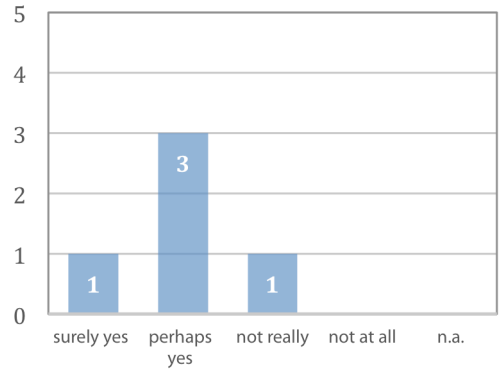
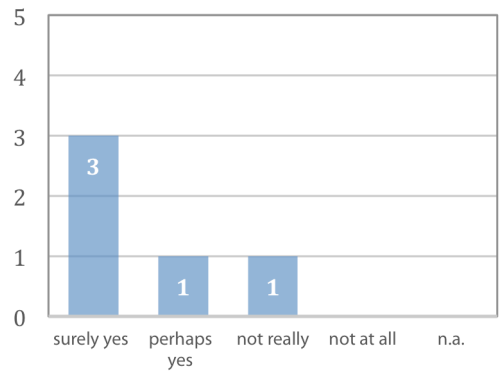


Figure 5
"Do you regard DPI to be intrusive to privacy?"
(number of groups that selected the answer)



Besides its role in maintaining and protecting digital infrastructure, participants saw some national security advantages in the use of this measure in intelligence and crime prevention and in targeted surveillance of suspects of serious crimes. However, participants thought DPI to be highly intrusive to privacy when it is used as a general tool for mass surveillance, and regarded surveillance by this measure as excessive and not at all reasonable. They feared the exaggerated and disproportionate surveillance carried out by DPI in a completely invisible manner. The following negative effects were raised most frequently:

- ❖ it harms freedom of expression, because the feeling of being observed also affects the way that people think;

[11] Acceptability was asked on an individual basis, but it was suggested to include as a separate dimension in Chapter 12.2.
[12] See the detailed description of the Surprise Decision Support System in D7.3.

- it has the potential to harm democratic freedom (can be used for censorship of internet content as well);
- citizens worried that data and information collected by DPI could be manipulated, modified, or interpreted out of context; and
- the security of data storage was also an issue.

Another negative interpretation of DPI was the possibility that minors may become involved. Citizens thought that DPI, similarly to smartphone location tracking, based on the unique identification number of the device, makes it theoretically possible for the user to be identified.

A number of participants suggested defining and restricting the fields and cases when DPI is permitted to be used, adding that its acceptability is strongly context related, and they could only judge the technology on a case-by-case basis. Owing to this fact, a number of citizens could not answer the generalised question whether they support the use of this SOST. Acceptability also depended on how "just" the government is and if fair and effective regulations are in place. They thought that it may be a useful tool if it is handled with legal and judicial authorisation.

There was a general criticism among the participants that deep packet inspection is too loosely regulated and that there are too many grey areas for it to work in a non-intrusive manner. Participants believed that clear boundaries had to be drawn to limit the use (e.g., by governments) of such a potentially intrusive technology.

They thought that it is necessary, as well as difficult, to establish a legal framework that regulates the use of this technology at national or EU level. In some countries, citizens were also concerned about private bodies using the technology, and that this would lead to their personal information becoming a commodity.

6.2 Smart CCTV

With regards to the intensity of using CCTV cameras by security agencies, the two extremes were represented in the sample by Norway, where security cameras are almost exclusively used by private bodies, and by Denmark, where currently the number of CCTV cameras per inhabitant rivals the UK[13] if is not the highest in the world. However, smart cameras also still represented a new technology with limited use in Denmark. Owing to a lack of knowledge and experience of smart cameras, opinions often did not differentiate between smart and traditional cameras.

Figure 7
"Does the use of smart CCTV improve the national security and your personal feeling of security?"
(number of groups that selected the answer)

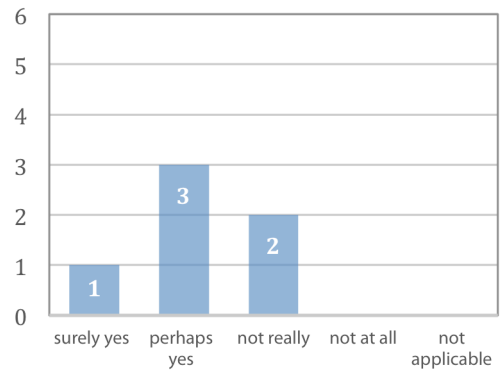
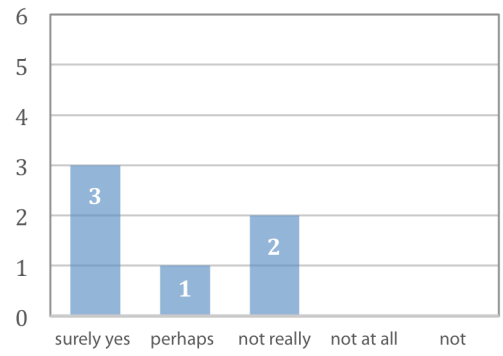


Figure 8
"Do you regard smart CCTV to be intrusive to privacy?"
(number of groups that selected the answer)



[13] http://politiken.dk/indland/ECE1362271/sikkerhedsfolk-overvaagning-er-for-udbredt/ (Politiken is one of the biggest newspaper in Denmark; the article appeared in 2011). http://www.sikkerhedsbranchen.dk/index.asp?http://www.sikkerhedsbranchen.dk/artikler.asp?mode=vis&artikel=true&id=252&kategoriid=10 (Sikkerhedsbranchen is the Danish Trade Organization for Safety and Security; the article appeared in September, 2013).

The majority of participants were not convinced that (smart) CCTV has the potential to increase national security as such. They regarded video surveillance as useful in law enforcement because it might help to detect crimes in a retrospective manner, but the main advantage of the cameras was seen in their dissuasive and preventive effect with regards to smaller crimes. They were not perceived as tools that could effectively help to solve immediate problems, but – because of their psychological effect – could deter criminals, therefore increase citizens' feeling of safety in areas where they are fitted.

In addition, number plate recognition and crowd control were mentioned as fields of useful and effective application of smart CCTV cameras.

As for advantages, it was pointed out that (smart) CCTV could be more successful and more cost-efficient than human control. In fact, participants stated that humans could be more distracted and less impartial than (smart) CCTV. Another argument supporting cameras rather than human control was that it is easier to manage a large amount of information using technology. If cameras film public spaces exclusively and do not film private homes, CCTV cameras were generally perceived in a very positive manner.

Traditional cameras were often regarded as the least intrusive solutions to privacy out of the five technologies discussed, primarily because they do not target individuals. However, smart cameras were often considered intrusive if they include biometric recognition such as facial or iris recognition. Another perception of smart cameras saw them as the improved and more effective version of surveillance cameras, and some people even regarded smart cameras as being less intrusive to privacy than the traditional ones, because they could potentially be programmed to cover sensitive parts of images. The group evaluation of intrusiveness was influenced by a lower trust in the field operators who control these systems.

In fact, it was suggested that the overall effectiveness of cameras does not depend on the number of cameras installed, but rather on the content of the recording and on the ability of professionals to interpret and act according to the displayed images. The emphasis was therefore placed on the interaction between human being (security operator) and machine (Smart CCTV).

Participants agreed that one of the most important issues is the professional qualification of those who manage this technology and visualise and analyse the related contents. They thought that camera operators should be people with appropriate training, operating under a strict and structured protocol.

In Hungary, the question of the cost of cameras also emerged. CCTV cameras were regarded as expensive, but this aspect was seen more as an obstacle to deploying more of them, and not as a financial burden on society.

The question of proportionality emerged in the context of its use in enforcing traffic rules. Although people regarded cameras as suitable for improving traffic control, this problem was not considered as important as fighting crime, and their mass deployment on this field was considered to be excessive.

6.3 Drones

Only few participants were aware of drones being used as a surveillance-oriented security technology. A large number of the participants had never seen or heard about drones. Two types of attitudes could be observed:

- **Positive attitude**: drones are modern, practical devices that can be used in several situations - they represent a form of technological progress; and
- **Negative attitude**: distrust and concern about their use, because the image of the device is often linked to their military use, and how they are often portrayed in the media.

Opinions were divided as to whether drones improve national security or citizens' personal feeling of security. However, there seemed to be a consensus among citizens of all the five countries, that drones can promote national and personal security only if they are used in specific dangerous situations and not for prevention in general.

Compared to CCTV, drones were perceived as tools that can infringe privacy significantly more, as they can monitor private areas. Their reduced visibility also increases the perception of intrusiveness. However, their use was felt as detrimental to privacy only when they are continuously used for

improving public security or for crime prevention, while in certain situations such as an accident, disaster or serious crime, when their deployment is felt to be highly justifiable, citizens agreed that nobody would be worried that they are also observed by a drone. This is why group ratings were rather uncertain when evaluating their effect on privacy.

The possibility of false alarm was also perceived as greater, because drones were seen by participants as measures operating more freely of human control than fixed cameras.

Another fear was related to the possibility that anyone can purchase a drone. Citizens saw a possibility in drones for terrorists to send explosives into a crowd. They regarded their use as risky if not used by qualified operators, as a drone might crash and cause damage.

Figure 10
"Does the use of drones improve the national security and your personal feeling of security?"
(number of groups that selected the answer)

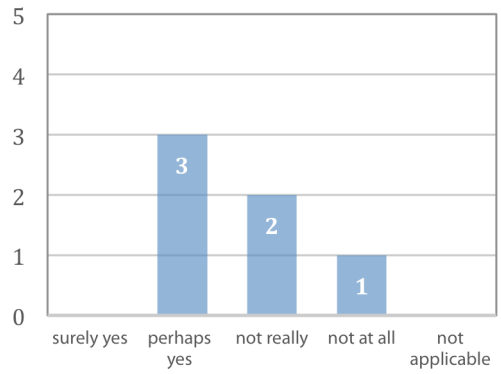
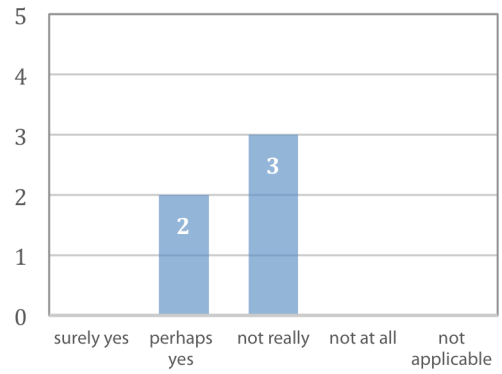


Figure 9
"Do you regard drones to be intrusive to privacy?"
(number of groups that selected the answer)



Drones were regarded as appropriate in the following cases:

- accidents, disasters, terror attacks or fire for providing an overview of the situation;
- in search and rescue as a substitute for putting people into hazardous situations;
- after a serious crime has been committed (e.g., a bank robbery) for following criminals, or in a hostage situation;
- in dangerous situations in order to increase public safety (e.g., mass events).

Citizens regarded it as important that the use of drones should be controlled in terms of personnel, application and timing. In some countries, it was suggested that use of drones by the general public should be prohibited, or otherwise, ownership should be regulated in much the same way as for guns.

6.4 Biometrics

Biometrics can entail a wide range of different technologies. Participants in all the five countries tended to talk about biometric identification systems and they did not discuss behaviour recognition.

Some participants found this technology hard to discuss in any detail because they had little personal experience of biometrics.

Biometrics was not seen as "classical" surveillance-based security technology, but rather as a technology that simplifies everyday life. In addition, citizens felt that this technology is still in the early stages of development. For the time being, citizens appeared to be curious rather than negative about biometrics.

Biometric technologies, in general, were considered highly reliable and safer than many of the other technologies discussed. Data is provided quickly and effectively and can rarely be refuted or manipulated. It was believed that the theft or falsification of someone´s identity using this system is very unlikely, although participants realised that when it happens, it can have very serious consequences.

Biometrics was not seen as a measure that improves the feeling of personal safety, but was regarded as particularly useful in the context of investigation or to ensure security in the workplace or while travelling. The fact that biometric-based solutions can identify criminals with a high level of certainty contributed to the feeling that biometrics can improve national security.

The main fear with regards to biometrics was the development of large databases storing biometric data. A number of citizens felt that a national or international database would be very intrusive, even if they thought it potentially efficient in solving crimes.

Figure 11
"Does the use of biometrics improve the national security and your personal feeling of security?"
(number of groups that selected the answer)

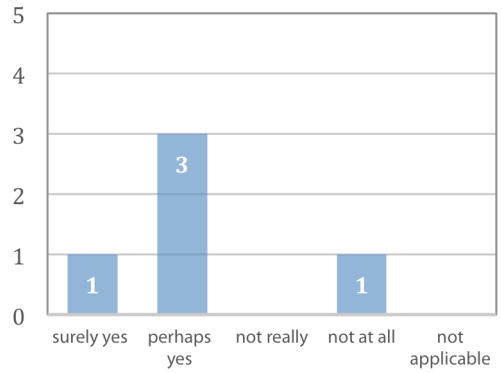
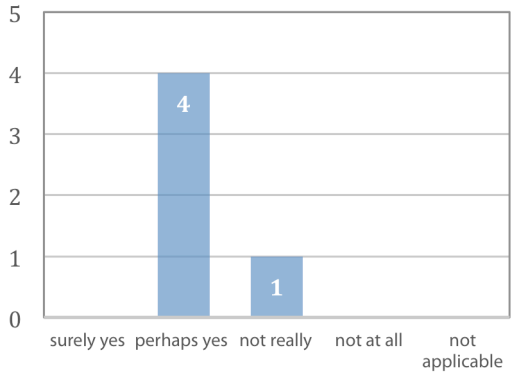


Figure 12
"Do you regard biometrics to be intrusive to privacy?"
(number of groups that selected the answer)



Another group of citizens saw the main problem as being in the human factor, i.e., lying with the people who have access to such databases, and not purely in the establishment of such databases. Others saw one solution as limiting the duration of storage of data obtained by biometric systems. Agreement from the individuals concerned was seen as a prerequisite to storing biometric data. Participants thought that data should always be stored in publicly owned and managed databases.

Another question that arose in the discussions was who would have access to biometric monitoring and to what use it could be put. Participants feared that the consequences of misuse could be dire and might lead to identity theft and similar crime.

Perhaps partly because of fewer personal experiences with this technology, none of the groups regarded it as being strongly intrusive (Figure 12).

Although opinions were divided as to whether its use should be supported as a national security measure, and citizens agreed that there were many challenges related to its use, they also thought it would be problematic to not take advantage of the possibilities that the technology could provide.

6.5 Smartphone location tracking

Smartphone location tracking (SLT) is a technology that the participants of the citizen meetings' were most acquainted with, and a great number of them used applications that employed location tracking on their phones.

Participants were the least convinced that SLT improves security, while it was definitely regarded as an intrusive technology. In the only country where participants saw it as not being particularly intrusive, the importance of transparency was emphasised, as was the possibility of switching off this functionality. The distrust of this technology was largely related to a distrust of the security agencies that might use it.

SLT was seen rather as a convenient technology, which provides a mild feeling of security via convenient features such as accessing information quickly, finding places easily and following children. Another perceived advantage was the ability to locate an individual in need of help, and this contributed to a general sense of personal safety. However, this sense of safety can be regarded more as a socially constructed feeling. Some participants pointed out that before these devices were introduced, people

did not feel more unsafe or insecure, but now that smartphones are part of our life, we feel insecure without them.

SLT was regarded as a useful tool in investigating or preventing crime but only in a restricted manner, because citizens supposed that criminals or terrorists are aware of technology and know how to avoid it. The easiest way to avoid geolocalisation is to leave the phone at home. There were some participants at the meetings who confessed that – to be on the safe side – they had not brought their mobile phone to the meeting.

SLT was generally perceived as highly intrusive to privacy both as blanket surveillance and when used to target people in specific areas without a court order or similar legal instrument. There were participants who worried that it might have a chilling effect on people who wanted to practise their democratic rights, and there was a fear that citizens could not control conclusions drawn from their location data.

Figure 13
"Does the use of SLT improve the national security and your personal feeling of security?"
(number of groups that selected the answer)

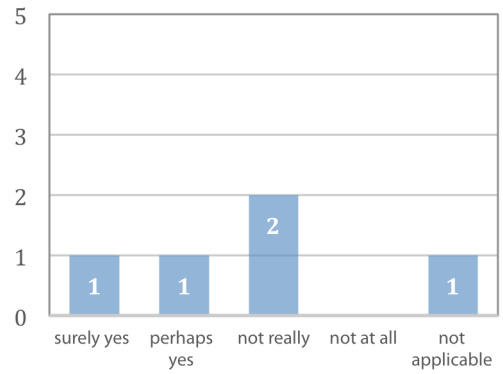
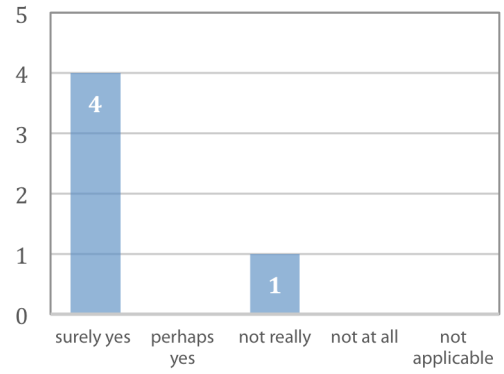


Figure 14
"Do you regard SLT to be intrusive to privacy?"
(number of groups that selected the answer)



A more significant distrust of service providers stood in the background along with, to a lesser extent, a distrust of security agencies. Of great concern was the potential misuse of location tracking by companies and third party operators from other countries. Those who were sceptical with regards to its use as a national security measure argued that they do not know who accesses the data, and they did not trust that regulation actually protected privacy.

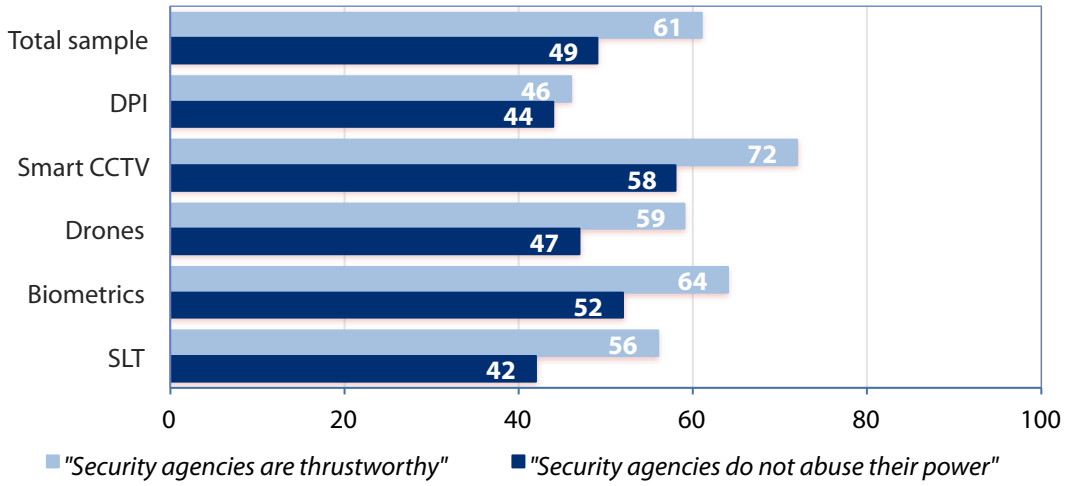
7. Security agencies

Acceptability of a surveillance-based security technology depends partly on the operation of the technology itself, i.e., how appropriate and effective it is in achieving the security goals set. The other component is related to the assessment of the surveillance executed by these technologies. In itself, surveillance is an activity that always infringes privacy to some degree. Owing to this fact, the acceptability of technology used to conduct the observation strongly depends on the perception or image of the user of these technologies, in our case the security agencies.

The topic of security agencies was discussed in the second part of the citizen meetings in relation with the particular SOST discussed at the table. Before the open discussion, participants individually evaluated two questions that had also been used during the large-scale citizen summit. At the end of the discussion, each table voted as a group on their trust of the security agencies using the given SOST.

Data in Figure 15 suggests that, similarly to the large-scale results, trust in security agencies was often tempered with concerns that such agencies will abuse their power. The level of trust in security agencies varied according to technology, but these differences seemed to be more related to the acceptability of the technologies themselves.

Figure 15
Opinions on the national security agencies when they use a particular SOST[14]
(averages on a 100-point scale[15]; the higher the average the more favourable are the opinions)



It is interesting to compare the results of the initial individual voting with the group voting at the end of the open discussion on this topic (Figure 16). While based on individual voting before the discussion, security agencies were regarded as the most trustworthy when they use smart CCTV, and the least trustworthy when they use DPI. By the end of the discussions, trust in these authorities increased in relation to their use of DPI and decreased for their use of CCTV.

A very probable explanation for the change of the evaluation may be that, while the initial individual opinions were influenced by the perceived effectiveness and privacy infringement capacity of the given SOST, table discussions were more concentrated on the security authorities and how they operate these technologies. In these debates, participants often distinguished between those who direct the whole systems (perceived not in terms of individuals, but of authorities and institutions) and the field operators. Participants were often more concerned that the field operators, who have access to data, abuse information because *"they are humans"*, and also because they are not sufficiently controlled or trained, and those employed in such positions are not the most suitable or most trustworthy, and so on.

[14] The total number of respondents at the two questions was 161 and 152 respectively.
[15] The original four-point scale was projected to a 100-point scale, and then the average scores were counted in order to better visualise the differences in the answers.

The visibility of field operators seems to influence the way in which citizens evaluate trustworthiness. Whenever the operators are more "visible", such as in the case of CCTV systems, citizens' (positive or negative) evaluation of trustworthiness focussed on the individuals. Whenever the operators are hidden (e.g., in case of DPI), participants tended to evaluate the authorities, and their assessment varied depending on the authorities' general image.

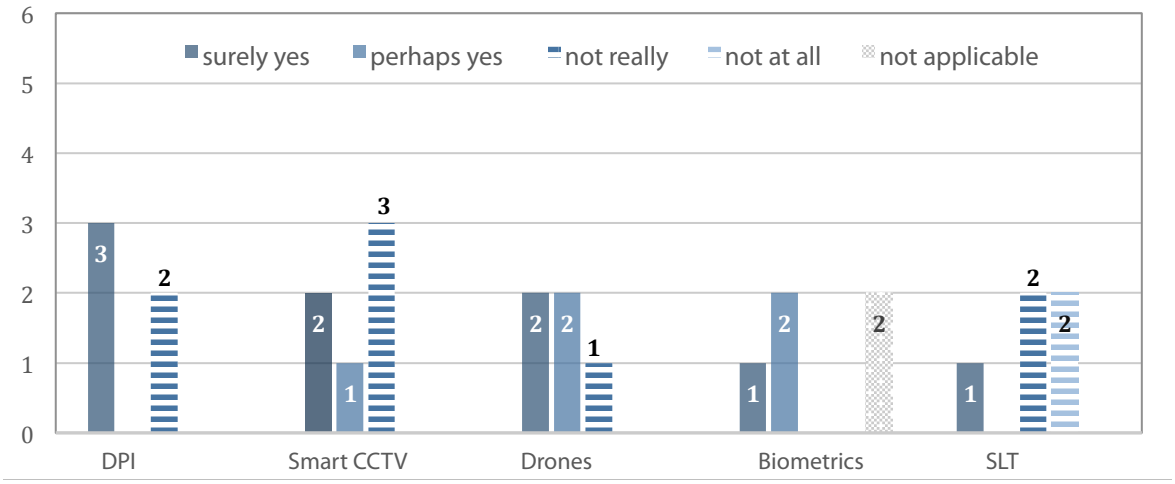
Trust towards security agencies, when they use drones, improved by the end of the open discussion, because the evaluation was often based on the supposition that they are used not for mass surveillance but only in special, dangerous or threatening situations.

Biometrics was the least known technology, and two groups were not able to vote as a group, because the opinions diverged or because they lacked sufficient information on this technology and its use.

Security agencies received the most negative evaluation when they use SLT. Citizens in all the five countries often stated that they trust security agencies significantly more than (profit-led) private companies. Such distrust of private actors affected the evaluation of the behaviour of security agencies when they use SLT.

Figure 16

"Do you trust in security agencies who use the given SOST in your country?"
(number of groups selected the answer possibility)



A widespread general opinion was that those empowered to carry out surveillance on others also have "the power to abuse their power". Furthermore, the extended use of surveillance-oriented security technologies in itself increases the risk of abuse.

According to citizens, security agencies (and other state authorities) will be trustworthy if:

- people have positive personal experience about them;
- no abuses have been associated with such institutions;
- more information is made available about the collection, storage and use of personal information;
- their actions and the operation is transparent;
- they do not have unfettered discretion;
- they are controlled; and
- the employees of the institution who have access to the data:
  - are well trained;
  - do not abuse their power, they are not corrupt;
  - are well paid (and therefore are less influenced by corruption).

8. Regulation, control and legal safeguards

An important element of acceptability lies in how the deployment of technology and data processing operations are regulated and controlled, as well as what kind of legal safeguards protect citizens against abuses.

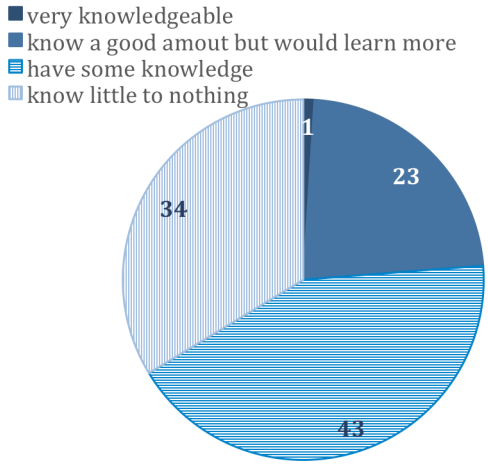
Recommendations formulated by citizens during the large-scale event often featured demands for safeguards to protect their privacy. They also requested more information about regulation and control of the deployment and use of SOSTs. The small-scale event aimed at finding out what citizens exactly know about the regulation, control and legal safeguards that apply when SOSTs are used by authorities. The topic was discussed in the first discussion round on a general level, and it was also included in the second, SOST-specific phase.

8.1 Knowledge about regulation, control and legal safeguards

The hypothesis formulated following the large-scale research, wherein a great number of citizens lack sufficient knowledge in regard to this field, was confirmed by the small-scale research (Figure 17), supplemented with the observation that even those who believed they knew quite a lot, had a superficial and often incorrect knowledge. Against this background, depending on the level of trust in security agencies and state authorities, positive and negative attitudes were formulated:

- Especially in countries where trust in state authorities was less pronounced, citizens often stated that the use of SOSTs was not sufficiently regulated, and even if it was, security agencies would not abide by the rules;
- Rumours were also formulated as a result of incomplete and false knowledge *(e.g., "Facebook was invented by National Security");*
- Despite a lack of sufficient factual knowledge, a number of citizens maintained positive attitudes, and supposed that even if they were not aware of regulation, it exists.

Figure 17
"How would you rate your knowledge on regulation and control of SOSTs?"
(percentages; individual answers; N=190)



Citizens worried that even if there are regulations, it is difficult for lay people to understand such matters. Others pointed to the lack of information made publicly available about these topics. Those who claimed they were more aware of the topic stated that the laws on the subject are outdated in relation to the contemporary technological development.

8.2 Information hunger

The hunger for more knowledge about the surveillance-oriented security technologies and their regulation and control was already evident from the large-scale event, and also characterised the participants of the small-scale research. We call this "information hunger".

The participatory methodology, which is actually a deliberative opinion research, unlike the usual methods, not only asks people's opinion, but also provides them with information on the related topics. In addition, while sharing opinions with fellow citizens, participants are strongly involved in reflecting on the topics raised and in developing personal opinions. Because the citizen summits and meetings provided an opportunity for practicing democratic rights, participants realised that the basis for formulating their interest, and that of society, is to have sufficient and relevant information.

To be sure, the information hunger was partly generated by the fact that the participatory research methodology itself drew attention to the relevance of knowledge, however, the lack of information is evident.

8.2.1 Content

Although participants often praised the information magazine sent to them in advance of the citizen meeting, this was only a starting point for them to take stock of the several other things of which they were not aware but would have liked to know. When formulating what else they would like to be aware of, a number of citizens felt that too much effort and resources have been invested in developing these technologies, while insufficient resources had been dedicated to public information campaigns. Participants felt such campaigns should address: how these technologies work; how they are, and should be regulated and controlled; and the rights and obligations of authorities and citizens.

Participants lacked sufficient information on the following areas:

- "*Who are 'they'?*"

  This sentence is a good example of citizens' frequent use of the word "they", understood loosely as anyone who can access and process technology-generated surveillance data. This semantic choice seems to reinforce the finding that citizens are not particularly aware of who can control their data and where it ends up. Sometimes the "they" turns to singular referring to a mystic, powerful someone on the top of the system and in the background.
- How does it work and what is the process, in the case of the particular SOST? How does the technology itself work? How and when do "they" gain access to personal data? How is personal information collected, stored and used?
- What kind of information is collected, and for what purpose?
- "*How am I myself affected*", and "*how can I keep certain information private*"? (the individualistic aspect)
- What are the rules, legislation and rights in general with regards to authorities and citizens? With whom is the information shared? How can an average citizen be protected?

  Those who were more aware of the regulation of SOSTs wanted to learn more about national and EU regulation.

  Those who knew less, required more basic information written in language, understandable by lay people (e.g., about the content of the privacy act of the county).
- How did the relevant regulations develop and what are the intentions behind the regulations? Who participates in the process? Who has a say (e.g., are lobby groups involved)?
- How can citizens find or access relevant information and documents, and whose responsibility is to inform the public?
- What are the effects of the SOSTs on privacy and security on the individuals and on the society?

Citizens wanted to know all these things not only with regards to surveillance carried out by security agencies but also **in relation to private companies**: when they collect data about their customers, and also with regards to when they observe their employees.

Citizens, especially older people, tended to feel lost in the world of these new technologies like smartphones and the internet, and they requested some form of opportunity that would help them to better understand the **operation of these technologies**, and not only in relation to surveillance.

8.2.2 Channels of communication

Similarly to the large-scale results, there was a strong consensus among citizens in each country that information on SOSTs and privacy issues should be provided to the various segments of society, starting at school level as part of the public education in order that children might make informed choices later in life.

The channel of communication, as well as its content, should depend on the target groups, and should take into consideration the characteristics of the different segments of society. Besides common media such as TV, radio, printed press, internet, and information leaflets, citizens also suggested forums similar

to the citizen meeting organised for them by the SurPRISE project. Another idea was to establish a legal aid service in order to provide information on privacy rights of citizens and assistance.

Another important attribute of such communication and materials is that the language should be easily understandable by the general public and digestible (e.g., short, entertaining and educative video clips between TV programmes or on posted YouTube)

8.2.3 Responsibility

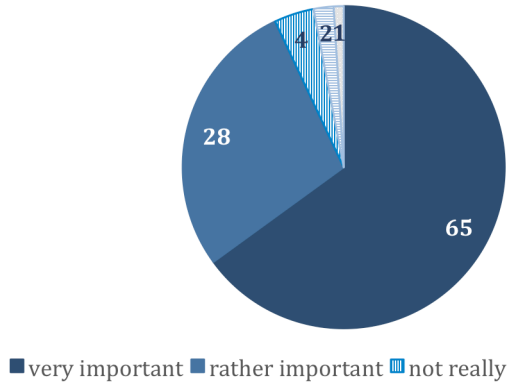
There were participants who thought that the communication to, and education of, citizens about these topics should be the responsibility of the state, while others preferred civil organisations.

Public institutions operating on different levels of society were mentioned such as the government, the police, the ministry of interior, the data protection authority, public administration, municipalities and social care systems. With regard to children, schools and the education system were mentioned as relevant bodies for increasing knowledge of SOSTs and privacy.

8.3 Control over the information gathered about citizens

The vast majority of participants believed that they should be able to control their own personal data and information collected through the use of SOSTs (Figure 18). This was often regarded as a precondition for limiting the use of such technologies.

Figure 18
"Do you think it to be important that people could control the data and information collected about them?"
(percentage; individual rating; N=190)



Several times, some kind of online solution, wherein citizens can be informed as to what kind of data is being collected about them, was mentioned.

However, when discussing possible implementation, a few worried that such online databases would also carry risks. Others questioned the feasibility of such databases, referring to too many participating bodies and too much information.

8.4 Expectation towards legal safeguards

Requests for more or better legal safeguards were another common topic among the recommendations of citizens during the large-scale event. The small-scale research tried to collect more particular information about what citizens would require.

Participants were asked to indicate the level of legal safeguards they expect to be in place when security agencies collect information generated through SOSTs (e.g., judicial authorization) and perform data-processing operations, and post-verification of accuracy. Citizens evaluated these three dimensions (authorization, data protection and verification) individually, answering to close-ended questions (see Figure 19). Despite the fact that the questions were formulated on an abstract and general level, the majority of participants were able to provide an answer. The majority of them said there should be a medium-high to high level of protection of their personal data (Figure 19). There was only one out of the 190 participants who declared that, instead of legal safeguards, data collections by SOSTs should be forbidden.

The majority of citizens said that they did not require a direct say in the regulation and control of SOSTs, but they would leave this work to professionals, with the proviso that there should be public communication about these matters in comprehensible language.

The most frequently mentioned requirements and attitudes were as follows[16]:

- Judicial authorisation of the access of public security agencies to the collected data;
- Active, permanent control over security agencies that use SOSTs by a body or organisation, which should be independent from politics, industrial and commercial interests as well as from the users of SOSTs, to ensure accountability and to avoid unfettered discretion;
  - A possible solution: to set up a new independent organisation with extensive democratic control, at the European or international level, to better advise, regulate and control the use of security technology;
- Securing access to an individual's own personal data upon request;
- The necessity, adequacy and proportionality of each measure should be assessed by means of judicial review;
- Citizens should be informed about lawful data collection and processing operations and existing legal safeguards;
- Legal safeguards should also cover private companies' use SOSTs. Actually, on a general level, citizens trust less in private companies than in security agencies who use the collected data. "Terms and conditions" should be more transparent and written in a more comprehensive language;
- Data protection authorities should be proactive in making information accessible and understandable for citizens;
- While citizens require transparent and strict control mechanisms, another opinion also appeared: the safeguards cannot be so bureaucratic as to make it difficult for the police or other public security authorities to do their job;
- Regulation should be SOST-specific, not general. In the case of less intrusive technologies such as CCTV, fewer safeguards than with technologies such as DPI may be sufficient.

[16] The majority of the listed requirements are spontaneous mentions but also the answers to the legal closed-questions (see Figure 19) were taken into consideration in this summary.

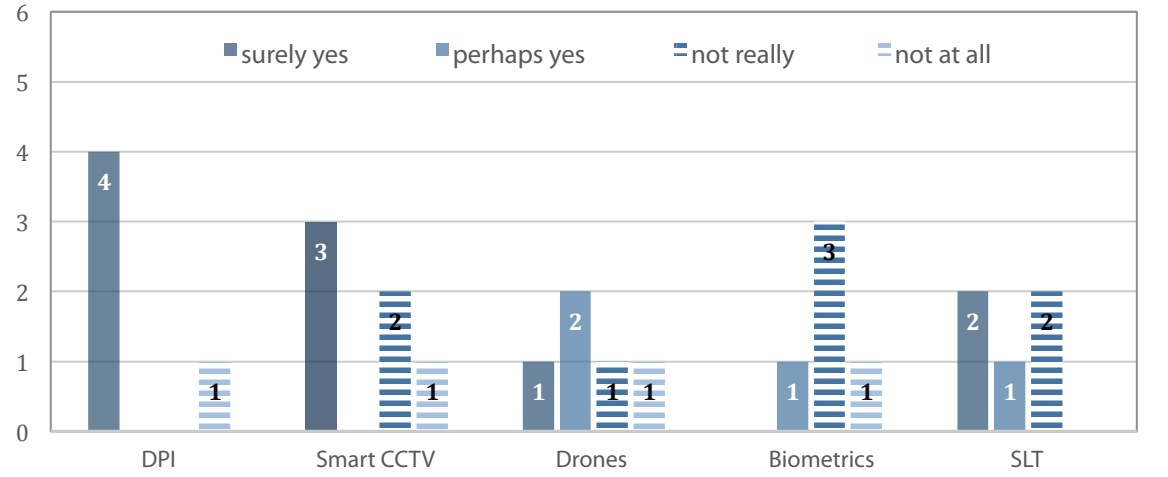
Figure 19
"What kind of safeguards do you expect to be in place when security agencies use SOSTs?"
(rate of those who selected the particular answer possibility; percentage)

	N	*percentage*
Authorization	*178*	
Judicial authorisation by a public court with all parties presented		32
Judicial authorisation without hearing the affected parties		57
Administrative authorisation without judicial control		9
Data protection	*162*	
Active control by the DPA, including individual access to an individual's own personal data		54
DPA acting in the interest of citizens but not securing their access to data		31
Security agencies subject to their internal data protection controls		10
Verification	*162*	
Necessity, adequacy and proportionality of each measure is documented and subject to judicial review		51
General monitoring of the necessity, adequacy and proportionality of the measures taken		33
The law calls for necessity, adequacy and proportionality of any measures, but this is subject to administrative decision-making and review		12

9. Trade-off through the citizens' eye

Participants were asked to reflect on the trade-off concept, i.e., whether they agree that privacy and security are incompatible: one can be increased only at the expense of the other. Opinions were divided (Figure 20).

Figure 20
"It is often said that privacy and security are incompatible: the one can be increased only at the expense of the other. Do you share this opinion?"
(number of groups selected the answer possibility)



Those who accepted the trade-off model tended to frame it in the SOSTs context, i.e. when evaluating the relationship between privacy and security thought exclusively about surveillance technologies. They felt the model is valid, because they thought that surveillance *per se* entails the infringement of privacy. For them, the biggest challenge is finding a balance between the two. However, even those who embraced the model often thought that safeguards for the personal data collected must be in place.

Those who were unsure held the view that a trade-off between security and privacy is not necessary in the following cases:

- If clear and fair rules are in place, because privacy is damaged not by the mere introduction of technology, but by the way and by whom the collected data are used;
- When the SOST is not deemed to damage privacy (e.g., often, the biometrical identification was regarded as not/ or not so intrusive);
- In particular situations, when it is worthwhile sacrificing privacy (e.g., in case of a natural disaster, nobody would be worried about observations by a drone);
- If SOST is not used for prevention but after the event (because, in the first case, a large quantity of information about innocent people is gathered); and
- In the long run, because, for example, better quality of life could lead to more security without affecting privacy, and it would no longer be necessary to control people to ensure security even if in the short run, it may be necessary to give up some privacy to have more security.

The main arguments of **those who rejected** the trade-off model were as follows:

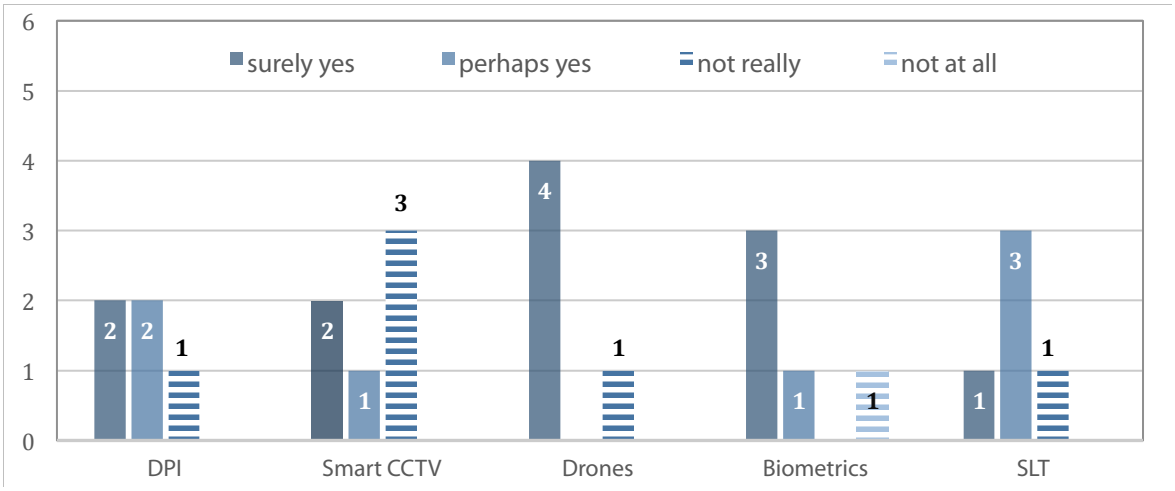
- The most frequent argument was that security can be improved by methods that are not based on surveillance technologies.
- Others felt that a society can be secure and at the same time protect citizens' right to privacy. They thought that the development of security technology should take into account both respect for privacy and data protection legislation.
- A few rejected the model by arguing that fear and insecurity is not real, but instigated, and public authorities may have an interest to instil it in citizens in order to persuade them to waive some of their rights, such as privacy.

10. Alternatives

An interesting result of the large-scale citizen summit was that, while the acceptability of SOSTs as tools to improve national security was rather high, a great majority of citizens preferred alternative security solutions. The small-scale citizen meeting tried to solve this contradiction.

Besides being the SOSTs less accepted among participants of the small-scale event, the preference for alternative solutions was again very strong. The only exception was in relation to CCTV, the most accepted surveillance solution out of the five discussed (Figure 21).

Figure 21
"Should higher priority be given to alternative approaches, which do not involve surveillance oriented security technologies?"
(number of groups selected the answer possibility)



The fact that people would like at least to minimize the negative consequences of mass surveillance strongly contributed to the preference for non-surveillance-based security solutions. However, the most likely reason behind the apparent contradiction was that a great number of citizens handled the question on two different levels: in the short and in the long term. They thought that, in the long term, technological solutions would not improve security. Rather, the root of the problem should be addressed with education on social, civic and moral responsibility; an increase of solidarity, social cohesion and social wellbeing (including more economic security); and an improvement of the social safety net, the fight against poverty and social exclusion, etc.

Such changes, especially because of their timeframe, cannot help to solve immediate security problems. This is why citizens accept the use of SOSTs, although – as described in earlier chapters – not unconditionally. They think that technological, surveillance-based solutions play a role in improving security in particular situations. In addition, there are technologies, primarily DPI, and also biometric identification, which cannot be substituted with solutions such as more police, better public lighting, more civil guards, neighbourhood watch schemes or similar, that were mentioned as possible alternatives in the shorter term.

Those who overlooked alternative solutions often referred to the fear of excessive cost in terms of financial and human resources. However, in Hungary, where human resources are significantly cheaper than in Western Europe, participants often regarded the SOST-based solutions as more costly.

An example mentioned a case when an alternative solution would be more intrusive: a manual search at an airport compared to a body scanner.

Another attitude was that the way the technology is used is problematic, rather than the technology itself. The same challenge applies to alternatives, e.g., police patrols on the street could also increase insecurity if implemented incorrectly.

Denmark was the only country in the sample, where all the five tables preferred alternative solutions to SOSTs. They were also most pronounced in their rejection of surveillance-based security technologies. One explanation is that avoidance of uncertainty is not at all characteristic of Danish culture, according to the famous national culture research of Geert Hofstede[17]. In such cultures, security is not an especially important element of individual motivation. In contrast, this index is very high in the cases of Hungary, Italy and Spain [18]

[17] See: http://geert-hofstede.com/countries.html [name the source/title, because websites can change]

[18] The "uncertainty avoidance" scores are as follows (on a 100 point scale): Denmark: 23, Norway: 50, Italy: 75, Hungary:82, Spain: 86 (http://geert-hofstede.com)

11. Messages and recommendations

Each topic that was discussed in the second discussion round concluded with the formulation of a common message or recommendation for European and national policy-makers. The individual messages are listed in D7.1 at the end of each national report. [19] The recommendations cover more or less the same topics as the recommendations of the large-scale events, and no special new elements could have been identified. In addition to the open discussions, the recommendations also provided a basis for the analysis provided in the previous chapters. Here we summarise the main topics the messages covered.

Strategies for use

Instead of mass surveillance, participants suggested proportionate use, which can be realised if:

- the purpose of the use is thoroughly considered, and, if possible, on a case-by-case basis (SOSTs are used only for appropriate purposes)
- the circle of the people under surveillance is limited
- the time span the data may be used is limited

SOSTs should always be used in a legal and responsible manner. In addition, people in general regarded the human control of the use of the "machines" as important.

Regulation and control

A great number of the recommendations contained references to the regulation and control of SOSTs.

In addition to the general requests referring to the fact that the deployment and use of these measures should be strictly regulated, and the use should be transparent and under intense control, a few specific suggestions also were formulated:

- EU regulation should form the basis of national regulations;
- Especially with regards to DPI, global regulation is needed;
- In addition to internal control, external, independent supervision is the basis of confidence;
- Judicial authorisation and control is necessary;
- Regulation should be clear and understandable for citizens;
- There should be transparency about:
  - how personal information is used,
  - how the data is processed, and
  - the positive and negative aspects of each technology;
- Regulation should include the right to be forgotten.

The role of alternatives

This topic was discussed in greater depth in Chapter 9. People generally accept the use of SOSTs especially on the short term, but expressed the fear that technology will take control from humans, and result in the suppression of traditional security solutions.

Participants emphasised the supplementary use of surveillance security technology on the short term, and demanded that remedial action be taken to deal with societal problems that are indirectly responsible for a great number of crimes in the long term. In addition, they emphasised the importance of the encouragement of social cohesion.

Surveillance should respect privacy and civil liberties

There were suggestions rejecting surveillance and/or the trade-off between security and privacy. Yet, some would be satisfied with the limitation of surveillance and the protection of the core of privacy.

[19] Marianne Barland, Jacob Skjødt Nilsen, Vincenzo Pavone, Maria Grazia Porcedda, Elvira Santiago, Márta Szénay, Teresa Talò, D7.1 - Report on decision support testing (five national reports), 2014. *http://surprise-project.eu/wp-content/uploads/2014/10/SurPRISE_D7.1-Report-on-decision-support-testing.pdf*

There was consensus among the participants that democratic freedoms should also be protected (freedom of speech and exercising citizens' rights).

Demand for information

Participants felt that the information held by the authorities and the population is asymmetric. In addition to information about the legal safeguards that were discussed separately in Chapter 8.4, they required information about:

- the positive and negative features and consequences of the SOSTs;
- the purpose of SOST's use;
- the effect of SOST's use;
- the manner of use of the information collected by SOST's; and
- the operation of the technology itself.

Another request was public campaigns and education about SOSTs and related topics starting at primary school level.

Trust and distrust in security agencies

Chapter 6 provides a more detailed analysis on this topic, based partly on the recommendations of citizens. Additional recommendations covered the claim that data collected by security authorities should be retained within the authority, and the role of private partners in the collection of data should be limited. SOSTs should only ever be used in a legal and responsible manner by security agencies.

Involvement of citizens

Participants required public discussions, open debates about the use of these technologies, and opportunities to have a say when these measures are deployed and used. They discussed the possibilities that they could somewhat control their data collected by these systems in the first phase of the citizen meeting (see in Chapter 7.3), but the topic emerged again when formulating recommendations and messages. The minimal request with regards to this was that authorities should inform citizens about the data collections in detail, defining the circle of those affected.

At the same time, people should be educated to use these new technologies in a more responsible manner.

Development of the technology in order to protect privacy

SOSTs should be further developed in order to protect privacy to a greater extent. Developments should also include improvements to prevent misuse and false positives.

12. Reflections on the research methodology

At the end of small-scale citizen meetings, participants filled in an evaluation questionnaire. Moderators and note-takers evaluated the research design and the web-based decision support system (DSS) that facilitated the event, and the role of information debate in the acceptability of SOSTs.

12.1 Evaluation of the event by participants

The majority of participants agreed that the event was largely a pleasant and positive experience. The overwhelming majority (88 percent) felt that they had gained new insight by participating (Figure 22). Opinions were more divided about the influence the meeting could have on politicians, although the great majority (69 percent) agreed that it generated valuable knowledge for politicians (Figure 23).

Figure 22
"I have gained new insight by participating in the citizen meeting"
(percentage; individual rating; N=190)

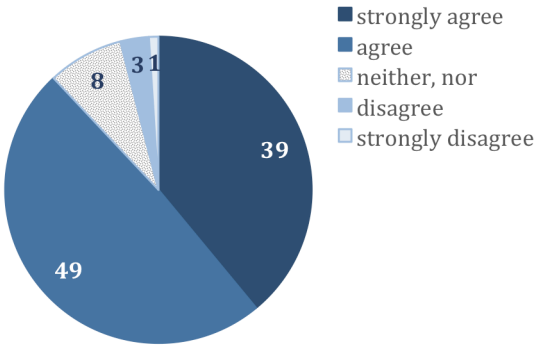
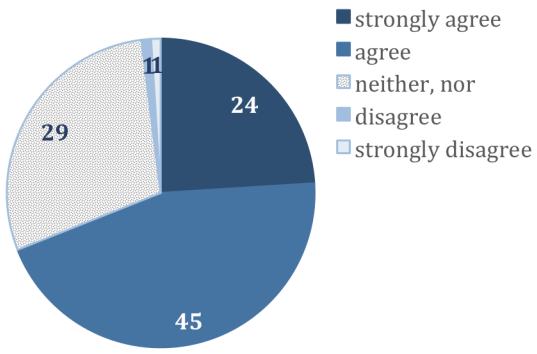
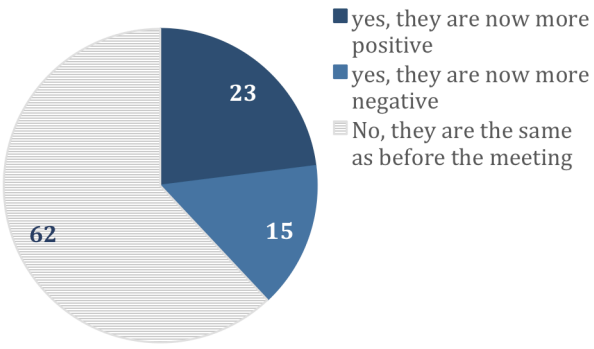


Figure 23
"I believe the citizen meeting has generated valuable knowledge for the politicians"
(percentage; individual rating; N=190)



Participants regarded the topics of the discussions as interesting, and, in some countries, the relevance of the questions was emphasised. They appreciated the knowledge they had gained by participating, often referring to the information magazine with satisfaction, and to the possibility that lay people would have an opportunity to express their views to politicians.

Figure 24
"Has this experience changed your attitudes regarding security oriented surveillance technology?"
(percentage; individual rating; N=188)



The process itself was a remarkable experience for the participants. They praised the good atmosphere of the discussions, the exchange of experiences and knowledge, and the opportunity to express their own opinion and have those heard and respected.

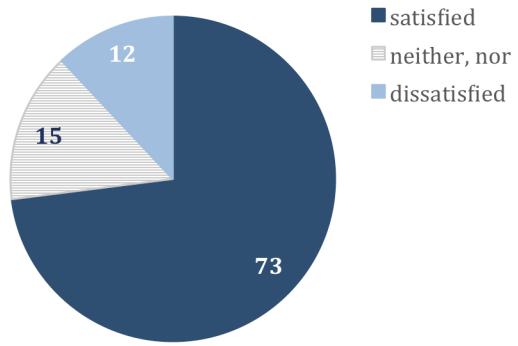
The great majority could not mention any negatives. If they did have criticism, it was that not every question or notion was well formulated, and this referred mostly to the legal questions that were not easy to grasp for every participants. Another topic of critics was the timeframe of the discussions. A few regarded the event as too long, while others would have liked to talk more about particular topics.

The meeting did not change the opinion of the majority of participants (62 percent), who felt that their attitudes towards the SOSTs remained the same as before becoming involved in the research. Participation changed the opinion of every third participant. Among them, slightly more said that their attitudes regarding SOSTs had changed in a positive direction (Figure 24).

12.2 Evaluation of the research design and the DSS

The Surprise Decision Support System (DSS) was evaluated by table moderators and note-takers at the end of the meeting (Figure 26) in order that the methodology and the DSS could be finalised for future use.

Figure 25
"Overall, how satisfied were you with the DSS?"
(percentage; N=41)

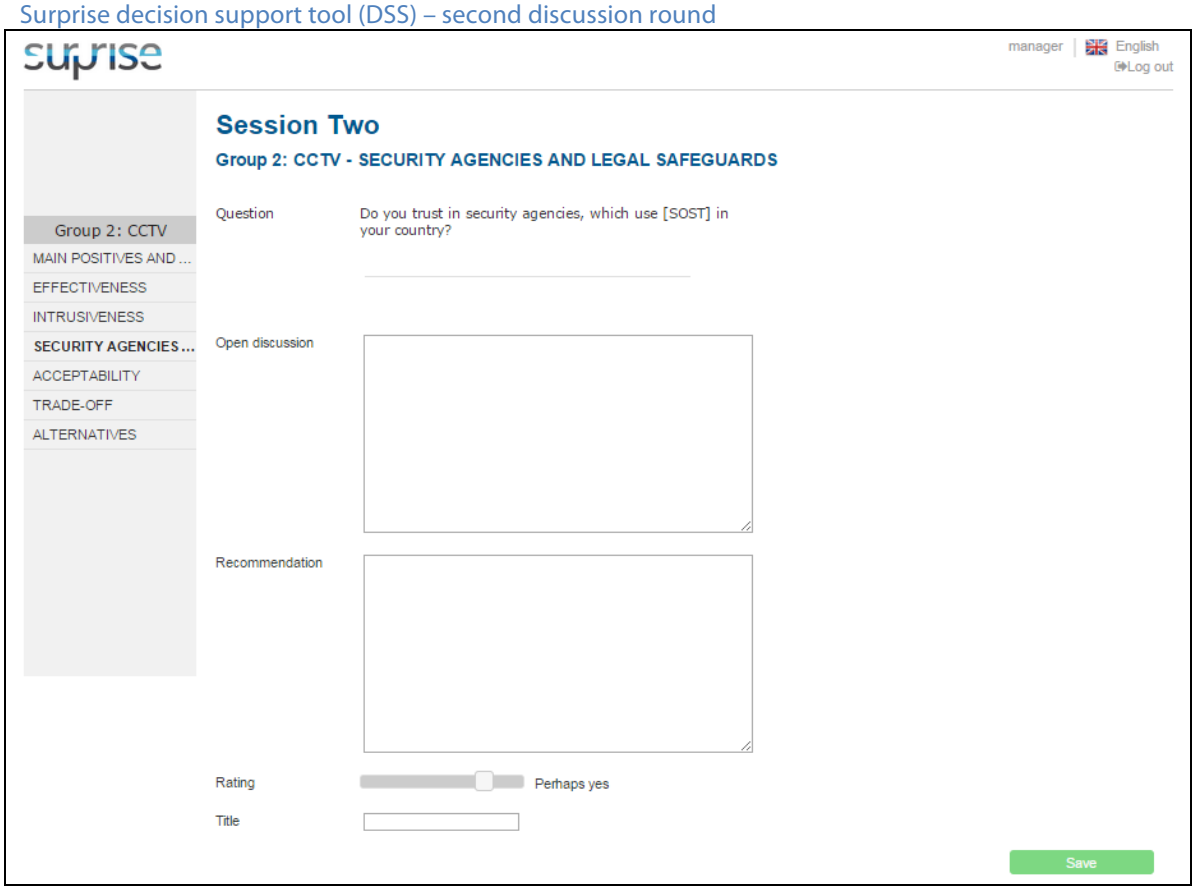


In some countries, the two individuals who facilitated the same table filled in the evaluation questionnaire together, in other countries, they did this separately. We received 41 completed questionnaires in total from the staff of 52 in the five countries. In general, table moderators and note-takers were satisfied with the DSS (Figure 25). They felt that using the DSS, citizens were given the opportunity to define a shared consensus on single statements and remain focussed on the discussion at hand. They regarded the DSS as a good tool to collect information in a systematic and structured way, using the same process in each country and at each table, and receiving a quick overview of the discussion and the results during the event.

However, a few criticisms were expressed. Taking this into account, along with consequences emerging during the analysis of the information gathered by the system, the following changes are suggested for further developing the research design and the DSS tool:

- The length of the event should be increased by another half an hour (the total length should be planned to 3.5 hours);
- The DSS should have an automatic save function;
- The second discussion round should contain questions for group evaluation exclusively (the three questions added for individual evaluation resulted in confusions for the moderators, and some of them at some tables accidentally were skipped);
- Acceptability of the SOSTs should be involved as a separate dimensions in the second discussion [this was originally planned, but, owing to time constraints, it was finally deleted and asked as an individual question];
- A few paragraphs should be included about the trade-off concept in the information magazine;
- A separate chapter about the legal aspects of the SOSTs would also be helpful in the magazine;
- The seating around the tables and the placement of the second screen should be better considered, because not all the participants could see the screen well;
- A detailed guide on how to lead the table discussions and how to record notes is a basic requirement for future wider use of the methodology and the DSS.

Figure 26
Surprise decision support tool (DSS) – second discussion round



12.3 The role of information debate and group dynamics

Group dynamics and information debate had many positive effects on the formulation of recommendations and messages to politicians:

- The individual voting results helped spark the discussion around the table;
- Discussions featured concrete and real examples, which helped to establish clear standpoints on the themes dealt with during the event;
- Citizens' open dialogue contributed to well considered and unconventional recommendations because:
  - participants broadened each other's views and raised and considered new points of view, which others perhaps would not have thought of;
  - ideas were affected through constructive table discussions: participants felt free to give different views because of the group atmosphere respecting everyone's opinion;
  - participants helped each another in the formulation of opinions and refined one another's opinion;
- The exchange of views was an appropriate tool to reveal the different attitudes of citizens;
- The interaction among table companions was very productive, especially during the second discussion round.

There were a few less favourable effects as well:

- There were participants who did not like to talk about sensitive topics, such as about the evaluation of the police, about distrust (the recording also might have played a role in this[20]);

[20] Note takers recorded the main points of the discussions in the DSS, and some countries audiotaped the discussions.

- Formulation of a common recommendation or message sometimes diverted the process of discussion (but at the same time, it was helpful to read the free discussion they had about the topic earlier);
- When opinions converged, it was easy to formulate recommendations and messages, but when table companions were too heterogeneous, the opinion of the more dominant personalities tended to be recorded, despite the fact that opinions were divergent. In these cases, those with minority opinions could not participate in the formulation of recommendations, or the focus of the discussion became narrowed. (however, the possibility to formulate individual opinion on "postcards" was a possibility to balance this);
- Large differences between the prior knowledge of participants were also sometimes difficult to bridge;
- Sending messages to politicians is connected to the picture that people form about politics in general. If this was negative, cynical comments also appeared in the debate, which could have discourage table companion in formulating their opinions. Fortunately this happened only sporadically; the great majority of participants took the task of formulating recommendations with high responsibility;
- Based on personal and subjective experiences, it sometimes proved difficult to provide general recommendations that could be interpreted on both the national and supranational levels (it was sometimes difficult to bridge this level difference).

We observed that the deliberation process, in less known and not very easily understood or accessible topics, generates information hunger. At the same time, it supports the development of responsible, democratic citizen behaviour by empowering people to think about the raised topics more deeply and responsibly. Thus, strong demand for information is partly the result of the involvement of citizens in the democratic deliberation process of the research.

The participatory event resulted in strong involvement, and had an effect on participants. Many of them regarded the process itself as a good opportunity to gain knowledge about surveillance technologies as well as to involve citizens in political decision-making.

12.4 Validation of the large- and small-scale methodologies

The main results, including the quantitative data of the small-scale research, were identical to the outcome of the large-scale events, and validated the main research results. This small-scale research supplemented earlier results with a few additional aspects, and helped derive explanations to a few apparent contradictions. At the same time, the similarity of the main findings of the two series of participatory events justifies the relevance of the small-scale research design as well as the web based Surprise Decision-Support System.

13. List of Figures