"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 7.1 – Report on decision support testing

Lead Beneficiary: Medián

Author(s): Marianne Barland (NBT), Jacob Skjødt Nilsen (DBT), Vincenzo Pavone (CSIC), Maria Grazia Porcedda (EUI), Elvira Santiago (CSIC), Márta Szénay (Medián), Teresa Talò (EUI)

Due Date: August 2014

Submission Date: October 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

1 Introduction

As part of the SurPRISE project, two series of participatory events were organised in order to learn more about how the general public interpret the use of technology with surveillance functionality to address security problems. These events were public meetings where citizens gathered to have face-to-face discussions about 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 citizens in each country. In addition, five countries out of these nine organised “Small-Scale Citizen Meetings” in June of 2014.

This deliverable (D7.1) contains the five national reports presenting the main findings of the second series of participatory events, the small-scale citizen meetings. A separate deliverable, D7.2 contains the synthesis report summarising the main national findings.

The first chapter of the current deliverable describes the methodology and objectives of the second series of participatory events. The following five chapters contain the five national reports. Each national report starts with an executive summary, then the detailed findings are arranged in subchapters closing with the list of messages and recommendations formulated by citizens during their discussions. A separate section is dedicated to the process design, and the last chapter of each country report summarises how participants and table moderators evaluated the event at the end of the meeting using the evaluation questionnaires included in the Appendix.

2 Objectives and methodology

The main objectives of the small-scale deliberative research completed in WP7 are to supplement the results of the large-scale citizen summits:

- by investigating the societal context of SOSTs selected in WP2 but not included in WP5
- by further investigating factors and criteria influencing trust and citizens' concerns about security challenges

Additional objectives of the research in WP7 are as follows:

- To develop a web-based tool to support and streamline the facilitation of the decision support system, which helps involve citizens into the technology evaluation process, as well as test this system through small-scale participatory events
- To evaluate the role of information debate and the role of group dynamics in citizens' acceptance of SOSTs

The detailed research objectives/questions below are formulated on the basis of the model developed in WP2, the theoretical background analysis completed in WP3 as well as the preliminary results of the large-scale citizen summits:

- What security and insecurity exactly mean to respondents
- What the main perceived security challenges are
- How citizens perceive surveillance in general and in particular with regards to the SOSTs
- How security issues/threats are connected to the surveillance-based security measures
- How the surveillance itself affects, if at all, citizens' everyday life
- How people interpret privacy and data protection
- What is the core of privacy that should be protected the most
- What citizens know/believe about the legal framework and control around surveillance-based security technologies, and what kind of information/communication they require
- What kind of legal safeguards citizens require and how these safeguards contribute to the acceptance of the particular SOSTs
- To understand better the connection between trust and the fear of abusing power with regards to security agencies that employ these technologies
- How judicial and legal safeguards can play a role in determining the level of institutional trust
- What people mean by effectiveness as well as intrusiveness with regards to these technologies in general and the discussed SOST in particular
- To assess the reasoning behind the acceptance and rejection of the trade of theory
- To understand better whether preferring alternative solutions are simply votes against surveillance or citizens have particular ideas and requirements for supplementing the surveillance-based solutions in general and with regards to the discussed SOST in particular

A new and innovative, web-based[1] research design, developed on the basis of experiences of the large-scale research and tested during pilot studies in Denmark and Hungary, facilitated the five citizen meetings. Small-scale citizen meetings were organised in Denmark, Hungary, Italy, Norway and Spain involving about 35-40 participants in each country. Besides the three technologies of DPI, smart CCTV and Smartphone location tracking that were also discussed during the large-scale citizen summit, two additional technologies were included in the assessment process: Drones and Biometrics.

The informed discussion was supported by a new information magazine, which was a reedited, adapted and actualized version of the one used during the large-scale event and supplemented with new chapters on Drones, Biometrics as well as Alternative solutions.

The 3-hour citizen meetings consisted of two discussion rounds:

[1] See the description of the so-called Decision Support System tool in D7.3.

- The first session tried to provide deeper insight on a general level into how citizens feel about security, surveillance itself and the surveillance-based security technologies, privacy and data protection as well as regulation and control connected to the use of these surveillance-based technologies. This discussion round was completed using a well-structured web-based tool. The alternation of individual and group work characterised the table work.
- The second session focused more on the deliberation process. Each table discussed one SOST out of the five included in the research[2]. Citizens attempted to formulate recommendations and messages to European politicians with regards to the SOST in question or, alternatively, more generally about each particular topic they discussed.

A short introductory plenary session preceded the group work at the tables, where open discussions and individual or group voting to answers of a questionnaire alternated. At the end of the meeting, participants as well as moderators assessed the event using a self-administered questionnaire.

[2] 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.

3 Country report of Norway[3]

3.1 Executive Summary

The SurPRISE small-scale event in Oslo took place on June 16th. 22 engaged participants met to discuss different aspects of surveillance, privacy and security.

The participants expressed a high feeling of safety in their everyday lives, but could also identify several challenges to their personal and national security. This included terrorism, online fraud, cybercrime and nature disasters caused by climate change. They found surveillance-oriented technology effective to take on these challenges to a certain degree, but they also had concerns regarding the effectiveness, appropriateness and intrusiveness of these technologies. They were especially concerned about mass-surveillance, and were negative to the thought of a general implementation of surveillance technologies, even if the goal is to improve national security.

The participants had some knowledge of regulations and legal safeguards, but wanted to know more. They emphasized that such information had to be written in an easy and understandable way, so that citizens could understand it, in order to take informed choices about their use of technology.

There were different views on the so-called trade-off between security and privacy. Some participants agreed that increased security would lead to decreased privacy, while others opposed this theory. One group identified another trade-off that many participants were interested in: the one between privacy and convenience. As we become more and more dependent on digital services, it is sometimes inconvenient to take the extra steps to protect privacy. One example of this is smart CCTV. It will often be inconvenient to avoid the cameras, as you will have to walk another route than the one you originally planned. The same is for online services: as Google and Facebook continue to grow, it might be difficult and impractical to be on the "outside" of these services, even though you could choose to use other services to protect your privacy.

Another important issue identified by the participants is the transformation of personal information into a commodity. They feared that private actors that had commercial interests would to a larger degree than now, use surveillance-oriented technology to collect and sell personal information.

Many of the participants were positive towards alternative security solutions like more police in the streets or neighbourhood watch-programmes. But they argued that this would probably demand more resources than surveillance technology, and that it also had to be done in a thought-through way. No matter what measure is implemented (technological or not), the way the measure is used, will always be one of the most important factors when citizens decide whether to accept the measure or not.

[3] The author of this chapter: Marianne Barland, The Norwegian Board of Technology (NBT)

3.2 Perception of security and insecurity

3.2.1 Safety

At the beginning of the event, the participants were asked about their perception of security, and their feeling of safety in their everyday life. Most of the participants felt safe in their everyday life. The majority also agreed that Norway is a safe country to live in. Several participants compared Norway to other countries when they discussed this, and especially Russia and China was mentioned as examples of countries they perceived as less secure than Norway.

> *"I generally feel safe, but I worry about development in the future"*

Even though most participants had a strong feeling of safety, several of them mentioned that the terror attacks in Norway in July 2011 had opened their eyes to the fact that terrorism and violent incidents could happen in Norway. Before this, they had thought that such incidents were unlikely to happen in Norway.

Some of the younger participants had strong opinions about safety, and argued that Norway was very safe for most groups in the society. They thought the focus on security was sometimes exaggerated, and seldom worried about their own safety.

3.2.2 Main security challenges

When trying to identify specific security challenges, many participants highlighted the rapid technological development as an important factor. The fact that laws and regulations are not able to keep up with the technological development can create gravy zones where illegal surveillance can occur. This imbalance also made some of the participants worried about the future. How surveillance technology and techniques might develop in the future is a challenge that must be tackled by policy-makers.

The participants who were worried about their everyday safety were concerned about surveillance and collection of their personal data. They argued that citizens get far too little information about the surveillance that do happen, and that they were worried about how this could develop in the future.

Others worried about societal issues like climate change and breakdown of the Norwegian welfare state. When it came to their personal safety, they worried about traffic accidents, robbery and health related issues. Some also specifically mentioned the chilling effect, and that they feared our democratic values would diminish in the future, because of the near constant surveillance in their everyday life. The lack of transparency about surveillance practises could also contribute to a chilling effect.

Several participants identified foreign security agencies as a challenge to their personal safety. The lack of international cooperation and control bodies also contributed to this perception. Many of the participants mentioned the revelation about the NSA scandal and mass surveillance on a global scale as one of the reasons they worried about this. They feared that Norwegian policy-makers don't know enough about the surveillance being done by other countries, and don't have the power to stop it if it happens. This is an example of an important challenge: that security measures, also when implemented by governmental security agencies, contribute to a feeling of insecurity. The measures that are meant to increase societal security actually lead to the opposite. The perceived security and feeling of safety is quite different from the participants' understanding of national security.

One participant argued that our personal information will become more and more valuable. Because of this he feared disloyal employees would "steal" your information and sell to others.

3.3 Opinions on surveillance-based security solutions in general

3.3.1 Appropriateness and necessity

The participants had several examples of situations where surveillance could be both appropriate and necessary.

Several mentioned deep packet inspection as an important tool for discovering and prevent terrorists. Some also hoped that online surveillance could prevent economic fraud, for example by discovering unusual activity in bank accounts.

The participants discussed how new and "smarter" technologies can help make surveillance more targeted, and this development was seen as positive. One participant mentioned specifically smart CCVT, and the possibilities to "blur" parts of the pictures, so that only a specific area was subject to surveillance and analysis.

One participant expressed that some biometric solutions could be appropriate, especially if the information was stored locally, and not in a larger database. Using fingerprints for logging into your iPhone was mentioned as one example of this.

In areas where it can be difficult for humans to move around safely, surveillance technology could be both appropriate and necessary. Using drones for search and rescue after an avalanche was mentioned as one example of this.

A general remark from many participants was that surveillance is appropriate, but only if it is targeted. Mass-surveillance was considered very negative, and not very effective. Several participants also mentioned that they thought surveillance was more acceptable if it was done by governmental security agencies, and they were more sceptical towards surveillance done by private companies.

3.3.2 Awareness of the kind of information gathered

Location was one of the types of information many of the groups discussed. The participants mentioned their smart/mobile phones, toll roads and "Flexuscards"[4] as technologies they knew collected information about their location.

Using credit cards or "bonus-cards" from specific stores or shopping online leaves a lot of information and several participants were concerned about how much their shopping habits could reveal about them. Some also mentioned metadata as information that is being collected, and a type of data that could actually tell a lot about a person.

One table discussed where the limits are for what types of information that can be collected, and they were concerned that security agencies could find out almost everything if they really wanted.

> *If the Policy Security Service is interested in me, they could know what size my underwear is, in less than a week.*

Some participants were concerned about new technology that enables collection of information that one previously could prevent. One example was that drones could take pictures in areas that had previously been kept private, for example by fences.

3.3.3 Effect of surveillance on everyday life

Most of the participants did not change their behaviour because of surveillance-oriented security technologies. But several said that they had a feeling that they "should" do something. Many also mentioned that unawareness and lack of knowledge makes them more passive. If they had more knowledge they thought they would try to avoid surveillance more actively than now. This demand for information was recurrent at many of the tables. One of the younger participants was quite positive towards surveillance, and argued that law-abiding citizens should not worry about this.

> *"Why should I be worried? I have nothing to hide"*

Even though many participants didn't change their behaviour, some did. One participant was very aware, and used encryption-services to make sure that his email and internet activities remained private.

[4] Flexus is the e-ticket used by the public transport companies in Oslo and surrounding areas.

A couple of participants said they used cash instead of cards, so that their shopping patterns are not registered by their bank. One participant also used cash because she worried about fraud, and that someone might steal her PIN-code.

Some participants mentioned that they had stopped using social media, like Facebook, because they felt uneasy about the revealing character of the service. One also said he used different services for different things, so that one service provider didn't know everything about him.

A recurring topic in several of the groups was the "conflict" between convenience and privacy. Even though one saw that there were CCTV-cameras in an area, and wanted to avoid them, it felt inconvenient to take another route. For several participants, convenience was mentioned as a reason for not changing their behaviour.

3.4 Privacy in the Norwegian culture

3.4.1 Interpretation of privacy

Privacy was by all participants considered a fundamental right and an important element in a democracy. The Norwegian notion "personvern" is a broad concept, and includes both privacy and data protection. When the participants tried to define what privacy meant to them, this duality became apparent.

Several participants focused on that privacy was a right. A fundamental right to choose what to share with others, whether these others are friends and family, the Government, your co-workers or private companies. Some participants also included the right to be anonymous in their explanation. This also included the right to be left alone in both physical and digital space.

Other participants focused more on actual data protection: that privacy means to have control over your personal information and know who collects and stores it.

Some meant that privacy is a means for maintaining the balance of power between the state and the citizens. 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.

3.4.2 Concerns about surveillance

Almost all the participants were concerned that surveillance erodes privacy. They feared that one would lose values like freedom of speech, anonymity and freedom. The participants who mentioned this, said that they thought it would be even more difficult to uphold values like freedom of speech in the future.

Some participants identified our digital society as one of the reasons for this. When we leave digital traces everywhere, it will become more and more difficult to protect privacy.

> *"Privacy as we know it is an illusion. It needs to be defined in a new way."*

The transfer of data between countries was especially worrying for some of the participants. Even though there are oversight bodies, they feared that these bodies do not have the genuine power or resources to correct wrongdoings. This worry had been sparked by the revelations about NSA's surveillance of European citizens.

When discussing the actors that use surveillance, some of the participants said that they were not that concerned about the Government and security agencies, but that they to a larger degree feared the surveillance done by private and commercial actors.

3.4.3 The inviolable core of privacy

The participants tried to identify the core of privacy, and what they thought was most important to protect from surveillance. Some groups discussed how this core is in many ways was defined by a country's culture – and that this might differ from country to country. In the end the inviolable core is also something very personal, and should be defined on the individual level. At the same time, the participants mentioned many of the same elements when describing what they thought was most important to protect.

Almost all participants mentioned information about their health as important to protect. Many also mentioned political and religious views, and sexual orientation.

Social security number was also mentioned by several participants, even though this is not considered sensitive personal data by the Norwegian Data Protection Authority. The participants argued that if someone gets hold of your social security number it is quite easy to steal your identify if you combine it with other types of information (for example your address). They look at the social security number as a "key" to many actions, and it was therefore something that was important to protect.

3.5 Regulation and control around SOSTs

3.5.1 Awareness and a need for more information

The majority of the participants reported that they knew a good amount about regulation and control related to privacy and surveillance. A few of them had only some or none knowledge on the topic.

In the discussions, they expressed concern about the lack of knowledge, and said that information about regulation is hard to find and it is often written in a language that is difficult to read. Those who were familiar with regulations had mostly gained this knowledge through their work or studies. For example there were a couple of participants who were employed in the health care sector, who had knowledge about the regulation related to patient journals etc.

Even though most of the participants reported to have some knowledge about regulation and control, there were many things they wanted to learn more about.

A general introduction to the Personal Data Act and how this is regulated was mentioned by several participants as something they would like to know more about. Others wanted more specific information about how apps and services collected, stored and used their personal information. Even though Norway is not a member of the European Union, several participants wanted to learn more about international and EU regulations, as Norway still implement many EU directives, through membership of the EEA.

One table discussed how and why regulations were made, and this was something they wanted to know more about. If there were lobby groups heavily involved in these processes, this would be important information for the public. Some participants expressed disappointment in Norwegian politicians in the area of justice, both in Government and Parliament. They thought they cared too little about citizens' privacy.

When discussing who should be responsible for informing the public and how this could be done, there were many different suggestions. Some participants felt that the Data Protection Authority should be more active than today, and spend more resources making information accessible and understandable for citizens. Other participants meant that the Data Protection Authority was a too universal body, and that other, relevant institutions had to take more responsibility. For example should the hospital or nursing home be responsible for informing patients and their families about privacy and data protection in the health sector.

Many of the participants mentioned schools and the education system as relevant actors for increasing knowledge about privacy. They argued that kids need to learn about data protection and privacy from a young age, so that they could take informed choices later in life.

At one table the participants also discussed how the Norwegian Broadcasting Corporation could play a role. They argued that short films could be a good format in order to communicate in an understandable way. These short films could be showed between programmes, like commercials are shown on TV-channels today.

3.5.2 Expectations towards legal safeguards

Almost all the participants found it important to give citizens the opportunity to control the information collected about them. Several were interested in a "my page" solution, where they could log in and get an overview of the actors that collected data, what data they collected and stored and how this was used. During the discussion, many others agreed to this suggestion. However, a couple of participants argued that even though they would like this, they didn't think that it would ever be a reality. There are just too many actors and too much information. To coordinate and compile all this information would not be a manageable task.

The participants were asked what kind of safeguards they expected to be in place when security agencies use surveillance-oriented security technology. They were introduced to three different levels; judicial authorization, data protection and verification. For many of the participants, this was difficult to relate to – both because they felt they lacked knowledge about what different alternatives entails, but also because they would assess this differently for different technologies. One table did not give answers because they thought the questions were too general and vague.

For the participants that did answer, most of them were in favour of quite strict control mechanisms – but not necessarily the strictest. Several said that they wanted involvement of public court or the data protection authority, but they did not favour very bureaucratic safeguards that would make it difficult for the police or others to do their job.

In the following discussions, most participants expressed different opinions on safeguards for different technologies. For examples, already familiar technologies like CCTV could be subject to fewer safeguards than for example deep packet inspection, which was considered a much more invasive technology.

3.6 Differences and similarities in the perception of particular SOSTs

For the second part of the event, the groups' discussions were dedicated to specific security technologies – one per group. The participants were asked to discuss positive and negative elements of the technology, how they assessed the effectiveness and intrusiveness and if they supported the adoption of this technology as a national security measure.

3.6.1 Deep packet inspection

Internet surveillance by deep packet inspection is a quite complex and difficult technology to grasp, but the revelations about NSA surveillance programme has put this on the agenda. Several participants mentioned the media attention on the NSA scandal as something that has made them more knowledgeable on the subject. The group that discussed deep packet inspection saw several positive features with this technology. They thought it to be an important element in maintaining digital infrastructure, and also an effective tool for targeted surveillance of suspects of serious crime. They agreed that deep packet inspection could improve national security.

But at the same time, there are several drawbacks related to deep packet inspection. The participants thought it to be highly intrusive, especially when it is used as a general tool for mass-surveillance. One participant meant the deep packet inspection was the most intrusive surveillance technology of today. Even though she saw positive elements, she was worried:

> "Deep *packet inspection has huge potential, but the chance of everything going to hell is much greater"*

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 way. They were also concerned about private actors using the technology, and that this would lead to personal information becoming a commodity.

When asked if they supported adaption of deep packet inspection as a national security tool, they refrained from answering. They argued that the use is highly contextual, and even though they thought it would be acceptable in certain situations it would be too intrusive in many other contexts.

3.6.2 Smart CCTV

Traditional CCTV cameras are not widely implemented by security agencies in Norway. There are probably less than 15 cameras put up by the police in the whole country. However, there are many private actors which use CCTV – for example in shops, buses or on private property. Smart CCTV is, as far as we know, not yet implemented in Norway as a national security measure.

The group that discussed smart CCTV were negative to a general implementation of this technology, but saw several positive features if it is used to solve very specific tasks. One common use of smart CCTV is number plate recognition for cars, and the participants thought this could be effective. They also mentioned crowd control as a potential use.

On the other hand, the participants were quite negative when they discussed smart CCTV with facial recognition. If smart CCTV is used to target individuals, it was considered more intrusive than other tasks (for example number plate recognition).

The group did not think smart CCTV improved national security. They thought it could be positive for certain tasks, but not as a general measure. For this same reason, they did not consider it very intrusive, as long as it is only used for very specific tasks.

The group was split in two when they discussed if they would support the adoption of smart CCTV as a national security measure – one half agreed and one half disagreed to this.

3.6.3 Drones

Drones are a quite new security technology in Norway, but there have been debate about the implementation (especially by the police) in Norwegian media.

The group that discussed drones saw several positive features with the technology. They thought it was very positive that one could use drones in situations that could be dangerous for people – for example after an avalanche, earth quake or forest fires. Drones can give a good overview of a dangerous situation, without having to put security personnel in danger.

The participants thought the development of drones had moved very fast, and several of them mention that they have not even heard about this technology until the last year. They wanted to put emphasis on the imbalance between technology development and the development and adaption of laws and regulation. When the regulation lags behind, the participants saw several challenges with the use of drones. In what situations should it be allowed to use drones? Who should be allowed to use it? And how can one protect the privacy of individuals?

The group did not think implementation of drones would improve national security. They were sceptical of a general implementation, and thought it should be allowed only in certain situations. Use has to be strictly regulated and defined, so that misuse can be easily discovered and stopped.

When assessing the intrusiveness of drones on privacy, all the participants thought it was intrusive. They feared that this could be a tool for people to spy on each other, and invade each other’s private space. They also highlighted the possible physical danger – a drone out of control could be very dangerous to people on the ground.

3.6.4 Biometrics

Biometrics can entail a wide range of different technologies. Some biometric techniques, for example using pictures for identification, are common in Norway. However, the group that discussed biometrics focused mostly on the not so common techniques, like fingerprints, iris scanning and DNA testing.

The group was negative towards the technology that is used for biometric identification with fingerprints or iris-scanning. The fact that no two samples are identical opens up for uncertainty and errors. One has to be aware of this and not put too much trust in the technology. They were also worried about the regulation related to biometrics, and were not sure that the development of the laws was able to keep up with the technological development and implementation.

On the positive side, they thought biometrics is a good solution for identification – for example when logging into your bank online. It is user-friendly, because you use yourself and your physical features, instead of having to remember a password or PIN-number. They also mentioned that biometric information (for example fingerprints and DNA) could be used to prove innocence, and exclude someone from an investigation.

The group did not agree that biometric improved national security, but would support the adoption in certain contexts. They were very negative towards implementation if it meant that the whole population would be listed in a database with biometric information. They were more positive if implementation entailed a database with information on registered criminals. They saw intrusiveness in the same way and felt that a population wide database would be very intrusive, but were more positive towards registration of criminals.

On a general note, the group agreed that there were many challenges related to the use of biometrics. But they also thought it would be problematic not to take advantage of the possibilities the technology could bring.

3.6.5 Smartphone location tracking

Smartphone location tracking is a technology many of the participants were familiar with. It has been referred to by media in criminal investigations several times, and it is also a technology the participants use themselves thought various apps and services.

When it comes to location tracking for security purposes, the participants were quite positive. They specifically mentioned tracking of missing persons (for examples kids and seniors with dementia). They also thought movement patterns could be effective in police investigations of for example terrorism.

On the other hand they did not like the feeling of someone knowing where they were. One participant argued that everyone has some places they have been, that they might be ashamed about – and that this should be able to remain secret. The group assessed the technology as intrusive to privacy, especially if it was used to track people in general. They were more positive towards targeted tracking of specific individuals, but that this would have to be assessed and decided for each case because of the possible intrusiveness of privacy.

The whole group strongly disagreed to adaption of location tracking as a national security measure. They were sceptical because one doesn't know who access the data, and they didn't trust that the regulation actually protected privacy. They also thought the technological development was going faster than the judicial framework was able to – resulting in grey areas where surveillance infringed their privacy.

3.7 Security agencies and legal safeguards

The participants at the event had quite different opinions on whether security agencies are trustworthy and if they abuse their power. This disagreement was evident for all the technologies that were discussed. The group that discussed deep packet inspection argued that those with the power to surveil others, also have the power to abuse this power. Since it is difficult to know when deep packet inspection takes place, it is very easy to take advantage of this power.

The group that discussed smart CCTV said that they trusted some actors, but not all. They mentioned the police as a security agency they trusted, but even for the police they would like to know more about how they used the information and for what purpose. They had little trust in private companies, mostly because these acted on commercial interest, and the participants feared that this could easily lead to abuse.

A general remark from most of the groups was that they put more trust in governmental actors than private actors. They did not like the development of personal information being treated as a commodity, and thought personal information was more likely to be abused by private actors abused. Several participants also said that they would be more trusting if the security agencies proved that they didn't abuse their power. The media stories about the NSA had made them more sceptical, as this was clearly seen as abuse of power. They also said that more information about collection, storage and use of personal information would make them more positive.

3.8 Reflections on the "trade-off" concept

There were quite different opinions about the so-called trade-off between privacy and security at the Norwegian event. Several groups disagree and actively challenged the trade-off model. They thought that there were good chances of keeping society secure and at the same time protect the citizen's privacy, but this demanded a lot from policy-makers and security agencies. Even though it might sometimes be the "easy way out" to prioritize security over privacy, the participants did think it was possible to achieve both things.

Some participants argued that a rejection of the trade-off model demanded a new definition of privacy that fitted the digital society we live in today. They thought the current definition and use of the concept did not capture neither the challenges nor the solutions we have at hand today. Some participants thought that one might have to define and prioritize security policies in a different way than before.

3.9 Alternatives

In the information material the participants received before the event, several alternatives to surveillance-oriented security technologies were presented. At the event, they were asked if they thought such alternatives should be given higher priority. Several of the groups supported this approach, but not all gave their full support.

There was a general remark made by one group that alternative approaches probably demanded more resources (both economically and with regards to human resources), but that it should be implemented anyway. Several groups mentioned more police in the streets as a measure they would like more of. They also supported the concept of neighbourhood watch and thought this could strengthen social relations in society. Strengthening these social relations could be an important element in increasing the feeling of safety in people's everyday life. One group also discussed if the media contributed to the feeling of insecurity by focusing on threats and danger in their reports.

One of the groups was a bit more negative towards alternatives, and did not necessarily think that alternatives would be better for the citizens. One participant mentioned that it felt more intrusive to be searched manually by security personnel at the airport, than walking through a body scanner. This group also emphasized that it does not always exists an alternative. Deep packet inspection was mentioned as an example where they didn't think it exists an alternative.

A general remark from several of the groups was that more often than not, it was the use that was problematic, not the technology in itself. And that surely, the same challenge could appear with alternatives. Police patrols in the streets could also create insecurity, if done in the wrong way.

3.10 Recommendations and messages for European and national politicians

The groups got the possibility to formulate concrete recommendations to policy-makers on different topics during the discussions. Some groups formulated recommendations on all topics, while others focused on some of the topics.

3.10.1 Deep packet inspection

Table: DPI

Discussion phase: Positive and negative assessment

Recommendation/message: We need common, international regulation of deep packet inspection. It is challenging to define what kind of use which should be allowed and what should be illegal. Due to cultural and personal differences, people will assess different kind of uses in different ways: what is considered ok for some might not be ok for others.

Table: DPI

Discussion phase: Positive and negative assessment

Title: Deep packet inspection is a necessary evil, which needs strict regulation and limited use

Recommendation/message: Surveillance can help create security

Table: DPI

Discussion phase: Intrusiveness

Recommendation/message:

Deep packet inspection is probably used more than we know, and we don't know how and if it is done according to regulations.

Those who use this technology should follow strict regulations and deadlines.

Table: DPI

Discussion phase: Security agencies and legal safeguards

Recommendation/message: Power will be abused because people are flawed. There are power struggles and interests internally in every system.

Explanation: Citizen's distrust of the police when it comes to privacy was clearly shown during the debate about the data protection directive. We need transparency to trust institutions. The Government has to be open and prove that they are able to tackle challenges with reason.

Table: DPI

Discussion phase: Trade-off between privacy and security

Recommendation/message: There are people who wish to use surveillance to save money on traditional investigation. If you allow infringement of privacy to increase safety, you'll end up with neither.

Table: DPI

Discussion phase: Alternatives

Title: Nothing is wrong with the technology, but we need to know why it is use

Recommendation/message: Automatic surveillance is positive as long as it is used the right way, but at the same time, it increases the chance of abuse.

3.10.2 Smart CCTV

Table: Smart CCTV

Discussion phase: Positive and negative assessment

Recommendation/message: We are sceptical of general mass-surveillance, for example of Karl Johan's gate[5], but positive to more specific tasks, for example number plate recognition.

Table: Smart CCTV

Discussion phase: Effectiveness

Recommendation/message: We are uncertain of the effectiveness of smart CCTV. In some ways, it can improve security, but several requirements have to be met – especially control mechanisms.

Table: Smart CCTV

Discussion phase: Security Agencies and legal safeguards

Recommendation/message: We don't believe that security agencies systematically abuse their power, but there will be made mistakes.

[5] Oslo's main street

3.10.3 Drones

Table: Drones

Discussion phase: Effectiveness

Recommendation/message: We do not think the effectiveness of drones is fully thought through.

Table: Drones

Discussion phase: Intrusiveness

Recommendation/message: The information is asymmetrical.

Table: Drones

Discussion phase: Trade-off between security and privacy

Recommendation/message: The trade-off is real.

Table: Drones

Discussion phase: Alternatives

Recommendation/message: There should be more focus on preventative solutions.

3.10.4 Biometrics

Table: Biometrics

Discussion phase: Positive and negative assessment

Recommendation/message: Be aware of possible false positives and negatives, and the built-in sociological elements – than one connects certain bodily features with certain actions.

Table: Biometrics

Discussion phase: Intrusiveness

Title: Guidelines, practice and control

Recommendation/message: It is less problematic to use biometrics, than to not use it. There is a lack of regulation and it is important to establish control mechanisms.

Table: Biometrics

Discussion phase: Security Agencies and legal safeguards

Recommendation/message: Cautious distrust – we have doubts about how this is practiced. Authorization can be misused, and security personnel might misjudge their personal judgment.

Table: Biometrics

Discussion phase: Alternatives

Title: Creating trust

Recommendation/message: There are a lot of things one can do before using surveillance-oriented technology. Focus on stimulation behaviour instead of regulating it!

3.10.5 Smartphone location tracking

Table: Smartphone location tracking

Discussion phase: Positive and negative assessment

Recommendation/message There are clear advantages, but also evident disadvantages and several unresolved issues. We need open debate and transparency about how personal information is used.

Table: Smartphone location tracking

Discussion phase: Intrusiveness

Recommendation/message Smartphone location tracking is intrusive to our privacy. The regulations are vague and the system lacks transparency.

Table: Smartphone location tracking

Discussion phase: Security agencies and legal safeguards

Recommendation/message We think scepticism can be productive. Security agencies have to earn our trust through their actions, and give us sufficient information about how they collect and use our personal information.

3.11 Process design

The SurPRISE small-scale event in Norway took place on 16th June, in Oslo. The venue was "Litteraturhuset" – a well-known venue for meetings and debates. The event started at 5 PM, and lasted three hours.

The recruitment was done through several channels: ads in local newspapers, the NBT's website and social media profiles, posters at Universities and local societal organisations in the Oslo area. 32 persons registered for the event and 22 participated.

The group of participants had a quite good demographic distribution – with the exception of gender. There were more men than women attending (13 men and 9 women). The participants were between 27 and 76 years of age, and mostly from Oslo and the surrounding areas. Most of them had a university degree.

3.12 Evaluation of the event

3.12.1 How citizens assessed the meeting

At the end of the event, the participants got the opportunity to assess the meeting. They were asked if they have learned something from their participations, if the discussions had produced valuable information for policy-makers and if the experience had changed their views on surveillance-oriented security technology. They were also asked to give additional feedback if they had any.

Almost all the participants had gained new insight from participating at the event, and all, with the exception of one, thought that the event had produced valuable insight for policy-makers. For most of the participant (16 people) the experience did not change their opinion. However, four people became more negative towards surveillance technology, while two became more positive.

The general feedback from the participants was that they were very happy to attend such an event. They thought it touched upon a very important subject – and that it was important that citizens also got a say. There was some criticism of the questions, that the topic was too complex to answer "yes or no", but for the most parts, the participants found it interesting and enjoyable to discuss with the others at their table.

3.12.2 Evaluation of the DSS by the research staff

The moderators/note-takers were asked to evaluate the decision support system. Most were quite satisfied (1 completely satisfied/3 rather satisfied), while one was rather dissatisfied. In the feedback, two moderators said they found it disturbing with several different kinds of "voting", especially in the second part of the workshop (one "top-question" with rating plus the individual voting questions.). The DSS made it easy to progress through the event, and made it easy to take down notes. Some suggested fewer questions, so that one would have enough time to discuss each questions more in depth.

3.12.3 The role of information debate and group dynamics in citizens' acceptance of SOSTs

The participants at the event were self-recruited, and therefore almost all had a specific interest in the topic. Some had a quite clear stand, and could be perceived as quite dominating during the discussion. The moderators did a good job in letting everyone have a say, but the topic of the discussions was often influenced by the first person to speak. Therefore, the focus of the discussion sometimes got a bit narrow, if the first person to speak already had very strong opinions on the subject.

The participants reacted positive towards the voting using the "booklet". The voting results helped spark the discussion around the table. One participant also said that he put more thought into his voting, as he knew he had to give arguments for his choice in the discussion afterwards.

4 Country report of Spain[6]

4.1 Executive Summary

The SurPRISE event in Madrid took place on 25th June 2014. Participants attended the meeting in a hotel in the business district of the capital. It lasted from 6 to 9 pm with a half hour break in the middle of the event. During the three hours event, the 39 citizens who attended the event were divided into five tables, each table addressed, first, a general session on security and privacy issues, and then a second session, which depending on the table, focused on one specific surveillance technology: DPI, smart CCTV, drones, biometrics, and SLT.

One of the main findings of the event is that, although "security" remains a difficult concept to define for Spanish people, it is generally understood as a holistic concept, which is often defined as a sense of safety and lack for fears, worries and concerns. The participants in the event generally feel safe in their daily life and believe that the country is a safe place to live but their lack of knowledge in relation to these new technologies often can increase their feeling of insecurity instead of reducing it.

This sense of uneasiness with new SOSTs is also due to the fact that the participants tend to consider that these technologies are applicable and useful only in combating major crimes. With regards to minor, daily life type of threats and crimes, they are unsure about the actual advantages of SOSTs and feel that, in general, these technologies do not increase their own personal security. As a result, many participants argued that the level of insecurity is not high enough to justify the use of many of these SOSTs, with perhaps the exception of (traditional) CCTVs. Moreover, quite a few participants are concerned that the information collected from them through security technologies does not really respond to real security needs and, therefore, demand greater protection and guarantees of their private data.

In general, participants are concerned about the invasion of privacy that surveillance-oriented security technologies may involve. They consider that privacy must always be protected as far as their private life is concerned, and state clear that their home, and whatever is connected to it, must be considered inviolable. On top of that, considering that the growing implementation of surveillance technologies in people´s everyday life can often generate a feeling of insecurity, it is widely suggested that these technologies should only be used when they are strictly necessary, with the minimum degree of surveillance, which must always be appropriate and proportionate to real, urgent and pressing, security needs.

Participants discussing their own degree of awareness and information about operation and regulation of these technologies explicitly considered that there is a general lack of information on technologies already in use; it is often known what they are but rarely how they actually work. They demand, thus, more information on the operation of the SOSTS and on the rules that regulate them: politics and society, as they put it, should go evolve at the same pace. However, when the kind of legal and procedural safeguards expected to regulate when security agencies use surveillance oriented technology was discussed, many participants could not really come to a concrete proposal, as they found existing regulations and requirements very obscure and difficult to understand.

The major concern regards DPI is related to how this technology could really be regulated in order to avoid abuses, or make them highly improbable. In the case of Smart CCTVs, there was more support but several participants insisted that this technology, be smart or not, offer only a sense of increased security but does not really increase security as such. Therefore, the participants agreed that the negative aspects of the cameras are primarily related to the use that is made with the information collected. The biggest advantage of the drones would be the ability to record images from angles previously

[6] The authors of this chapter: Elvira Santiago, Vincenzo Pavone (CSIC) in collaboration with Maria Casanova.

unattainable with other technologies or by humans. Regarding Biometrics participants considered than precisely the reliability of data provided by this technology can be a major problem, for the risk of fraud when individual identities are stolen. The Smartphone Location Tracking (SLT) is the technology most familiar to all participants, who agreed that one of the positive sides of SLT is that it can help to locate individual in danger and offer them support or rescue them in case of accident. In contrast, the negative side is that location data can be used for commercial purposes and to produce a reliable list of those people that, for instance, participate to politically loaded events, such as a political demonstration.

When it comes to the trade-off between security and privacy, many participants that the exchange of privacy for increased security is a decision that can only be made by the society as a whole depending on the social and political context. However, they also insist that such an approach should not be considered the only possibility and that it only makes sense as part of a broader, complex strategy that tries to improve the overall level of security by addressing also the social causes and origins of violence and crime. Some participants also underlined, that the trade-off approach is a strategy that is based on fear, and that there is interest on the part of the authorities to instil fear and insecurity among citizens in order to nudge them to renounce to some of their privacy. The exchange of privacy for security, thus, is not the only way to improve security and privacy increases or decreases depending on the use made of the information obtained through surveillance based technologies, and no just by the mere introduction of these technologies.

As a result, the participants involved believe that the best alternative to SOSTs is the direct fight against the causes of insecurity. Yet, they are pragmatic, too, and admit that this may take time and may not be enough to ensure the safety. Consequently, they accept the use of SOSTs as complementary measures that should be taken into account *always in combination with* a greater investment in human resources and better education on technologies and democratic values. Spanish citizens recommend policy makers to develop a clear and transparent use of SOSTs, and agree on a uniform regulation for all EU countries.

4.2 Perception of security and insecurity

“Security” is a difficult concept to define for Spanish population. Most of the time, the term is used as a holistic concept, which comes to cover all areas of life. This holistic concept of security, as a matter of fact, comes quite close the way the concept is defined, framed and reflected both in the European and in the Spanish National Security Strategies. For instance, in one discussion table, security challenges are defined as "[…] *the right to privacy, freedom of opinion, speech and participation; transport safety, eliminate marginal zones, moderate security forces and the abuse of power; work and overcome the crisis, street cleaning; social exclusion; international terrorism; modify existing legislation and Criminal Law* [and adding] *dynamism and flexibility of justice*" (Drones table). Other participants define security as a positive feeling characterised by a lack of concerns, fear and worries: "*Security is a comfort feeling, free from danger and insecurity is the opposite; not having to be thinking or worried about incidents*” (Table SLT).

The participants in the Spanish event generally feel safe in their daily life and believe that the country is a safe place to live: "*Spain is generally safe. It depends on what you compare it to, there are more troubled countries. We can walk the streets relaxed*" (DPI table). However, they recognize that there is a background insecurity feeling that does not necessarily correspond to a real threat, *"All participants feel safe in their daily lives and think that Spain is a safe place to live. Spain is a country where there is not a high robbery or direct violence but the feeling is not of absolute security because often directly identifiable threats are not perceived but they exist."* (Biometrics table)

This insecurity feeling of is also reinforced by the fact that many participants perceive that the authorities and the security forces are corrupted, and this obviously plays against national security. *"The country is not safe because we have corrupt politicians, corrupt police that go over, sometimes you are more insecure calling the police"* (DPI table). However there are discrepancies with this idea, and despite the poor widespread perception that Spaniards have of their politicians, attitudes toward security forces are divided between those who believe that police abuse of their power, against those who value positively *“Spanish police are highly valued in general, compared with other countries"* (Biometrics table)

In relation to new technologies, the lack of knowledge of its mode of operation *de facto* increases the insecurity feeling *"Internet security. I feel insecure due to ignorance. Although I do not stop using it. There must be a strong safety* “(DPI table). In spite of their declared purpose of increasing security, SOSTs are perceived to increase the feeling of insecurity. *"It should not be just control and control, with this excuse they are taking us to the big brother; the challenge is to adapt security to the real needs, because too much security also creates insecurity"* (SLT table). The real challenge, as they say, is to achieve an effective and justified data and information collection: *"Security measures seem very vast, designed to collect data just for the sake of it. The challenge would be to be effective in gathering information”*

It is also clear from the data gathered in the Spanish small-scale event, that there are, indeed, two ways of framing security. On the one hand, security in individual terms, or at the level of citizen, is a feeling, which makes it difficult to extend this feeling to a more objective measure of whether or not the country is safe, as this feeling may not be related or consistent to the real level of threats in a country. The second interpretation of security is at the national level, which implies the responsibility of political authorities and of security forces. When security is understood in national terms, security technologies are generally perceived to be effective because they allow getting where the bare human action does not reach. Therefore a paradox arises: while Spain is considered a safe place - except for minor offenses or acts of vandalism - the SOSTs are only considered useful to improve national security and the fight against major crimes, like terrorism, which is perceived as immediately relevant in people’s daily life in Spain. In other terms, whilst SOSTs are perceived to increase national security, they are considered much less relevant and effective in people’s daily life to address their daily insecurity concerns.

4.3 Opinions on surveillance-based security solutions in general

4.3.1 Appropriateness and necessity

In the general discourse at the tables, the participants understand that SOSTs are applicable and useful in combating major crimes. But that little or nothing can be done through SOSTs in order to protect ordinary citizens. We quote: *"Drones improve national security, but there is not a perception that they can do that on the personal level"* (Drones table). As a result, these technologies should never be used in private sectors: *"The effectiveness of the technology is proven in cases of crime, pornography, terrorism, closed circuits as airports, atmospheric phenomena, but is not effective in the private sector"* (Drones table). Therefore, SOSTs are considered to be an important complement to a broader and more sophisticated security strategy, where they can integrate human’s abilities and/or make up for any human error: *"Nobody can be two hours focused on a room, a camera is safer*" (DPI table). However, several participants considered that in Spain there isn’t a level of insecurity so high to justify the use of SOSTs, which are perceived to be of benefit for others type of business or domains, such as commercial purposes or private security needs: *"I am against the CCTV for the arrangement of the information is done for non-legitimate purposes"* (CCTV table); *"These* [technologies] *are used as a lucrative tool for companies as Securitas Direct"* (SLT table). There are, of course, exceptions. In the SLT table, one participant refers to a personal history where the SLT contributed to save one human life: an event that the participant lived as a direct experience. In this case, obviously, the evaluation of the technology is much more positive: *"I was injured and through smartphone localization system I could be located and saved by rescue team"* (SLT table).

4.3.2 Awareness of the kind of information gathered

Citizens are concerned that the information is collected from them through security technologies does not respond to real security needs and, therefore, demand greater protection and guarantees of private data: *"Information is power and they information they can get may hurt and be manipulated* "(DPI table). As a result, the participants insisted that the information collected should always receive a high level of protection: *"We must exert actively control of who manages the data and we need to know what they do, where they go"* (Drones table). Citizens are also concerned about who finally manage their personal information, and are worried about who watches over those responsible for the collection of personal data. In this respect, the participants clearly prefer public institutions to private ones: *"The problem is not the information that is collected, the problem is the control that exists about who has access to that information, who controls the controller? The problem is not the information but who collects it and what for. And in this sense, agencies and public agencies generate more confidence that private companies"* (Biometrics table). Finally the population is also concerned about the impact of current collection of personal data may have in the future: *"Although currently it does not involve a major concern, in future issues related to privacy can arise*" (Biometrics table).

4.3.3 Effect of surveillance on everyday life

As we have seen, the effect of surveillance in people´s everyday life can increase the feeling of insecurity. Consequently, it is necessary that surveillance should be measured and adjusted to real needs. And if the general attitude towards surveillance is generally negative due to the infringement of privacy, it becomes even more hostile when surveillance is exerted in the private sphere of life. This, for instance, explains why CCTVs may be tolerated but DPI is not: *"I do not like being watched, cameras could be ok, but no internet data"* (DPI table). Although this is the general feeling, some people argued that they do not feel worried about it because they have nothing to hide: *"I do not mind being watched, I know there are people that you are concerned. I have not done anything wrong to be looking for me "*(DPI table).

4.4 Privacy in the Spanish culture

4.4.1 Interpretation of privacy

Consistently with what is explained in detail in the Spanish citizen summit national report (deliverable 6.9), the participants are used to conflate the word privacy "privacidad" with intimacy, "intimidad". One participant said: "[Privacy is] *whatever happens when I close the door of my house"* (SLT table)
Due to this conflation of terms, the highest respect for the protection of privacy is attributed to whatever is considered to be intimate. The private home, for instance, is seen inviolable due to protection that the intimate space of family life provides to our privacy. Moreover, and as expected (see again D6.9), privacy also is associated with decision capacity, to be able to decide what data is public and which is not. Participants highlight the word "control", control over one self's information.
"It is essential to be able to control what is public and what is not" or *"What I do not want to be disclosed should not be disclosed"* (Biometrics table).

Some guests emphasize the importance of the data known about each one of us, the importance of not giving too much information, because information is power, and information can be manipulated against you and it can hurt you. Some others reject this idea arguing that everyone shares what they want to share in public: *"If they have your data it's because you have given them away. It happens whenever you click "I agree" and continue. I click but I don´t care, I don´t think my data are so valuable"* (DPI table). Others disagree with this argument, which they consider a trap because it seems obligatory to provide certain information if you want to access certain services. It is well known that you are not going to read what you accept the conditions to use these services and if you do not accept, you cannot benefit from these services: *"It is a trap, they know that no one will read it"* (DPI table).

4.4.2 Concerns about mass surveillance

In general participants are concerned about the invasion of privacy that surveillance-oriented security technologies imply but not all participants show the same degree of concern or have this concern present in their daily life. A participant revealed that she had a great concern for the data collected by the new technologies and thought about it when she had to make plans for the day. She felt threatened constantly: *"when booking a plane, to do a banking process, when booking a hotel..."* (Biometrics table) Most participants, however, did not show such a high concern, and many agree that is important to be concerned but not to be obsessed: *"I'm not obsessed because, otherwise, I could not live"* (DPI Table) They point out that using a new technology involves learning, and it is necessary to acquire sufficient knowledge to be able to use them with caution.

Attendees are especially concerned about the abuse of these technologies. They stress the importance of making good use and provide a good education to citizens. They also point out that, indeed, there are some sectors of the population that are more vulnerable to mass surveillance. For example, some participants argued that young people are more vulnerable because they do not generally have a concern about the risks that these technologies involve, even they know how Internet works better that elderly people. In this case, the type of education or training proposed is not be about on the management of the technology itself, but about the risks that certain practices entail: *"It is not so much about what you download, it is what you upload"* (DPI). Needless to say, it is also mentioned how the new technologies ordinarily used for private purposes, such as Facebook, may have unpleasant consequences in other areas of life, such as the professional domain: *"For example, a company is looking for you, they see on Facebook that you've been drinking hard (botellón) and they decide not employ you"* (DPI table).

However, some participants considered that perhaps not only the information that each one makes public is incorrectly used, but also private information, and that often we are not aware of this. They point out, for instance, at the remote, and unauthorised, use of the camera embedded in our tablets of computers:

"I put a piece of paper to cover" (DPI table). The discussion concludes with a concern about future problems that are likely to arise around these technologies. In general the participants considered that, while it is important to ensure a high degree of individual privacy, it is also necessary to avoid unnecessary data traffic and prevent surveillance technologies become a tool to governments or companies to work out social control: *"Thanks to our new security law* [Ley de Seguridad Ciudadana, approved in the days of the meeting]*, they can now control our position with GPS and know if we go to demonstrations"* (DPI table).

4.4.3 The inviolable core of privacy

The inviolable core of privacy lies in the individual, the home and the family environment. All tables agreed on the importance of protecting this area from surveillance technologies. A participant is concerned about his inability to protect his children from the negative effects of these technologies; thereby he shows distrust and rejection against these technologies. In his table, other participants do not share his opinion and say that you cannot, nor should, escape from them: *"You cannot isolate them from the world"* (SLT table). In general, they are aware that privacy is being reduced because today there are many data records in public organizations such as health centre or finances but also in business enterprises. They point at the impact that stored data can have for the professional domain. Second, they also show a growing concern for the privacy of banking and/or financial data. There was general agreement that medical records must be kept in hospitals and this kind of data must be always well protected. Someone even suggested that citizens should have full access and exclusive possession of these data: "*Doctors have your medical history and you cannot even move it*" (DPI table).

4.5 Regulation and control around SOSTs

When asked about their knowledge on regulation and control of SOSTs, many participants feel between the position of those who have some knowledge and those who have very little or any knowledge. Only one person at each table admits to have sufficient knowledge about SOSTs, although it would be helpful to learn more. In general during the discussion, it often remarked that very little is known; that there is a lack of information about the technologies already in use. In a way, while it is known what they, little is known about how they work and what for they are used or how it is their use regulated. Some participants consider that it is their duty to get information on these technologies and their regulation: "*It's our fault for not having the knowledge, laws are on the Internet. There are net users associations, too*" (DPI table). Some other participants, in contrast, consider that this ignorance is the result of a deliberate strategy that prevents proper information from being delivered to citizens, showing show distrust towards regulators and technology developers: *"Information is not accessible because they do not want it to be accessible"* (Biometrics table).

4.5.1 Awareness and need for more information

Citizens are demanding more information on the operation of the SOSTS and on the rules regulating them: politics and society, as they put it, should evolve at the same pace. As a result, there is a widespread concern that too much effort and resources have been invested in developing these technologies whilst way to little has been dedicated to set up appropriate information campaigns on how these technologies work or on how they are, and should be, regulated. The existence of a clear and consistent legislation across the EU is deemed urgent and necessary, for each country has its own rules when data now easily flow worldwide: *"Each country differs while data is transferred too easily"* (Smartphone table). The kind of information required is about the management and regulation of these technologies. The participants expressed clearly their wish to be informed in detail about what information is collected, when, what is the purpose, who collects it and with whom it is shared: *"For what purpose and what it is used for. Lack of comprehensive global legislation, there is a difference between countries technological advances"* (Smartphone table) by the same token, they want to know, for example in the case of cameras, if their location or the process of images viewing is done correctly. They also want to know who, if anyone, has the responsibility of providing this information about the operation of public authorities; some participants considered that it should be the responsibility of the Ministry of Home Affairs, others that it should be the European Union. Whilst the state is seen as holding the responsibility to keep information about the use of these technologies available and accessible to the public, excessive state control produces rejection in some participants. *"Through court orders and other legal proceedings, sure, but then it becomes the Holy Inquisition"* (Smartphone table).

Some participants also elaborated this issue further and suggested how the operation of SOSTs should be disclosed, often through massive campaigns carried out both on the Internet, radio and television. Television means that the message will reach to more people. *"Internet is good way, complicated for old people, television is widespread and generally reliable way"* (Smartphone table). There are also complaints about the Law Bulletin (BOE) that is considered a tool too complex and difficult to access and understand for most people. As they put it, if the Law Bulletin is only way to transmit information, the latter remains quite inaccessible, causing mistrust for it seems that there is no interest in sharing information. *"The law has to be simpler and more concise. Not like 70 pages BOE"* (DPI Table). Consequently, they suggest preparing easier documents to understand, more user friendly and more accessible, such as the comic used to explain the national constitution: *"For example, in this country when the Constitution was to be explained they made a comic…they should be doing something like this"* (DPI table)

4.5.2 Expectations towards legal safeguards

In general, the participants have the expectation that, at some point, it will be compulsory to make public who manages the data, what they do with it and where it is sent. It remains difficult for them to decide exactly who should be doing this permanent dogwatch operation, how this should be organised and implemented, as there are many agencies that collect data and coordinating their operation would prove hard and difficult. When participant were asked to suggest what kind of safeguard they expected to be in place when security agencies use surveillance oriented technology there was a general lack of orientation. The question, formulated in general and abstract terms was not easy to answer, nor was it easy to correctly and quickly explain the different procedures of judicial authorization, data protection and verification that are at work. So no definite answers to these sections could be collected. The questions perhaps should have been formulated only in relation to the specific technologies and illustrated by different degrees of control of accountability, illustrated perhaps by different colours (red/stricter controls, yellow/medium level of control and green/low level of control). Despite this difficulty most people think that, whenever SOSTs are operated by security agencies, judicial authorization with or without representation from all parts is necessary: *"Our data must always be used with judicial authorization"* (DPI table). However, some suggest that some independent body, free from commercial and political influence, should be entrusted with the responsibility of conducting a permanent control over security agencies' operation. The moderators had the feeling that the data protection and verification sections were completed without a proper understanding of the question.

4.6 Differences and similarities in the perception of particular SOSTs

4.6.1 Deep Package Inspection

Deep package inspection is a technology was perceived to entail both positive and negative aspects. Participants indicated that this technology could help in several ways. For example, helping with national security or at the enterprise level, as it can issue warnings about hacker attacks. It may also avoid cybercrime or virus. Participants accepted, in principle, this technology, provided that its use is well regulated. They consider that it may be a useful tool if it is handled with legal and judicial authorization and only when individuals have a real understanding of how it works: " [we need] *regulation, control and proper use of this technology"* (DPI table). However, the group noted that this technology could also be used for negative purposes, such as terrorism or paedophilia. It can also easily infringe privacy so it is necessary, as well as difficult, to establish a legal framework that regulates the use of this technology not just at the national level, as there is a feeling of a great existing legal vacuum, especially outside Europe.

In effect, there was an intense debate on the regulations that other countries should adopt in relation to this technology. Participants expressed that the US regulations are worse since there is no special data protection policy there. Participants, thus, considered that they did not want to be as United States. They also point out at the other extreme of the spectrum, such that in Asian or Muslim countries, where the web is often so strictly monitored that it reaches the degree of a real censorship. Moreover, the participants are clearly worried about their personal information being misinterpreted through DPI: *"the police arrested a guy who wrote the word bomb several times chatting with a friend"* (DPI table). Other participants admit that DPI is intrusive, but they do not feel worried as it may be operated for good purposes: *"We give our privacy up to prevent crimes that may affect us"* (DPI table).

4.6.2 CCTV

In this group, the participants consider that smart and traditional cameras offer both individual and collective security. At the individual level, cameras help verifying real situations where they may be able to identify the cause, or the causants, of crime. Some participants also suggest that cameras may have a dissuasive and preventive effect, as their present may scare off people with bad intentions. Yet, others replied that cameras can really be useful only retrospectively, by sorting images that may help to solve crimes, but only after crime has already been committed and the damage has already been done. They think that cameras increase the sense of individual security but do not offer a true increase in security. *"CCTV collects information that can be used to solve crimes"* (CCTV table)

The information recorded by the cameras can also be used collectively to detect incidents, as for example, with the traffic on highways or other possible road alterations. However, at some point the group discusses at length about the case of the Madrid Arena accidents, where the camera recordings showed a great crowd of people pressing to exit the venue of the concert but did not prove useful to prevent the tragedy, not it helped ensuring the safety of attendees.

Opinions strongly converge on the negative aspects of the cameras, which are perceived to be primarily related to the use that is made with the information collected. They show concern about the possibility that this information may be used in a non-legal or arbitrary way. Only a few participants, though, think that excessive camera control may lead to a wrong profiling creation of population. They point out at the importance of legislation on the use of these cameras. Some participants also highlight the feeling of intrusion that this technology can produce: *"I feel under surveillance and it can violate the privacy of individuals"* (CCTV table).

Finally, the participants agreed that one of the most important issues is the professional qualification of those who manage this technology and visualize and analyse the related contents. They consider that camera operators should be persons with an appropriate training, operating through a strict and structured protocol for action. In fact, it is 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 is, thus, placed on the interaction human being (security operator) – machine (Smart CCTV): *"They are not only cameras but also professionals with capacity of control and reaction"* (CCTV table).

4.6.3 Drones

The participants at the discussion table on Drones considered that this technology may be effective because it provides an image from an angle that human could not get on its own and would need other more complex tools: *"Great application in buildings or other places with a wide field of view day and night, which cannot be reached by the human eye"* (Drones table). In general, drones are considered part of the scientific development in the 21st century, which allow, for instance, a more effective investigation about atmospheric phenomena. Several advantages of this technology are appreciated. For example, drones have the possibility of incorporating sensors that measure weather elements such as temperature, humidity and wind. Moreover, they are able to reach quickly position and move away quickly, too; they can examine land and terrain, delivering very important information that prove useful for preventing fires, avalanches, accidents or catastrophes. Some participants also mention the possibility of military use to watch, for example, over the battlefield and count the number of victims. As drones are a small technology it is thought that have very low energy consumption. They also commented on Amazon's plan to deliver their packages.

The disadvantages of this technology are strictly related to their advantages. Drone is a lightweight technology and is suspected to be unstable and could fall to the ground causing damage. They show concern about the possibility that anyone can have access to and operate drones, and they fear that also terrorists could. For example, a drone could carry an explosive to a specific, perhaps crowded, place. Some participants, thus, suggested that it should be regulated as a weapon: *"A drone could carry an explosive, watch out for terrorism"* (Drones table). Finally, participants suggested that drones can be highly intrusive, when for instance they are used to record images and conversations in the intimate space of our homes: *"A camera cannot record your house, but a drone can: this is a privacy offensive*" (Drones table)

4.6.4 Biometrics

Biometric technologies, in general, are considered highly reliable and safer than many of the other technologies discussed. Data provided is quickly and effectively and can rarely be refuted or manipulated. It is believed that the usurpation or falsification of someone´s identity using this system is very unlikely: *"They are the most effective systems, it is difficult to falsify information obtained through biometrics"* (Biometric table). However, participants also added that precisely this inexorable reliability could be a major problem because if your identity is eventually usurped or cloned or falsified, it would be very difficult to prove this fraud or to correct and restore the original one. Therefore they suggest that this technology should be further developed in the future in order to detect possible faults. *"If we give a high reliability, this involves major problems arising in the situation that someone usurps for example your fingerprint, how you get to report fraud of this kind?"* (Biometric table). As a result, they suggest having a trial period: *"It is a very new technology but that does not mean that it has to be safer"* (Biometric table).

Physical injuries are also a special cause of concern. Many participants believe that biometrics can, in a way or another, be harmful to human health. For instance: *"Iris recognition, does it hurt your eyes?"* (Biometric table). In a working environment, where fingerprints are permitted to record the entrance and exit of workers in and from their working offices, the group believes that the intention of this technology is to control the workers rather than the overall security of the premises. They give the example of a company with a particular interest in controlling its employees, which used biometric surveillance systems in combination with other systems such as Internet records in order to monitor workers' activities and schedules: *"A* [biometric] *access system can, for example, be used to control the times of entry and exit in a company. It ends up being control instead of security."* (Biometric table).

Regarding the intrusiveness of this SOST, participants have different opinions: some believe that it is less intrusive than other technologies, others consider that it is more intrusive when it records private behaviours than when it analyse bodily features: *"It's only physical, while other technologies use more personal information"* (Biometric table). Yet, others again consider that bodily features and characteristics are so inherently personal that biometrics tracking these characteristics has to be considered very intrusive. *"Physical is equalled to personal"* (Biometric table).

Consensus is reached, though, about the storage of data obtained by biometric systems, which all consider should only be temporary and only as long as the individual gives consensus for. The data should always be stored in publically owned and managed databases: *"In the case of storing biometric information in public databases"* (Biometric table).

4.6.5 Smartphone Location Tracking (SLT)

SLT is the technology most familiar to all participants. The phone features have advanced rapidly in recent years and it is well known that many of these features may be used for surveillance and/or security purposes. Participants think that the low price of phones, utility improvement and facility of operation are the factors that have caused a deep entrenchment of their use and options in our daily lives. The positive side of SLT is generally considered to be the use it offers when people in danger or in need to be rescued can geographically located. Occasionally, as they say, SLT can save your life. A guest mention his/her own a personal experience in which, being injured, could be located and reached thanks to this system: *"Through the smartphone location system I could be rescued"* (SLT table)

During the discussion most participants see that the benefits of this technology are directly related to the disadvantages, depends on the situation and on people´s intention in any given moment: *"You have an interest to be located in dangerous situations, searches ... but, at the same time, you may not want to controlled at all times"* (SLT table). *"Be located and locate anything in every moment, this allows you to find whatever you need"* (SLT table).

One participant seems completely satisfied with the operation of this technology and considers that is the best way of security. Other, more concerned, considered that there should be a control of the use of the data, i.e. that data collection should be limited. *"Being located is against the privacy of individuals"* (SLT table). *"It can be used indiscriminately by jealous boyfriend, girlfriend who wants to control whether he or she lied when he/she went to..."* (SLT table).

The concept of the sense of security produced by SLT is perceived, however, as socially constructed. Some participants, for instance, argues that before these devices were introduced people did not feel unsafe or insecure, and now that they are part of our life we feel insecure without them. Others suggest that this is a paradox, which leads a security system to cause an even greater sense of insecurity in people: "*The technologies that are said to increase people´s security need people feeling insecure to be able to turn into profitable tools*" (SLT table).

4.7 Security agencies and legal safeguards

Participants showed a wide variety of opinions on the security agencies and on the legal safeguards that are supposed to regulate the use and operation of SOSTs. Most people trust on the National Security Agencies but other participants are distrustful of those who manage the technology even if they work for the public sector. *"Overall security agencies are good. Some might have been bad but generally I believe they can trusted"* (CCTV table) *"At the end, they are people and can boast of such information or share it"* (CCTV table)

In general, however, participants agreed that public security agencies can be trusted more than private security actors: *"I understand that I live in a state of law and I may not distrust public institutions. However, in a private agency everything is moved by economic reasons, and there is no possible control"* (CCTV table); " [it is important to] *avoid fraudulent use for profitable uses"* (Biometrics table); *"Information generates power and power can be then used"* (Drones table)

As a general recommendation, the participants suggest the formulation and implementation of clear protocols, whose structure and details are easily accessible by, and available to, citizens. They propose legislation to control, regulate and manage these technologies but also public campaign to raise awareness, improve education and promote an ethical use of these technologies.

4.8 Reflections on the "trade-off" concept

Participants were asked to assess the trade-off between privacy and security through the following question: *"It is often said that privacy and security are complementary: when one increases the other decreases. Do you agree?"* The general answer is that this balance actually exists: *"Safety and security are antagonist to privacy"* (CCTV table). So increasing security, *through greater surveillance,* it is perceived to provoke an intrusion into the private lives of individuals and the consequent erosion of their privacy. *"If you increase security with more surveillance you end up intruding in most people´s life. You may amplify security but there is more intrusion into the lives of each one of us* […]. *This is what happens if you want to increase security through the implementation of this kind of measures "* (Table Smart CCTV). That is why citizens agree that, as long as surveillance technologies are used, the balance between security and privacy remains a complex and delicate issue: *"They all agree, what is really hard is to find the balance"* (DPI table).

If there is a real security risk, many participants agree that the cession of privacy is not a problem if that means that this risk is effectively minimized and provided that such cession of privacy does not occur in the inviolable core of privacy, which their consider to be their family home *"Facing a risk, I would rather lose privacy and gain security. At the end, the invasion of privacy is in the public sphere, as long as they do not get into our house* "(CCTV table). Yet, even for those who wholeheartedly adopt the trade-off approach and believe that the cession of some of their privacy may impact positively on effective security improvement, it remains essential that certain conditions be always fulfilled in relation to the protection of the privacy of the personal data collected. Others however, insist, that security and privacy can actually go hand in hand: *"For security and privacy can be maintained and increased at the same time… it is important for instance to ensure anonymity (through numerical identifiers, encryption, etc..) of stored data"* (Drones table). Finally, it was also recognized that the exchange of privacy for security is not the only way to improve security *"They are not necessarily opposing concepts, safety increase does not always mean a decrease or an intrusion into the privacy* (Biometrics table). Privacy increases or decreases depending on the use made of the information obtained through surveillance-based technologies, and no just by the mere introduction of these technologies.

In fact, the participants agree that the cession of privacy cession in exchange for higher security levels is a scenario that is essentially due to the adoption of surveillance technologies. They consider that the decision to adopt these technologies to improve security must be made by the society as a whole, depending on the context, and it must not be considered the only possibility. *"Depends on the situation you live. In the U.S.A after September 11th they did exchange privacy for security. That extreme experience drove them to that kind of control they have now. In Spain, after the M11, we have not lived the same situation. Is more balanced security with privacy*" (Table CCTV).

Finally, some participants argued that the trade-off approach is part of a security strategy based on fear, and that public authorities may have an interest to instil fear and insecurity among citizens in order to persuade them to renounce to some of their rights and privacy. They insist that the fear and insecurity generated in this way is not real and does not correspond to a lack of real security. *"The unknown always generate fear and ignorance, too. They reinforce fear, paranoia and insecurity since childhood. They want us to live in a society of fear and this is more dangerous than any kind of insecurity. The Spanish people, however, we do not have that feeling.*" (Table CCTV)

This distrust and helplessness towards the real purpose of surveillance is reflected in a final message delivered by one participant in the event*: "We do not know how we are managed. We are manipulated, but we do not know how they do. And we cannot defend ourselves* " (DPI table). It does not comes a surprise, then, that all participants ask for more information about the operation of the SOSTs and greater knowledge of the regulatory framework in relation to the surveillance and control over private information. *"It must be warranted and justified in any case that the application of biometrics technologies achieve the expressed purposes from the beginning"* (Drones table).

4.9 Alternatives

Citizens believe that the best alternative to the massive deployment of surveillance-oriented security technologies is to fight against the causes of insecurity. Yet, they recognize that this is not enough to ensure security, and consider that SOSTs should be used in combination with complementary, alternative measures: *"Alternative approaches aimed to fight against social inequality, poverty, exclusion,* *are considered important but not enough"* (Biometrics table). These complementary alternatives could be divided in three groups: a) more investment in qualified staff b) better education, and c) the fight against poverty and social exclusion.

The participants acknowledge that the biggest disadvantage to implement such alternatives is that they are economically less profitable than SOSTs: *"Alternatives are always more expensive and therefore they are not considered interesting"* (DPI table). However, it is also acknowledged that certain technologies are difficult to substitute, to find an alternative for: *DPI has no possible alternative"* (DPI table)

4.9.1 Investment in more qualified staff

Some participants suggested that plausible alternatives to SOSTs may not only be identified looking into the future but also looking back at the past: for example, they mentioned "*el sereno*", a night-watch man guarding neighbourhoods in Spain in the 50s and 60s, who was the only legitimate holder of the keys of the building entrances, so that when people got back home at night they had to call the night watch guard to access their building. In case the latter identified them as neighbour, he would let them in, otherwise he would warn the police. As a result of this system, in which various night guards patrolled the streets at night, citizens felt overall safe on the street. Other participants insist that the key to an increased security is the interaction between the human and the technological factor: *"Machines and technologies are just tools, which can only be operated by people: they must complement each other"* (CCTV table). Regardless of how much we invest in technology, behind it there should always be a qualified, conscientious, educated human network as it is not possible to delegate security to machines. The interaction between the two factors is crucial, for humans do make mistakes and are not infallible. As a result, the use of SOSTs to complement the human effort remains crucial: *"A person cannot be even two hours, for example, pending a living. A camera is safer. "* (DPI)

4.9.2 - Improve education

Participants felt that education is essential and complementary to the use of SOSTs, both to understand its operation and, as we have seen in previous sections, to prevent violent and antisocial behaviour: *"Education is also important. Not as an alternative but to supplement it. Educate not just to self-protect but not to attack and not to be watched"* (Table CCTV)

4.9.3 Fight against inequality and exclusion

Last but not least, the participants agreed that security could only ultimately be improved through a serious strategy against poverty and social inequality, which are considered often the real causes of insecurity. If these were reduced, so the participants put it, the society would be safer and use of SOSTs could also be reduced to only those cases in which they are absolutely necessary. In most cases, however, security is better served by a socio-political action aimed at addressing the sociological, cultural and economic factors promoting crime, exclusion and violence: *"This type of alternative approaches should be explored and developed further. The use of certain technologies may actually produce more exclusion, so the security action should also be directed to address more elementary and basic levels of social reality"* (Biometrics table)

4.10 Recommendations and messages for European and national politicians

4.10.1 About the use of SOSTs (general aspects)

In general, the participants consider surveillance-oriented security technologies neutral, and the advantages and disadvantages discussed are mostly related to their use. As a result, the most important advantage that the use of these technologies may offer is the possibility to save human lives. In this specific case, the adoption and use of SOSTs is not only considered acceptable but also highly recommended. The more the intended purposes and outcomes take distance from this specific goal, the more the use of SOSTs is considered less acceptable. At the other end of the spectrum, in which the use of SOSTs is never, under any circumstances, considered acceptable, the participants place the use of SOSTs for commercial and for political purposes. Having said that, even in those cases where SOSTs are indeed considered acceptable, their use must always be strictly regulated, in a transparent way, proportionally to the scale of the threat, and under the control of a third party independent authority, be it the judicial authorities or an ad hoc created body. Their message on this point comes through clearly: “take it or leave it”.

Title: SLT saves lives

Recommendation: the proper use of security technologies based surveillance can help to save lives.

Explanation: positive personal experience of one of the participants at the table that has been rescued from an incident on the mountain thanks to the SLT leads other participants to highlight the positive aspects and ask to make a good use of SOSTs oriented to improve security. Citizens recognize the advantages of the use of these technologies, but they are aware that they are highly intrusive technologies; therefore they stress the importance of citizens having knowledge and education about them and transparent information on their uses and regulation.

Title: Users Education (DPI table)

Recommendation: create educational programs for global users

Title: Transparency and information (Drones table)

Recommendation: set up public campaigns to improve transparency and information on the advantages and the disadvantages of the use of SOSTs

Title: special attention to data storage period (Biometrics table)

Recommendation: The information obtained through biometric systems should be only temporarily stored (biometrics table)

Explanation: one way to reduce the perceived intrusiveness of these technologies would be to limit the size and time of the data storage to leave to the citizens the option to avoid surveillance wherever possible.

Title: Choice to be located (SLT Table)

Recommendation: Regulate the possibility to activate the geolocalization system, leaving to the citizen the option to switch it on, whenever possible.

4.10.2 Regulation and control

In order to ensure that the use of SOSTs is effectively oriented towards to the ultimate goal of protecting lives while, at the same time, protecting the citizens from the misuses of SOSTs, citizens suggest the implementation of a global regulation and clear and transparent information about the positive and negative aspects associated with each specific technology:

Title: Global regulation (DPI table)

Recommendation: A common international law must be created for all countries, to regulate SOSTs globally. (DPI table)

Explanation: citizens are concerned about the differences in European and American laws and, for that reason, when they use social networks and digital services regulated by other countries feel that their activity might be unprotected. This international and transparent regulation should clarify who are the authorities responsible for the use of SOSTs, how exercise the control mechanisms and who is the authority responsible of it.

Title: Yes to Drones but only if strictly regulated. (Drones table)

Recommendation: Citizen should be informed of the positive and negative aspects of the SOSTs, with a clear explanation of what problems may emerge with their. New technologies should be strictly regulated right from the start, in order to ensure their use only for appropriate purposes. (Table drones)

Explanation: citizens are concerned that the absence of a regulatory framework may facilitate the abuse of technology. They want a guarantee that it will only be used to improve security.

Title: Need for clear protocols of use developed and operated by public authorities (DPI Table)

Recommendation: Citizens consider that an effective regulation, based on clear protocols of action and operation, as an increase protection of their privacy and rights. They insist that these protocols must be developed and operated only by public agencies, in which citizens have greater confidence. This social trust is the basis for citizens to feel safe. Also, citizens must ensure that the agencies responsible for security do not commit abuse, which is why again is important to be clear which agency or organization makes use of these technologies; and, the use of SOSTs will be always approved by public agencies in order to avoid fraudulent uses.

Title: the cameras can be smart but people are more (CCTV Table)

Recommendation: The use of SOSTs should always supervised by qualified personnel

In sum, citizens believe that legislation is the best preventive measure against abuses of SOSTs, but also appeals to the education of the people who manage this information. Under these conditions, the participants find SOSTs more acceptable, but social trust in these technologies remains clearly dependent on their use by national security agencies and on the respect of citizens' rights.

4.10.3 Trade-off

Citizens consider that the use of SOSTs may improve national security, and occasionally also their individual security. However, as SOSTs always imply surveillance they inevitably affect individual privacy. The choice to accept their privacy be reduced by the use of SOSTs is therefore always context and purpose dependent. As a result, citizens feel they should be entitled with the right to decide, individually or collectively, when the use of SOSTs is appropriate, proportionate and legitimate and to what extent their privacy can be affected. Each of this decision is contingent and may vary as the conditions, threats and priorities change: trust cannot be taken for granted, presumed or activated once and for all. Each and every exchange between security and privacy required by the implementation of SOSTs is always contextually dependent.

Title: Security or privacy? It depends on the context (CCTV Table).

Recommendation: security and privacy can be maintained and increased at the same time, for example through the anonymisation of the data stored (via numeric identifiers, encryption, etc.)

Recommendation: It should also be ensured and justified in any case that the application of biometrics-based technologies serves for security purposes. The need and appropriateness of the adoption of SOSTs must be evaluated on a case-by-case basis. (Biometrics Table).

Finally people consider that in Spain they are not in a situation of constant danger and therefore the use of SOSTs as a permanent security measure is not necessary. In their opinion, the use of this kind of technology should be reserved for real danger situations.

Title: Security beyond SOSTs (SLT table)

Recommendation: There exist other types of monitoring that are better adapted to reality as Spanish citizens do not live in a situation of constant danger in which the permanent use of SOSTs may turn out to be necessary.

4.10.4 Alternatives

Participants in the event are aware that in the twenty-first century technologies are essential. That is why in their opinion the dilemma is to find a balance that ensures effective and non-intrusive use of SOSTs, and only whenever absolutely necessary.

Title: We need control and complementary measures (Table SLT).

Recommendation: Moving the clock back to 50 years ago does not make sense. The use of SOSTs must be maintained but under a new regulatory framework that ensures more control over their use, which must always be complement by non-technological, i.e. social, educational and economic, measures. A more responsible use of the tool is needed.

Title: The Human Factor (CCTV table)

Recommendation: Machines cannot work alone. Citizens also highlight the need that SOSTs always work under the supervision of trained and responsible personnel.

Title: More education, more confidence (Drones table).

Recommendation: Better education in the field of technology, security and surveillance is needed. This educational improvement must go hand in hand with the educational improvement.

Title: Social cohesion and citizen participation, first of all (Biometrics table).

Recommendation: The development of technology-based security monitoring should not replace the other actions that improve safety. Alternative approaches that promote or encourage citizen participation and promote social cohesion must be considered as a complement.

4.11 Process design

The SurPRISE event in Madrid took place on the 25th of June 2014. Participants attended the meeting in a hotel in the business district of the capital. It lasted from 6 to 9 pm with a half hour break in the middle of the event.

Recruitment was done by combining two techniques. Most participants were recruited on site by an experienced person, looking for participants in different areas of the city. After explaining the event and ensuring that they met the required socio-demographic characteristics and that they showed some interest in reading magazine and participating in the discussion, people were invited to attend. In the second part of the recruitment, participants were identified and contacted by the snowball technique. All people showed special curiosity about the subject after listening about the results of the previous event.

During the first contact on street, the phone number was requested and recorded in a database to activate contact a few days later. At this point, participants were called to explain the details of the event and to ask for their postal address to send the magazine. Five days before the event participants were called once again to confirm that they had received the magazine and still wanted to participate.

In the event 47 people were invited and finally 39 attended, 20 men and 19 women. There were 13 people on each age cohort, less than 35, between 35 and 50, and older than 50. Most of them had a university degree.

4.12 Evaluation of the event

4.12.1 How citizens assessed the meeting

All participants considered to have gained new insights related to security technologies. However, when asked if they believe that the citizen meeting had generated valuable knowledge for politicians there was no agreement. Disagreement was also clear in relation to whether this experience had changed their attitudes towards surveillance oriented security technologies. Half of the participants considered that their opinion remained the same, whilst the other half was divided between those who argued that their attitudes were more positive after the event and those who believed that their attitudes were more negative.

Among the highlights of the event, we can find:

- The knowledge gained
- A good atmosphere
- The opportunity to express their opinions
- The exchange of experiences and knowledge
- The positive feeling of being listened to.
- The opportunity to listen to different, sometimes even opposite, opinions
- The opportunity to make proposals and recommendations to policy makers

The only weakness citizen noted was that that the time was insufficient.

4.12.2 Evaluation of the DSS by the research staff

In general, table moderators and note-takers were satisfied with the tool.

The positive aspects were:

- The DSS allowed for debate face-to-face with citizens
- It also enabled participants to listen the different opinions of the citizens
- It enabled the collection of information in a systematic way

The negative aspects:

- Too many questions in a row: it was difficult to deepen the understanding of the topics discussed
- It was difficult to collect all the information discussed in the various sections of DSS
- Some technical problems, too. The tool takes time to load and save changes
- The dynamic voting-card system slows the debate down

4.12.3 The role of information debate and group dynamics in citizens' acceptance of SOSTs

- Citizens should have more information on the unknown technologies as drones
- Balanced participation allows for better proposals and recommendations
- Some citizens were sceptical towards SOSTs and failed to develop recommendations.

5 Country report of Hungary[7]

5.1 Executive Summary

The Hungarian citizen meeting was held with 40 participants in Budapest on 27th June 2014. After a short plenary introduction, participants discussed the topics with their fellow citizens at tables of 8 people in two rounds, each approx. 1.5 hours long. The first discussion was run on a general level, while, during the second round, each table discussed one particular technology out of the five discussed in the information material sent out to participants in advance of the meeting: deep packet inspection (DPI), smart CCTV, drones, biometrics and smartphone location tracking (SLT).

Hungarian citizens tended to thematise the questions through personal experiences or drew parallels with movies or TV programmes. Analogical thinking prevailed in which it was often Facebook through which they interpreted the questions of surveillance and privacy. Another frequent analogy that was used in the discussion was CCTV, which currently is the best known and understood surveillance technology among Hungarian citizens.

Citizens made a strong distinction between national and public security. They did not feel that the national security of the country was endangered, while public security was perceived as deteriorating. They often saw the reason for this in the country's worsening economic situation resulting in an increase of subsistence crime.

For Hungarian citizens, those surveillance-based security solutions were more acceptable, which were able to effectively improve their feeling of security.

Out of the five technologies, it was only CCTV that met this requirement, especially because of its deterrent effect. At the same time, because this technology does not connect data directly to persons, this measure was regarded as the least intrusive. Smart surveillance cameras were seen as improved versions of traditional CCTV solutions (more effective, less intrusive). Hungarian citizens generally demanded more and better cameras in public spaces.

The appropriateness of SOSTs to increase security strongly depends on the purpose and extent of their use. With the exception of CCTV, the discussed technologies were regarded as inappropriate for general crime prevention. When they are used for this purpose, they collect tremendous amounts of data about innocent people, thus intruding on privacy while they do not provide the expected benefits.

Citizens saw some relevance in the use of Biometrics and Deep packet inspection (DPI) for national security purposes. But when using them for these purposes, the consideration of proportionality was regarded as very important. The idea of observing everybody was strongly rejected. Citizens demanded that the circle of those excluded from among the observed people should be clearly defined.

Drones can be useful in improving security in particular situations. Their use should be restricted for cases of emergency, serious crimes and dangerous situations (e.g. mass events).

Smartphone location tracking (SLT) was not regarded as appropriate for improving either national or public security. Although it was recognised that SLT provides some kind of personal sense of security, this measure was regarded as rather intrusive. People also tended to be distrustful of service providers, and were afraid that they collect and abuse their data illegally or without their consent.

A number of citizens thought that their sense of security was also undermined in political terms. Distrust towards authorities as well as the operators of these surveillance systems was a problem that emerged several times during the table conversations.

While currently less known technologies such as drones and biometrics also evoked a feeling of pride that Hungary produces/possesses these up-to-date technologies, people worried about their disproportionate use. There were not concerned about the technology itself, but rather the fate and the protection of the data collected.

Other quantitative international research, including the large-scale research of SurPRISE, revealed that citizens of the relatively new democracy of Hungary care less about privacy in general than the citizens

[7] The authors of this chapter: Márta Szénay and László Beck, from Medián

of Western-European countries with stronger democratic traditions. Discussions suggested that the main explanation behind this is the lack of culture of individuals protecting their own interests. This approach was exemplified by remarks like: "*we have to accept the world as it is*", "*we are too little to change things*", "*our data is not interesting*", etc.

At the same time, citizens were afraid of mass surveillance or at least regarded it as inconvenient. They worried about political freedoms, and older people compared it to surveillance of the past (under the socialist dictatorship), although now carried out exclusively by machines.

They demanded the protection of their privacy, the inviolable core of which, to be protected by all means, being defined as home, family, personal connections and personal communications. In addition, all the information with which harm, loss or harassment may be caused (physical, bodily or mental) should be strongly protected against surveillance.

Sufficient and relevant information is crucial for practicing democratic rights. Because this event provided a possibility for practicing these rights, participants realised that they needed more information about the subjects discussed. They primarily wanted more information about the regulation and control of these technologies. They demanded control of these activities by an "external" body independent of politics and the producers of these technologies. They demanded insight into the development of regulation and an opportunity to comment on them.

They required information about their personal affectedness, the rights of the citizens and the data handlers controlling these systems, the purpose of information collection and its effect on privacy and security. It should be made possible for citizens to control their data if they require.

Communication about SOSTs and the related regulation and legal safeguards should be part of secondary school education, and information for lay people (not trained in law) should also be provided for the adult population.

Lacking sufficient knowledge, it was regarded as difficult for lay people to define what kind of legal safeguards they would require. They would leave the development of these safeguards to experts who are independent of politics.

The most frequent reaction to the trade-off concept was that there are security solutions not based on surveillance. The social, and educational aspect of crime prevention was also seen as a kind of alternative possibility, however, citizens were aware that these solutions could only provide actual results in the long term.

Strengthening the police both in number and in morale was the most frequent alternative suggestion. Deploying more civil guards was also seen as an alternative solution. Neighbours joining forces in protecting their possessions was also seen as a feasible solution but only in smaller communities.

The trade-off between security and privacy was regarded as relevant to a certain degree when no effective alternative possibilities could be applied, and thus security was increased by using surveillance-based security technologies. However, even in these cases, the relevance of the model, namely that more security means less privacy, was not always regarded as feasible. The effect of SOSTs to privacy strongly depends on the purpose of data collection and its use. Another important point of view of the evaluation was whether the increase of security as a result of the use of the measure could be justified and could be felt by the citizens.

5.2 Perception of security and insecurity

The discussions suggested that the personal sense of safety could be interpreted in many ways. The abstract notion of security seemed to be too complex and too abstract to use on a general level. Responses to the questions about security and safety were generally narrowed down to cases, personal experiences, stories, and generalised, overall judgements.

The influence of the media on perceptions and opinions of safety appeared both on the unconscious and conscious level. In the latter case, participants criticised the media for communicating so much negative and alarming news, while others unconsciously based their opinions on generalised communication on security related topics such as the homeless or subsistence crime.

Individual answers to the question about the perception of private safety reflected that the great majority of participants felt more or less safe in their everyday lives. Opinions were more divided when talking about the country in general, referring to the fact that, although they generally felt safe in their everyday lives, they were not satisfied with the state of public safety.

People made a strong distinction between national and public security. The state of both tended to be evaluated from their individual aspects.

With regards to the country, people did not fear some kind of physical attack, e.g. terror attack. The effect of the world economy, e.g. money economy, like some kind of outside threatening effect, or economic manipulation that perhaps could result in bankruptcy of the country, also appeared among the sources of insecurity, but there were not well-defined opinions in this regards. As they did not consider the national security of the country to be under threat in a way that would affect their lives, they did not think that it should be protected to such a degree.

At the same time, they saw a lot of challenges with regard to public safety, which have a direct effect on the life of people. The most frequently mentioned were as follows:

- Going home late/ going home in the dark
- Fear that someone breaks in and robs the flat while not at home
- Fear that something they leave on the street will be stolen (e.g. the car, bicycle)

> *"I have to think about where to park the car"*

- Fear of pickpockets (fear that smartphone/ credit card/ personal documents will be stolen from a bag while using public transport)

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 being attacked.

The lack of existential security was another source of perception of insecurity to be frequently mentioned. The fear of losing one's job, or – on a broader societal level – the problem of high unemployment, especially among young people, were also mentioned as security problems. There were citizens, who thought that the growing number of crimes was often the consequence of an economic downturn and financial instability.

Another popular topic was whether life was safer in big cities or in small settlements. Some felt that in bigger cities people did not take care of each other and that alienation was widespread, while the situation in smaller settlements was better in this respect.

There were participants who connected the higher rate of crime to particular regions in Hungary, where unemployment is very high, and where subsistence crime is a daily issue for people living in smaller settlements.

A few mentioned larger social problems such as the Roma problem[8] or the homeless problem, often with little empathy, seeing them as presenting a threat to general security.

[8] A special social problem here is that the rate of unemployment is very high among the Roma population, while the level of education is low.

> *"Homeless people can spread illnesses."*

In another group of opinions, the perception of legal insecurity and unequal opportunities were expressed.

Distrust of the authorities appeared in comments such as:

> *"The sense of security is undermined from the side of politics, because it is nothing but communication. Those in power can do anything they like." (young male)*
>
> *"If I defend myself, I may be dragged through the mud" (young female)*
>
> *"Those in power can do anything, they make all the decisions and this is frightful." (older female)*

Another common topic related to the state of the healthcare system and to the situation of ill or disabled people in the country. A rather significant source of insecurity was the fear of becoming ill and relying on the healthcare system or getting into hospital.

The context of insecurity was sometimes connected to the surveillance-based technologies themselves: these technologies were seen as measures generating insecurity, especially in terms of the use of the internet.

5.3 Opinions on surveillance-based security solutions in general

5.3.1 Appropriateness and necessity

Owing to many worries about public security, citizens typically only saw the potential advantages of public space surveillance. Cameras not only record the offender and can help in investigations, but their presence was perceived as having a deterrent effect and, at the same time, a positive effect on the subjective feeling of safety. This was the most important advantage that people saw in the use of cameras. In addition, they can be helpful in emergency cases (e.g. a building collapses or someone faints), can be used to protect citizens against the authorities in investigating police brutality. So much can be "*gained*" with them that privacy issues become secondary or do not arise at all. Similarly to the large-scale event, participants of the small-scale citizen meeting also demanded more public space surveillance cameras.

A few people thought that DPI could also have relevance, but the context was rather some kind of control role of how e.g. companies store data connected to purchases and transactions (e.g. credit card numbers). Another perceived advantage of the use of DPI was seen in the possible filtration of economic manipulation against the country. Fighting against terrorism appeared also as relevant in case of DPI, however, Hungarians did not typically fear a threat from terrorism.

> *"CCTV can be accepted, but DPI is not so good, although it could be useful in anti-terrorism." (young male)*

There were cases or situations when, independently of the technology, SOSTs were regarded as inappropriate, e.g. when SOSTs observe personal correspondence and communication. This was regarded as a rude invasion of individual privacy.

Citizens often debated the privacy infringement effect of surveillance, and when someone exposed a negative opinion about privacy infringement, a counter opinion almost always appeared with arguments like this:

> *"Nobody is interested in your private life. They only want to filter out the threat."*

Those opposed to the surveillance-based technologies were often not opposed surveillance as a whole, but its application, e.g. at a table where the topic emerged, CCTV cameras were regarded as acceptable in shops against thieves, but they felt that with a higher camera resolution "*they can also look into a* *customer's purse"*, so they did not support smart cameras. Another reason was that they did not trust the work ethics of the operating staff. Incidents were related by participants, where operators joked at the expense of those being observed. They could not exclude the possibility of recordings from CCTV being illegally leaked (there have already been such cases in Hungary), or that staff might collaborate with criminal circles. It can be concluded that trust of citizens in the operators of these systems does not appear to be very strong.

The majority of participants did not object to the surveillance of employees by employers in order to protect their own interests, but they objected to state of regulation and the lack of information on this subject (e.g. a case was mentioned about a colleague who had been sacked based on secret audio recordings of his opinions, because he was not aware that the camera in question also recorded sound).

Opinions about the relevance and reasonability of SOSTs used for national security purposes were supportive on a general level, however, it should be stressed that the notion of national security was a rather abstract notion. Hungarian citizens tended to view the appropriateness of particular SOSTs from their own perspectives, in other words, from the point of view whether they increased public security and their own feeling of safety. If a direct effect was not felt, participants tended to talk more about the intrusive effect of surveillance. Surveillance was acceptable for them only if they saw direct personal benefits.

With regards to public space surveillance, it was frequently remarked that it would be even better if they worked properly. These remarks referred to several cases when the camera was installed but was not connected to a viewing room or did not record anything, so it did little to improve actual security but only had a psychological effect both on criminals and on the citizens.

The question of proportionality often emerged in the discussions. In this context, the purpose of use was very important. People thought their use as being relevant when, e.g. a camera is used to detect or prevent crime or to ensure that people behave appropriately, i.e. conform to traffic regulations.

> *"The all-important question is how it is used: it is okay to use it for public security but no one should be allowed to sell the data to companies." (young female)*
>
> *"I accept the use of drone, e.g. if a nuclear catastrophe or landslide happens – in these cases they can be sent out to observe whether there are survivors."(middle-aged female)*

For some of the citizens, it was difficult to understand sophisticated surveillance technologies such as DPI. Distrust may be due to a general misinterpretation of how the technology works. There were people, mainly older females, who regarded surveillance as very personal, consequently very intrusive, based on automatic computer system messages.

There were participants who thought that concerns about surveillance were overstressed because of what people had seen in films. The following debate illustrates how people for and against SOSTs tried to convince each other:

> *Female in her 30s: People connect what is seen in movies, they overdimension and overworry these things. They (the SOSTs) don't read the content only search for keywords.*
>
> *Female in her 50s: I do not owerworry it. I don't consider it to be legitimate to monitor my correspondence or bank accounts if I have not given my express permission.*

Another issue that emerged was the cost of these technologies. However, this topic was generally raised in the context that having more or keeping these expensive solutions up to date may be hindered by a lack of available finance.

> *Let's have surveillance cameras everywhere, and let them work properly! But these cameras are too expensive to use everywhere in the city. We have not got enough money for them, even if it's vital. (male in his 40s).*

5.3.2 Awareness of the kind of information gathered

It was partly a lack of factual knowledge and partly the presupposition that any kind of information with regards to a person can be obtained by these surveillance-based technologies that dominated the opinions expressed. Those from the latter group were of the opinion that that data might be related to personal connections, political opinions, *"whether I had an accident*", data registered in the healthcare system, etc.

> *"You can never know; this can be personal or business related. Whatever. That's why I have not brought my mobile here to this meeting with me." (older male)*
>
> *"They can collect anything; what I say to my friends; intimate things." (young female)*

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

> *"I have never thought about how many things can be gathered about me! I went to the bank a couple of days ago and my life was in the bank statement!" (older female)*
>
> *"It's crazy. They need a lot of personal information even for a Supershop card." (middle-aged female)*

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 data bases. 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. They realised or supposed that this data might also be used in a way they would not like it or could not imagine. It was also mentioned that HR people could collect data about them from the internet and might reject their application because of this information.

5.3.3 Effect of surveillance on everyday life

Citizens reacted to surveillance of their everyday lives in a very many ways.

The majority accepted the fact of surveillance and tried to behave rationally: they protect their privacy as much as they can (e.g. do not use credit cards on the internet, do not register on Facebook or carefully select what they upload). However, this change in behaviour was often not a conscious protection against particular threats or abuse of their privacy but was a general precaution, which becomes a habit.

> *"I am not on Facebook, I do not share wedding photos, people have to be realistic, and then there is no problem. I cannot ask them not to monitor me." (older male)*

Other citizens did not give too much thought to surveillance for a various reasons.

One argument was the "I have nothing to hide" attitude:

> *"I am who I am in every situation."*

Other attitudes included a kind of resignation, saying that we were too little to change things:

> *"They observe us but we can't do anything about it." (older male)*
>
> *"I don't worry about surveillance because I am unable to control it." (young male)*

> *"I do not care that I am observed. Why struggle with it? They will get to know what they want to know anyway." (male in his 30s)*

A frequent argument was that if someone does nothing wrong, he/she does not have to worry about surveillance:

> *"People should worry who have skeletons in the closet! I am as white as snow." (40-year-old male)*

Another reason behind ignorance was that people generally do not feel/keep in mind that they are observed.

There were people who argued that their data was not interesting:

> *We are such little things; those they want to observe are Mount Everest compared to us. My data is nothing interesting." (young male)*

Those who did not accept the above arguments often referred to the protection of privacy:

> *We have personal, private things, and I do not like the fact that others could see into them (young female)*

A few were so worried about the use of these technologies that were beginning to show symptoms of paranoia:

> *"I have paranoia. I do not like that we live in such a robotic world. I was born at the wrong time, and I am fleeing." (young female)*

Even those who did not specifically worry about these technologies expressed, that surveillance creates a bad feeling in them.

When asked if he thought such technologies changed people's behaviour, one young man remarked: *"If we change our behaviour, this is one-nil to them."* By which he meant that surveillance is a tool in the hands of the authorities to be used against citizens. .

Another attitude was that, although we have a lot to worry about when it comes to surveillance, we do not have to change our behaviour because everybody knows everything.

SOSTs can also have a positive effect if they motivate people to behave according to common rules. A few participants mentioned that they tend to keep to traffic rules more when they are aware that CCTV cameras are present.

It also emerged that these technologies can increase insecurity, because criminals can steal information from such systems and can abuse them. Another fear was that criminals can find the *"weak link"*:

> *"I just have to tell a security guard that he/she can have 5%, and I have them in my pocket." (middle-aged male)*

There were citizens, who, although they accepted these technologies in the present, were worried about how these technologies might develop in the future.

> *"This is the technological development we cannot predict. Perhaps the time will come when everybody owns three drones."*

5.4 Privacy in the Hungarian culture

There is no direct translation for the English word "privacy" in the Hungarian language, e.g. the Hungarian Privacy Act is called Data Protection Act in Hungarian. The phrase "data protection" is a much narrower concept than the English word "privacy". We used another rather common translation "private sphere" in the research, which is a concept referring to the private life of people, and is often understood as intimacy. The concept was broadened in the information magazine in order that people from different cultures might understand it in much the same terms.

5.4.1 Interpretation of privacy

Possibly partly owing to the translation difficulties, privacy first of all means some kind of personal space, most frequently the home of Hungarian people.

> *"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 a third borderline: this is around their body sometimes referred to as their "aura" or "shell", giving a greater emphasis to their body as part of their privacy.

Another important element of privacy was regarded to be some kind of feeling of freedom that an individual can act and think freely, can decide with whom to share the physical sphere, their thoughts and emotions, with whom to communicate *("Everyone discloses only as much information about oneself as he/she wants")*. Habits, religion, political thoughts and sexual orientation were also listed as important aspects of privacy.

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.

It is largely due to the spread of these new technologies that more and more people have started to include personal and contact data (e.g. phone number, e-mail address, credit card number, passwords, healthcare data) as part of their privacy. They concluded that all types of data belong to the core of their privacy through which a person may be reached or in some way harmed.

5.4.2 Concerns about mass surveillance

Two out of three participants were concerned that the use of surveillance-oriented security technologies was eroding privacy.

Some of those, who did not worry, added that this did not mean that surveillance did not disturb them:

> *"I don't worry (about surveillance), but it disturbs me"*

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 the technological development. And they also worried about themselves, the general public, who would not be able to keep pace with such rapid development.

Another fear was that surveillance technologies are used for political purposes, which might keep people back from, say, attending political demonstrations.

The main rationales behind the concerns can be summarised as follows:

- Concerns about the future
- Being watched is an unpleasant, disturbing feeling
- Surveillance makes people compromised and defenceless
- The universality of surveillance and the possibility of connecting different databases
- It may harm democratic rights

5.4.3 The inviolable core of privacy

The home, the family, personal connections and personal communication were the elements mentioned most often as forming the inviolable core of privacy that should be protected most from surveillance.

Participants at one of the tables debated whether habits or communication should be protected first against surveillance. They came to the conclusion that communication was more important.

One table defined the core as all the information with which harm can be caused to someone whether physical (e.g. credit card number), bodily or mental (capture of communication).

> *"People are concerned that they might suffer a loss. This should be protected."*

At another table, people talked not especially about harm or loss, but about harassment, referring to unwanted phone calls, offers and advertisements.

5.5 Regulation and control around SOSTs

5.5.1 Awareness and a need for more information

Hungarian citizens generally knew little or nothing about the regulation and control of the use of surveillance-based technologies. However, even if they felt they knew quite a lot, it often turned out that this knowledge was rather superficial, e.g. when asked what they knew about these topics, only a few participants mentioned the existence of the Privacy Act, although they were not aware of its contents. One participant mentioned that there is a data protection agency in Hungary. Two participants referred to the data protection ombudsman, although they were not aware of the fact that this office no longer exists[9]. They generally knew nothing about the regulation of the deployment and use of these technologies.

A rather general belief of citizens was that the use of SOSTs was not regulated sufficiently, but even if it was, security agencies would not abide by the rules.

> *"Laws do not protect us as much as they should."*
>
> *"Secret services regularly violate the rules."*

The lack of sufficient regulation was sometimes regarded not as lack of intent but as a consequence of the swift development of the technology.

The lack of sufficient and factual knowledge, a few well-known scandals (e.g. the Snowden case, a recent scandal at the Hungarian National Tax and Customs Administration), as well as a general distrust towards official bodies and state administration seemed to be strongly responsible for the distrust expressed towards regulations and security agencies.

[9] The office of the ombudsman was unlawfully abolished in 2011 and replaced with the National Authority for Data Protection and Information Freedom.

Rumours were also formulated:

> 1st person: *"It is said that Facebook was invented by National Security"*. (male in his 30s)
>
> 2nd person: *"What a great idea! People share their information voluntary!"*

Although people were generally not aware of the regulations, there were some who supposed there should be something on this field. However, concerns were also formulated about the difficulty lay people may have in understanding such matters:

> *"It is certainly regulated, but we do not understand that."*

Another problem of citizens was the lack of information made publicly available about this topic:

> *"There should be some kind of regulations, and those who use these measures are surely aware of them, but no mention is made on the TV news when a new provision is released. It is not pushed in front of us, and we are the ones who should try to find them. But we do not do this."*

Recommendations formulated by the citizens during the large-scale event[10] often included requests for more information about these technologies. Although the demand for more information was also rather strong among participants of the small-scale event, it cannot be concluded that such a hunger for information characterises the majority of Hungarian citizens. One participant remarked that when he participated in the collection of signatures to demand more surveillance cameras in their district, people who signed the petition were not interested in what the cameras would be used for.

It seemed that this hunger for information was partly generated by the deliberation process itself, as, unlike other opinion surveys, it not only collected citizens' opinions, but provided them with information as well as the opportunity to share their thoughts with others. This, in turn, made it possible to formulate informed, more deeply considered opinions. In such a process, when people have the opportunity to directly practice their democratic rights, they understand that the basis of this is to have appropriate and sufficient information.

In this second, small-scale phase of the research, we wanted to better understand the information request of citizens.

They would require more information in the following fields:

- How they themselves are personally effected by the use of SOSTs
- Know the rights of the citizens and the rights of the data handler (who is allowed to pass or sell the information gathered and to whom)
- Who directs these systems, what the purpose of information collection is, and what is its effect on privacy and security
- Interest also emerged at one table related to how growing surveillance might affect society as a whole (they imagined research about this topic by some kind of social research institution)

There was a strong consensus at each table that information should be provided to the different segments of society, starting at school level. The channel of the communication as well as its content should depend on the target group. It was also regarded as important that the language of these information materials should be easily understandable by the general public.

When the content of this education was discussed, citizens expressed their request that this should not only be about SOSTs but also about how to protect personal information uploaded onto the internet or given to companies. Information should also be provided to citizens with regards to the rights of employees who are under observation by their employers.

[10] The citizen summit was held in Budapest in January 2014. The results are summarised in D6:4.

Education about these topics should be provided as early as secondary school, e.g. under the subject called citizenship/civil rights.

The adult population can be primarily reached via the media (TV, radio, printed press, and internet). But they also suggested forums such as the citizen meeting organised for them by the SurPRISE project.

They thought that setting up a legal aid service could also help to provide more information.

There were participants who thought that all the tasks listed above should be the direct responsibility of the state, while others preferred civil organisations.

5.5.2 Expectations towards legal safeguards

The great majority of participants considered it important that people could control the data and information collected about them. However, when discussions were held about the possible ways of realisation, it turned out that such possibilities would also involve risks (e.g. criminals would also have access to this data, if there would be "personal" databases; or if these databases were on the internet, they could also be hacked, etc.). What citizens actually wanted to express by requesting more personal control over their data was another form of expressing a need to better know how these things work, what kind of information is being collected about them and what happens to this information.

With regards to legal safeguards, the most important demand of Hungarian citizens was to establish an independent organisation to control the use of these technologies. This organisation should be free from politics and from the manufacturers and users of SOSTs: "*it should be external*".[11]

The request for legal safeguards was another common topic among the recommendations of citizens during the large-scale event, but these suggestion were given on a rather general level. This research has tried to collect more particular information about what kind of safeguards citizens would expect to be in place when security agencies use SOSTs.

However, this topic proved to be too complex for the citizens, and a relatively small number of the participants could answer the rather detailed questions. Using these answers, the following can be said about the safeguards requested:

- Judicial authorisation by a public court
- Active control by the DPA including individual access to an individual's own personal data
- General monitoring of necessity, adequacy and proportionality of the measure taken

5.6 Differences and similarities in the perception of particular SOSTs

In this chapter, we summarise how citizens see the five SOSTs that were selected for the research: deep packet inspection (DPI), smart CCTV, Drones, Biometrics and smartphone location tracking (SLT). While, in the first half of the meeting, citizens talked about SOSTs in general, in the second discussion round, they discussed one technology in detail.

5.6.1 Deep packet inspection

Observation by DPI did not, in itself, induce significant aversion despite the fact that DPI was univocally regarded as very intrusive to privacy. Participants saw some national security advantages in the use of this measure in intelligence and crime prevention; however, they regarded surveillance by DPI as exaggerated and not at all reasonable.

> *"They observe us even when they shouldn't."*
>
> *"They have plenty of data, which they can abuse."*

[11] We have to add here that in Hungary, the National Authority of Data Protection and Information Freedom is not completely independent of politics, because its leader is appointed by the president based on the proposal of the prime minister. However, the request cannot be interpreted as a political standpoint against the current situation which followed an earlier period of data protection ombudsman, who was really free from politics, because participants had no particular knowledge about these things.

Citizens do not think that DPI increases their personal security, thus they see no direct personal advantages in its use. In fact, the opposite, is true: people fear the exaggerated and disproportional surveillance carried out by DPI in a completely invisible manner.

However, this view was not shared by everybody. There were participants who thought that stepping up national security increases the sense of safety felt by those living in the country. We have to add here that, generally, in everyday life – as mentioned earlier in this report – people do not think about national security in terms of a terrorist threat and see the probability of external attack against the country as very low. Instead, those who expressed an opinion tended to start out from their own direct environment, and their own personal interests.

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

An important negative effect raised by the citizens was that it harms freedom of expression, because the feeling of being observed also affects the way that people think.

An especially important issue for citizens here was how safe the storage of data is.

More people suggested defining and restricting the fields and cases when DPI can to used, and to define the circle of non-affected people, who are not allowed to be monitored using DPI by security agencies.

5.6.2 Smart CCTV

This technology was the best known out of the five discussed and was also perceived as the easiest to understand. Citizens had several personal experiences with the cameras. This is why the perception of this technology often influenced general opinions about the surveillance-based technologies. However, we have to add that smart surveillance cameras are currently not widespread in Hungary. Not everybody found the smart functions so easy to understand. Owing to a lack of knowledge and experience with the smart cameras, opinions often did not differentiate between smart and traditional CCTVs.

CCTV cameras were regarded as the most effective tools to fight the biggest security problems perceived by Hungarian citizens, namely public security. If cameras only film public spaces and do not film private homes, CCTV cameras were generally perceived in a very positive manner. Smart cameras were seen as a possibility to improve the effectiveness of this technology and some people even regarded smart cameras as being less intrusive to privacy than the traditional ones.

> *"If it* (traditional camera) *sees an apartment, the operator can view it, but the smart camera excludes these parts centrally."*

People regarded them as useful in law enforcement because they might help to detect crimes, but their main advantage was seen in their deterrent effect. They were not perceived as tools that could effectively help to solve immediate problems, but – because of their psychological effect – they could deter criminals, thus increase the sense of safety, and provide a direct, perceptible, personal advantage.

CCTV cameras were regarded as expensive, but this aspect was seen more as an obstacle to apply more of them, and not as a financial burden on society.

Cameras were not seen as tools to improve national security. They were perceived as tools to increase the people's personal feeling of security, and to improve public security.

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

5.6.3 Drones

The basic attitude towards drones was positive: they are modern, practical, can be used in several situations when CCTVs cannot (e.g. accident rescue, in remote locations, in large crowds, for following criminals). Citizens saw the main problem as being when it was used for prevention in general and not for particular dangerous situations, or when a disaster had already occurred. They thought that drones violate privacy in these cases because they collect data about innocent people when it is still not sure whether anything untoward will occur.

People thought that drones improve national security, and the fact that Hungary possesses this technology ("*not only the developed West*"), improves the feeling of security. But in order to provide this feeling of security, it is important that people should be aware of the fact that Hungary has drones and when they can be used and by whom. (Some participants did not know that Hungary has surveillance drones.)

Compared to CCTV, drones were perceived as tools that can infringe privacy significantly more. This was seen as the largest risk of their use:

> *"It can get to know more about me, it can come into my garden."*
>
> *"It can follow me."*

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

> *"It can detect me as a burglar in my own flat"*

Owing to the above facts, citizens thought it important that the use of drones should be controlled: who, for what purposes and when is allowed to use them.

Drones were regarded as appropriate in the following cases:

- accidents, disaster, terror attacks
- after a serious crime has been committed (e.g. bank robbery) for following criminals, or in a hostage situation
- in dangerous situation in order to increase public safety (e.g. mass events)

Drones were regarded as inappropriate:

- to increase public security in general, to prevent crime (because they also collect information about innocent people, and too much privacy would be sacrificed – it is not worth it.)
- another reason why it was seen as not a good measure to increase public security was its perceived high costs; the number of the discovered crimes (e.g. thieves) would not be proportionate to the cost of the drones

5.6.4 Biometrics

Biometrics is not seen as "classical" surveillance-based security technology, but rather as a technology that simplifies everyday life.

In addition, citizens felt this technology to still be in the early stages of development. For the time being, citizens appeared to be curious rather than negative about biometrics. However, many said that they would quickly change their minds if they saw evidence that it posed some sort of threat.

> *"We know little about these technologies overall. Because of this, they do not seem to be so dangerous. But where will this process come to an end?"*

Some participants found this technology hard to discuss in any detail because they had little personal experience of biometrics. They also thought that its effect on national security cannot be felt and its use cannot be controlled.

> *"The National Security Service can be controlled with difficulty and we do not have any influence on it; it does not ask for our consent.*

Citizens did not see personal advantages in the use of biometrics, i.e. they did not feel that security would be significantly improved.

At the same time, they thought that we cannot stop developing technological solutions because this would mean abandoning progress, while technology should always be improved in order to make it more effective:

> *"We cannot give up technology because this is the future. We have to keep on improving it."*

With regards to biometrics, people also thought it true that:

> *"Its effectiveness and intrusiveness depends on which situation and what kind of threat we want to defeat."*

The main fear with regards to biometrics was the development of large databases. However, citizens saw the main problem as being in the human factor and not purely in the establishment of such databases. They thought that the human factor should be ethically improved and that control also has an important role.

5.6.5 Smartphone location tracking

This technology was generally seen as not being particularly helpful from the point of view of public security or national security.

It provides a mild feeling of security for users with convenient features (finding the way, following children), but does not prevent e.g. theft.

It was seen as a useful tool in investigating as well as preventing crime only in a restricted manner –, because citizens supposed that criminals or terrorists are aware of this technology and know how to avoid it.

> *If a terrorist came to the country, this would help because he/she wouldn't be carrying a mobile. And he/she could purchase another one right here and avoid being tracked."*

Among the possible positive aspects, participants said that SLT can be used to find lost phones, however, talking about this topic only helped to give voice to their general distrust of service providers:

> *"It is not in the interest of service providers to find lost phones. It is better for them if customers purchase a new one."*

Citizens thought that it is service providers who are not trustworthy rather than security agencies. However, when talking about the intrusiveness of SLT, they also mentioned its negative effect on democratic values:

> *"Because of SLT, people will not participate in demonstrations."*

They regarded SLT as more or less appropriate:

- to find lost people
- to help investigations
- to control those who have already committed a crime

At the same time, SLT was regarded as very intrusive. As well as having a chilling effect on people who want to practice their democratic rights, there was a fear that they could not control the consequences drawn from their location data. One way suggested to avoid location tracking was to leave a phone at home, and it seems that this is quite common.

5.7 Security agencies and legal safeguards

Although a general mistrust towards state authorities and state institutions was generally observable in the discussions, opinions were rather divided with regards to security agencies.

It was apparent from the answers provided that citizens know very little about the information gathering activity of security agencies. Participants agreed that this is due to the fact that these agencies cover their own activities. At the table where DPI was discussed in detail, one participant had a strong opinion claiming that the work of these agencies is organised on the basis of strict rules and under strong control. One controversial opinion was that those in positions of power have too much influence, and might distort the operation of the system. Finally, in the group rating, the table voted distrust in the Hungarian security agencies.

Perhaps the positive attitudes towards CCTV was related to the fact that the CCTV table expressed moderate trust in the security agencies that used CCTV cameras. The police operate most CCTV systems in Hungary, and their potential corruptibility was mentioned as possible cause for concern.

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

- citizens have positive personal experience about them
- no abuses associated with the institution can be heard
- the employees of the institution do not abuse their power, they are not corrupt
- the employees responsible for data handling are well paid (as a consequence, they cannot be corrupted)
- if they are transparent

The main reason that citizens feared that police abuse power was that they often hear about corrupt policemen and about cases when they abuse their power.

At one table, the moderator observed that the topic was unpleasant for some of the participants because the discussion was recorded. The table moderator thought that the positive votes on questions about the trustworthiness of security agencies did not reflect real opinions, which were rather negative due partly to personal experiences.

As the problem of abusing power was often connected to the behaviour of persons operating the surveillance systems, it was suggested that these people should change their approach:

> *"Abusing data is a question of social maturity: currently one can abuse data. But this is a question of social maturity whether it could be solved that people should not abuse them."*

5.8 Reflections on the "trade-off" concept

Participants were asked to reflect on the trade-off concept, i.e. whether they agreed that privacy and security are reciprocal: one can be increased only at the expense of the other. Opinions were divided on this.

At first sight, the trade-off concept seemed to be logical, especially to those who used the SOST context exclusively when evaluating the relationship between privacy and security. However, after talking about this question with table companions and thinking about it more deeply, new points of view were brought into the discussion:

- The most frequent reaction was that security can be improved by methods other than SOSTs as well. There are measures that are not based on surveillance, thus do not decrease privacy while increasing security.
- If an SOST is used for prevention, it harms privacy more than when it is used after the event, because, in the first case, a large quantity of information is gathered about innocent people.

- It always depends on the particular situation whether it is worthwhile sacrificing privacy: e.g. in the case of the drones, their use is felt as detrimental to privacy when they are continuously used for improving public security or for crime prevention, while in the case of an accident/disaster/crime, nobody will be worried that they are also observed by a drone, because people will feel their use justifiable to increase the feeling of general safety.

With regards to biometrics, people thought that the trade-off concept was irrelevant at least for now, because this technology was not regarded as intrusive to privacy. They saw possible problems in the human factor. They completely separated the evaluation of the technology and its user.

5.9 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 find a resolution to this contradiction, and find a racial explanation.

For ordinary Hungarian people, the threat caused by public security is significantly larger than the fear of a terror attack. This is why the use of some SOSTs to increase public security was characterised as "*shooting sparrows with a cannon" (grossly exaggerated)*: it is too expensive and it decreases privacy excessively, while its positive effect on security is not proportionate. However, these technologies do have a role to increase security in particular situations.

There were citizens who thought that, in the long run, it is not the SOSTs that improve public security. It is the root of the problems that should be cured with education, increase of solidarity, job creation, better morals, etc. At the same time, these long-term solutions sound utopian for them especially because of their long timeframe. This is why they rather accept the SOSTs in the present, because they provide immediate solutions. Thus citizens regarded alternatives as highly desirable but only suitable for supplementing technological solutions.

DPI was regarded as being so dependent on the given technology that alternative solutions were not mentioned. However, the DPI table also preferred alternative solutions to SOSTs, although all they suggested were more police and to strengthen civil guards.

The biometric group preferred alternatives less, because they saw effectiveness as the main positive aspect of this methodology, which cannot be replaced by an alternative. However, on a general level, they thought that people need both technological and non-technological security solutions. They mentioned the civil guards, and regarded self-organization and responsibility as important non-technology-based solutions. However, they regarded these solutions as only being relevant in smaller communities.

In the SLT group, the development of civil organisation emerged as alternative solution.

Distrust towards the police was also expressed, when people talked about a stronger police force as an alternative solution. The SLT group regarded the idea of more police as not an especially good solution because of the negative image of the staff (incapability, corruption).

5.10 Recommendations and messages for European and national politicians

The second discussion round was developed in the SurPRISE Decision Support Tool in a way that it would help participants first to discuss the raised topics, and then to come to formulate a common recommendation or message for European and national politicians[12]. In this phase, a second screen was used to show the notes of the note-taker in a way that everybody could see it. Citizens had the possibility to give a title as well add recommendations and messages. Detailed below, the recommendations and messages are listed as they were recorded in the DSS. A brief explanation is provided in some cases to help understanding.

[12] See the methodological description as well as the DSS in D1.4 and D7.3.

5.10.1 Recommendations regarding use

Table: Drones

Title: Proposals for use

Recommendation/message: We regard the employment of drones as advisable by the security agencies, fire service or disaster management; in case of securing large facilities such as nuclear power plants, dams, rescue services (mountain rescue).

Explanation: Citizens regarded the use of drones as not proportionate for general surveillance or for crime prevention both from the point of view of privacy infringement and cost.

Table: CCTV

Title: Proportionality

Recommendation/message: Install CCTV cameras in front of schools, institutions with children, who need to be protected and in places with a large amount of human traffic, such as airports, transport hubs. Proportionality also refers to the amount of data they collect via the cameras. It should not violate people`s privacy.

Explanation: Too few cameras do not have a deterrent effect but it is pointless to install cameras in places that are "not risky".

Table: Biometrics

Recommendation/message: Control and filtering out criminals in airports can be realised more effectively, if biometric data is also used (those involve in crime, drug trafficking or have priors)

Table: SLT

Recommendation/message: Only those should be observed via SLT by security agencies, who have already committed crimes. Other people should not be observed so intensively.

5.10.2 Recommendations regarding regulation and control

Table: Smart CCTV

Title: "Let's be in the picture" (Let us see the overall situation) – human and social control

Recommendation: The scale is positive with regards to the use of surveillance cameras. Human control and independent, outside control is needed.

Explanation: They differentiated between the two types of control. Human control was needed because "machines" should always be controlled by humans; technology works automatically, and this might produce errors that should be corrected. Social control is the control above the user of the technology in order to protect citizens' privacy.

Table: Smart CCTV

Title: Control and improvement of moral values

Recommendation: Internal or external control is needed at the security agencies; the improvement of the moral values at these agencies should be aimed at in the long run.

Explanation: The discussion started out from the topic of corruptibility. In the fight again it, control is important, but the moral values of the staff should also be improved. Participants were aware of the fact that this latter cannot happen from one day to another.

Table: DPI

Title: To define the circle of affected people

Recommendation/message: It is important to clearly distinguish between those affected and non-affected; should not observe everybody.

Explanation: Participants thought that a circle of people can be defined whom security agencies should be allowed to observe. This suggestion supports targeted observation rather than mass surveillance.

Table: Drones

Title: Ideas on regulation

Recommendation/message: Regulation should be as follows:

- should be used only with special permission in order not to avoid abuse: exclusively authorities should be allowed to own a drone or a permission for leading a drone
- smaller settlements should receive financial support for purchasing drones
- use should only be allowed for specific tasks
- citizens should have an overview of regulation – possibilities should be given to them to comment on regulation and express their opinion on it

Explanation: Citizens discussing drones regarded the privacy infringement capacity of this technology as significantly larger than that of CCTV cameras.

Table: Drones

Title: Our trust in the system

Recommendation/message: It would be the power of an independent organisation to decide which authority is allowed to use drones. Employees using them should be carefully selected and controlled.

Explanation: Citizens did not completely trust in the systems that use drones, although they felt they had no other choice.

Table: Drones

Title: Common agreement

Recommendation/message: Regulation should be developed in a way that the decrease of privacy would be acceptable for the majority of citizens.

EU harmonisation: the most appropriate regulation should be developed compared to the regulations of other countries. There should be a unified regulation within the EU on a base level, but smaller national differences should be allowed.

Alternative solutions should also be considered. The two should somehow be mixed: drones and alternative solutions (alternative solutions should be supported financially).

EU examples should be incorporated (in national regulations); it is important not to harm freedom of speech (participation on political events).

Table: Biometrics

Title: Reliability

Recommendation/message: Among strictly regulated circumstances, and only unblemished, credited and reliable people should be allowed to access the data. And also these people should be subject to surveillance and multiple control.

Explanation: Citizens do not have too much overview of the operation of national security agencies, however, in case of central biometric databases, they regarded it crucial that the power would not be abused, and the data cannot fall into the hands of any unauthorised person.

Table: Biometrics

Title: Security, trust, moral

Recommendation/message: In case of sensitive data, the responsibility is even bigger and data protection is even more important. Competitive salary and respect should be given to those who work in such positions. A thorough suitability test should be a prerequisite to the employment. The main aim is that the employee will not be corruptible and data storing will be safe. Control is crucial. A showroom or something like that could be set up to present to lay people how the data are handled.

Table: SLT

Title: Civilian control and transparency

Recommendation/message: Regulation should control the service providers. If data are collected, they cannot be linked with one's personal data. The application would not request location data unreasonably. The user of the application would be able to control their data, or at least would be aware of the data collected.

Table: SLT

Title: Transparency and control

Recommendation/message: We need control and encryption. It should be made possible that I could look at on request what they collect about me.

5.10.3 Recommendations with regards to development of the technology

Table: SLT

Title: Continuous development of the human and the technology

Recommendation/message: Security agencies should develop their own system. They should train their staff.

Explanation: Here the suggestion was based on the news about Angela Merkel's wiretap scandal.

5.10.4 Recommendations for increasing the knowledge based and responsible attitudes of citizens

Table: DPI

Title: We demand information!

Recommendation: Consciousness of individuals is important because they have to decide how to act. But they need information for this. Information transfer can be integrated into education.

Explanation: People who use the internet should be informed about the fact of surveillance and about the possibilities how to protect themselves against it.

Table: SLT

Title: Information and regulation

Recommendation: We would need more information about how SLT affects privacy, and also about its regulation.

Explanation: Participants worried about the consequences of SLT with regards to themselves, and lacked knowledge about what happens with the data collected by SLT, what kind of conclusions are drawn about themselves. They said that if they were aware of the existence of control they would trust more in the technology.

5.10.5 Recommendations regarding trade-off

Table: Smart CCTV

Title: Looking for a balance

Recommendation: We have to define a threshold beyond which intervention into privacy can be carried out. We have to find a balance between security and privacy.

Explanation: Opinions were strongly divided about the relevance of the trade-off concept. It was difficult for them to find common ground to their recommendation which can be regarded also as a balance (compromise) of diverging opinions.

5.10.6 Recommendations regarding alternatives

Table: Smart CCTV

Title: Supplementation instead of substitution

Recommendation/message: Surveillance technologies cannot be given up, but they should be supplemented.

Explanation: Actually, because CCTV cameras were seen very positively, the group did not support alternatives. However, they see some kind of long-term alternative solutions for helping to eliminate the causes of crime. Although these solutions were regarded as not currently realistic.

Table: Drones

Title: Alternative reality

Recommendation/message:

- Police, or an organisation developed on the basis of trustful connections like civil guards
- To increase public security, we would use personal presence not drones. Drones should be used only for particular tasks.
- Relationship of neighbours; they observe each other

Explanation: Participant at this table preferred human presence instead of the technological one (especially not drones), but they did not really trust the police, because of several corruption case. This is why they would prefer alternative solutions also for the police such as civil guards or other civil organisations or neighbourhood watch.

5.10.7 Miscellaneous recommendations

Table: SLT

Title: Increasing the effectiveness of police

Recommendation/message: The staff of the police should be improved. They should fight back corruption.

Explanation: The base of the suggestion was that people do not trust the police.

Table: Biometrics

Title: Unknown

Recommendation/message: With regards to our current knowledge, we cannot evaluate Biometrics. We are on a neutral standpoint.

5.11 Process design

The Hungarian citizen meeting took place in Budapest on 27th of June with 40 participants: 8 around each of the five tables. The location was the entrance hall of a secondary school.

The recruitment was completed by interviewers and group organisers of Medián using the screening questionnaire in the Appendix. In addition, the event was advertised on Facebook, and those interested in the participation could apply by telephone.

54 people registered, 45 received the invitation package together with the information materials, and 40 participated finally.

The event lasted from 5 to 8 p.m. There was a short break between the two discussion rounds.

Besides the table moderator, a note-taker was also sitting at each table. In the second discussion round, participants could follow on a second screen what the note-taker recorded in the SurPRISE Decision Support System.

In the break, coffee and sandwiches were served. Refreshment drinks and glasses were on the tables during the event.

The sample was balanced with regards to gender: 20 males and 20 females participated. The age-distribution was the following: 15 young people (below 35y) 18 middle aged people (between 35-50y) and 7 older people (above 50y). Lower educated people were slightly underrepresented. 3 participants had primary education, 24 had secondary education and 13 had higher education. The great majority came from Budapest, but there were 3 participants arriving from smaller settlements of the region.

5.12 Evaluation of the event

5.12.1 How citizens assessed the meeting

At the end of the meeting, citizens filled in an evaluation questionnaire (see in the Appendix).

Three out of four participants felt that they had gained new insight by participating. Opinions were more divided with regards to whether the meeting has generated valuable knowledge for the politicians: half of the participants thought yes while the other half were unsure about this. Only one participant had a definite negative opinion with regards to the outcome of the meeting.

The most frequently mentioned positives of the event were as follows:

- The possibility to express their own opinion and this was listened to and respected
- It was interesting to listen to other, often very different people's opinion
- The possibility to learn new things (information booklet was also praised)
- Good moderation of the groups and the good atmosphere of the discussions
- Pleasant table companions
- Good organisation (pleasant people, pleasant location, good catering, etc.)

The great majority (80%) could not mention any negatives. If yes, they criticized that not every question or notion was well formulated (3 participants), or made comments on their table companion (3 participants). One participant felt the event to be too long, and one criticized the quantity of the sandwiches with adding a smiley to his remark.

The majority of the participants (65%) did not change their opinion and attitudes with regard to SOSTs as a consequence of participating in the citizen meeting. The smaller part of the others had a worse and the larger part had a more positive opinion as a result of the deliberation. This was in line with what we observed during the large-scale event.

5.12.2 Evaluation of the research design and the DSS by the research staff

Moderators and note-takers[13] (10 persons) were generally satisfied or at least not dissatisfied with the research design and the DSS, however, nobody was completely satisfied.

The main positives of the system that tried to help the deliberation process were as follows:

- The idea of the citizen meeting; it helps the involvement of citizens, it has a kind of socialising effect
- Quick, immediate, real-time, online recording
- Participants can see the raised opinions together in the second round; this makes the process more transparent
- The same structure is used at each table
- Structured notes at the end: possibility of quick overview of the results

The main negatives were as follows:

- Forcing a consensus can have a negative effect on group work (e.g. opinions were sometimes strongly varied, and only one answer could be selected in the group evaluation)
- Time management was sometimes difficult
- Individual voting was better with the clicker system we used during the large-scale event (quicker, immediate feedback to participants)
- Too long (participants became tired by the end of the second round)
- The use of the second screen had little function: part of the participants did not see it or was not able to follow what was written during the discussion

5.12.3 The role of information debate and group dynamics in citizens' acceptance of SOSTs

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

- They helped each other in the formulation of opinions (e.g. clarifying which government body would be responsible for the authorization)
- They broadened each other's views, raised new points of view which others perhaps would not have thought of
- They were thinking about very different opinions as well
- They felt free to give different views because of the group atmosphere
- They could refine each other's opinion
- The exchange of views was appropriate to reveal the different attitudes
- The diverse opinions sometimes helped to find consensus or a common ground to a message or recommendation or consensus (e.g. to define the core of privacy)

There were a few less favourable effects as well:

- There were participants who did not like to talk about sensitive topics, like the evaluation of the police, about distrust (the recording also played a role in this)
- Formulation of a common recommendation or message tended to divert 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 converge, it is easy to formulate recommendations and messages, but when they are too heterogeneous, generally the opinion of the more dominant personalities win despite of the fact that opinions do not come closer to each other. In these cases, those with minority opinion cannot participate

[13] In Hungary, the note–takers were also moderators receiving the same training for the job as those who led the table discussions. At some tables, the two table moderator lead the two discussion rounds in turn

- To send messages to politicians is connected to the picture that people form of politics. If this is negative, then cynical comments also appear in the debate, which might decrease the relevance of others' opinions (fortunately this happened only sporadically; the majority saw the role and importance of politics).
- Based on personal and subjective experiences, sometimes it encountered difficulties to provide general recommendations that can be interpreted also on supranational level (it was difficult to bridge this level-difference)

An observation is that the deliberation process, in such less known, and not very easily understandable or accessible topic, generates information hunger. At the same time, it supports the development of responsible, democratic citizen behaviour, as well as empowering people to think about the raised topics more deeply and with more responsibility. Thus the strong information need and the several requests with regards to the protection of citizens' privacy are partly the effect of the involvement of citizens in the democratic deliberation process of the research.

Such kind of deliberative participatory events would be useful in a young democracy like Hungary, where the desire for the "good leader" prevails instead of an active, thoughtful, and responsible attitude.

The participatory event resulted in strong involvement, and had an effect on participants. Many of them regarded the process itself as a good possibility for science education as well as for involving citizens in political decision-making.

It can happen, that some participant has never thought about the possible risks and side effects of these technologies like the man who said in the debate:

> *"I have never before thought about it, but now that I hear from the others, I can imagine that some use it (the camera) for not especially good purposes."*

Another example is that a participant, who strongly supported CCTV cameras, was astonished that his table companions requested more regulation and information with regards to the use of cameras. He argued based on his own experiences that normally people are not interested in such information.

6 Country report of Italy[14]

This chapter[15] reports the findings of the Italian 'citizen meeting' (or small-scale event), held in Florence on June 17th, 2014, at the European University Institute. The event lasted over three hours and gathered 47 citizens. They were divided into 6 well-assorted tables and each group was facilitated by a moderator. Participants met to discuss security, privacy and surveillance issues, to answer a set of questions on smart CCTV, deep packet inspection (DPI), smartphone location tracking (SLT), drones and biometrics[16], and to formulate recommendations for European and national policy makers.

The chapter is divided into 5 sections. Section 1.1 contains a summary of the main results. In section 1.2 we illustrate the results of the first working session of the citizen meeting (SOST-neutral), whereas the outcomes of the second working session (SOST-specific) are described in section 1.3. Section 1.4 is dedicated to the process design. Finally, in section 1.5, we summarize how participants and moderators evaluated the event.

6.1 Executive Summary

This citizen meeting is a follow-up to the citizen summit held in Florence on February 8th, 2014, and was designed on the basis of the summit's outcomes[17]. Similarly to the summit, the citizen meeting was an opportunity for citizens to actively take part in the decision-making process. Moreover, as in the summit, participants discussed surveillance-oriented security technologies (SOSTs). Citizens expressed their attitudes on surveillance technologies, security and privacy by making reference to real-life situations.

Research-wise, the citizen meeting aimed at collecting more in-depth information about what affects citizens' acceptance of security measures and their view on trade-offs concerning security and privacy. In particular, it addressed the following issues, which were left unanswered in the February event.

The meaning and perception of security

- **Perception of security:** People feel fairly secure in their daily life and believe that Italy (Tuscany) is generally a safe place to be.
- **Main security challenges:** citizens think of different threats at the individual level (violence, physical aggression, misinformation, lack of control) and national level (quality of life: lack of social cohesion, economic insecurity, threats to the welfare system, environmental challenges, food poisoning and natural disasters).

It is interesting to note that at the citizen summit the share of respondents feeling secure in their daily life and in Italy amounted only to 42.8 % and 38% respectively (while here the corresponding numbers are 76% and 66%). There are two possible explanations for this divergence that, however, should be investigated further. One has to do with the voting method: participants in the citizens' summit voted anonymously with clickers, whereas at the citizen meeting they casted their vote publicly at tables. The sense of insecurity might have been perceived as a weakness that participants were reluctant to share publicly. The second explanation may relate to the different socio-demographic composition of the sample at the two events, in particular as regards age, educational level and being part of a minority.

Perceptions about surveillance in general, and SOSTs in particular

- **Use of SOSTs for specific threats:** citizens proposed: DPI for terrorism, child pornography, and to fight financial speculation; drones and SLT to look for missing people and natural disasters; smart CCTV for irregular migrants. SOSTs should be used to fight petty crime, terrorism, the consequences of nightlife, and to monitor public places.

[14] The authors of this chapter: Maria Grazia Porcedda (EUI, SurPRISE) and Teresa Talò (EUI).

[15] The authors wish to thank Claudia De Concini and Bart Provoost for their help in drafting this report.

[16] For a discussion of these technologies in the Italian context, see Maria Grazia Porcedda and Melissa Zorzi, 'Deliverable 6.5 – Country Report Italy. Surprise Project', Florence, European University Institute (2014).

[17] The results of the large-scale event form part of a different report: Porcedda and Zorzi (2014).

- **Impact of surveillance in daily life:** citizens have the impression that a lot of personal data are collected and worry about surveillance, but only few are ready to change strategies according to different circumstances;
- **Acceptance/acceptability of SOSTs:** Smart CCTV is the most accepted; SLT is the most well-known and convenient, whereas DPI creates the greatest concerns. SOSTs are OK if used to protect the needy, when necessary and if regulated by the law.

The general unawareness regarding what data is processed through SOSTs, the fatalism concerning data collection in our society, the apathy relating to different uses or exposure to SOSTs are in line with the outcomes of the large-scale event held in February. Citizens declared to worry about data processed by SOSTs and generally wished to know more. However, changing behaviour was not considered an option, either due to the convenience of technology, or because citizens do not know how they could avoid the pervasive effects of SOSTs.

The meaning of 'privacy' and the existence of a core

- **Meaning of privacy:** for citizens, privacy means freedom to be in control of personal information and respect for private life;
- **Do they worry for privacy?** Citizens were quite concerned about mass surveillance;
- **Is there an inviolable core? C**itizens identified the core as made up of: medical data, vulnerable people's data, religious and political beliefs, sexual orientation, and personal communications.

During the citizen summit held in February, the rate of participants worrying for the impact of SOSTs on their personal privacy was similar to that of the citizen meeting. However, the summit's participants worried more about privacy of the collectivity, whereas, during the citizen meeting, citizens' opinions were divided. This is an interesting result that requires additional research.

Transparency, applicable law, legal safeguards, and control

- **Transparency about SOSTs:** citizens expressed the desire to increase the low level of awareness about SOSTs. Public institutions should be in charge of ensuring transparency. The SurPRISE project was seen as a good tool for dissemination.
- **Applicable law:** ***attendees claimed to have*** limited knowledge about existing laws.
- **Legal safeguards:** citizens preferred strong safeguards, which would also increase trust.
- **Control:** most participants wished to have greater control, and to have instruments in place allowing doing so.

The results of this part of the citizen meeting provide important insight into the outcomes of the large-scale event. On the one hand, it confirms that citizens believe public institutions should be in charge of informing them about data collection and of providing greater transparency (which is understood as a precondition for real controls and respect for privacy). Also, citizens fear that private companies might misuse their data. *On the other hand, it gives a deeper understanding of the kind of legal safeguards strongly demanded (but not articulated) at the large-scale event.*

Trust in public institutions using SOSTs and fear of abuse

- **Trust:** most citizens trusted public security agencies[18] fairly high, but not unconditionally. Institutions should be accountable;
- **Fear of abuse:** the majority of citizens did not fear abuses, and tended to be more suspicious of usage of data by private parties.
- **Factors increasing trust:** legal safeguards, accountability and information could lead to higher levels of trust.

[18] Security agencies were defined as in the large-scale event, namely the different government bodies which are responsible for maintaining security, law and order (including a nation's territorial police forces, special police forces and border agencies). In Italian we used the word "Autorità di pubblica sicurezza", accompanied by the definition and some examples.

Effectiveness and intrusiveness of SOSTs

- **Reliance on SOSTs**: citizens believed we should not rely only on technology; it is useful if individuals interpret the results (in other words, technology is useful if integrated with traditional investigation methods).
- **Future uses**: the use of SOST should be based on the elaboration of precise plans and strategies.

The trade-off model

Citizens did not discuss in terms of trade-off before the related question was asked. Many citizens seemed not to accept the trade-off reasoning, and believed that legal safeguards and community building would eliminate the need to trade privacy against security. However, when prompted, some citizens did conform to the trade-off model and stated to be ready to give in privacy for higher security. This may confirm that even if some citizens do not formulate the problem in terms of a trade-off, they may conform to its tenets when presented with them.

Alternatives to surveillance and SOSTs

The overwhelming majority of participants seemed to insist on the need to fight a widely felt moral decay and on the importance of investing in community building.

6.2 First session of the citizen meeting (SOSTs-neutral)

This section addresses the main outcomes of the citizen meeting's first working session. In this phase, participants had technology-neutral discussions about four introductory topics: perceptions on security (6.2.1); perceptions on surveillance-oriented security solutions (6.2.2); the meaning of privacy (6.2.3); the role of regulation and safeguards (6.2.4). We discuss the outcome of the debate on each topic in sequence.

6.2.1 Perceptions of security

A majority of participants declared that they generally feel secure in their daily life (76% agreed or strongly agreed) and that they consider Italy a safe place to live in (66% agreed or strongly agreed). Although with many exceptions, there was a general sense of personal safety. Only 19% declared not to feel secure in their daily life. Some motivated their answers:

> *"I do not trust the authorities that should deal with security" – DPI table*
>
> *"The country is very fragmented… also, corruption makes me feel that this is not a safe place to live in" – 32 year old male professional*

Technology generally was not brought up at this stage of the discussion; however there was a citizen that motivated his general feeling of insecurity stating:

> *"Security is not given by technology but by interpersonal relations and they are not so strong anymore" - 2nd CCTV table*

However, when citizens were directly asked what they perceive as security threats, many fears were revealed. Furthermore, similarly to the outcome of the citizens' summit held in February, individual safety and societal/national security concerns generally differed. At one table (biometrics) it was explicitly remarked that answers to questions regarding security changed very much according to the context used as reference ("Tuscany is safer than the rest of Italy") and whether one considers immediate threats like physical aggression or wider phenomena such as environmental problems. Indeed, perceptions of security seem to differ greatly depending on the frameworks considered (e.g. personal vs societal, narrow conception of security vs wider outlook). People initially had a tendency to consider a narrower definition (this led many to dismiss concerns) while, later on in the discussion, they delved deeper into the issues and considered many threats that did not immediately come to mind when the word "security" was mentioned.

6.2.1.1 Perception of security at the personal level

The most frequently mentioned security challenges were physical *aggression* and violence. In particular, one woman reported being scared of walking late at night in isolated places (DPI table). Isolation was also mentioned by a woman as a factor that made her fear aggression. Another recurrent theme was that of *robberies*. Many referred to thefts in their home while others talked more generically about violation of property. A man said that he does not feel safe because thieves broke into his house three times already. A few participants stated that they do not have any personal security concern. Some examples are:

> *"I am not scared of anything" - 22 year old student male*
>
> *"I am an optimist, I am not scared" - 60-70 year old male*

At different tables, there were some citizens that mentioned *misinformation* as a security concern. This theme was widely debated at the biometrics table. The main argument brought forward at the table was that if people are ill informed they could make wrong and risky decisions. They gave the example of a plant in southern Italy (ILVA) that was later discovered to have endangered the health of its workers; citizens said that if people had been correctly informed, they could have avoided these risks.
A recurrent theme that emerged in people's discourse was insecurity due to *lack of control*.

> *"I am not able to control what is going on around me" -middle-aged woman*
>
> *"I don't feel safe because the world today is unpredictable" - middle-aged woman*
>
> *"I am scared of processes and decisions that I do not control" - retired man*

Similarly, some mentioned the "unknown" and an insecure future as sources of concern.

6.2.1.2 Perception of security at societal level

When considering society as whole, answers became more abstract, and citizens pointed at less obvious threats. In particular, participants seemed to be defining security mostly in terms of quality of life.

Many participants at different tables pinpointed "lack of *social cohesion*" as the main threat to security. Social disaggregation, indifference to others' needs, individualism, and lack of communication were mentioned. In particular, a citizen at the DPI table elaborated on the absence of a social safety net made up of friends and neighbours that are willing to help. A participant concluded that:

> *"Social relations are key to understanding risks and to have a general perspective. Also, they determine how resources are distributed within society. The lack of social relations therefore creates problems and inefficiencies" - biometrics table*

"*Cultural impoverishment*" and "*moral decay*" were also often cited as threats to security. Interestingly, these threats were generally accompanied by a sense of decadence. The feeling that gets through is that there used to be moral values and higher levels of culture but that they are withering away.
Another important topic that was brought up is *economic insecurity* and *unemployment*. A participant mentioned "world economic policies" (CCTV table 1), many cited youth unemployment, and someone pointed out that the "depletion of the welfare system" (drones table) was troublesome. Furthermore, a couple of participants referred to their personal fear of losing their job.
Some participants believed that *environmental* concerns are important security threats. Pollution, food safety, and natural calamities were among the issues mentioned.
Only a minority of participants mentioned classical security issues such as corruption, organized crime, and uncontrolled immigration. Terrorism was mentioned once; citizens seemed to worry more about misinformation and manipulation of information.

6.2.2 Opinions on surveillance-based security solutions in general

6.2.2.1 Appropriateness and necessity

A few participants said that SOSTs are appropriate when *regulated by the law*. However, one citizen (DPI table) pointed out that it is however hard for the law to keep up with the fast pace with which technology evolves (drones table). Someone else (1st CCTV table) specified that the government should not use SOSTs; rather, access needs to be limited to judicial authority. Some noted that authorities should use information collected through SOSTs only when necessary (drones table). One particular citizen said:

> *"It is appropriate to use these technologies only in the context of a well-functioning democracy. Ideally, those who deal with these technologies should do this for the public interest and only when it is necessary, for example, for climate change, storms, hurricanes, and fires" – 2nd CCTV table*

Interestingly, one person mentioned he would be more worried should Italy be ruled by a repressive regime (drones table). Two citizens declared that SOSTs are useful to *control potentially dangerous individuals*, while another participant proposed to monitor those that already committed a crime and to "spy on criminals using drones" (1st CCTV table). Furthermore, a citizen stated:

> *"These are means to fight problems (repressive strategies) but they cannot solve underlying problems (preventive strategies)". – 1st CCTV table*

It was pointed out at different tables that these technologies might be appropriate if used to *protect those in need*. One participant mentioned children, the elderly, and people with specific problems (drone table). Another citizen at the drone table said that SOSTs might be important for those that are ill (but then he added "if someone collapses will a drone detect it?"). Finally, a participant said:

> *"Geo-localization can be very important, for example, to find a lost child" - young unemployed woman*

Some citizens were rather *sceptical* about SOSTs being appropriate at all. Some mentioned specifically drones as dangerous. (A possible explanation could be that in Italian media they are often associated with military operations.) Referring to what was said concerning security challenges, some citizens (first CCTV table) claimed that SOSTs are not a solution to "moral decadence" and that they are not appropriate means to guarantee security. Likewise, at the second CCTV table a participant noted that surveillance is based on the "myth of machine's control", which however cannot replace good upbringing and manners. Participants also brought up the issue of manipulation for commercial purposes.

Other applications proposed for SOSTs included: DPI to control paedophile online activity and to block financial speculation; CCTV to identify irregular immigrants; and SOSTs in general to fight petty crimes, thefts, terrorism, and monitor public spaces and nightlife.

6.2.2.2 Awareness of the kind of information gathered

Participants seemed to have a vague idea about what information is actually gathered by SOSTs. They tended to assume that every aspect of one's personal life is accessible. A citizen (sarcastically) said:

> *"If they wanted to, they could know what our DNA is! They know everything!" - 2nd CCTV table*

There seemed to be a fatalistic attitude, as if these technologies were very powerful but out of one's control. A citizen said:

> *"I prefer not to know - anyways they definitely collect a lot of information." - Drones' table*

While many simply stated that "a lot" of information was gathered by SOSTs, some gave more precise examples such as: physical characteristics; everyday habits; online searches; email content; income; geo-localization; economic activities; consumption habits; lifestyles; and who they are friends with.

6.2.2.3 Effect of surveillance on everyday life

Answers to the structured questions reveal that the majority of participants rarely or never worry about the use of SOSTs. However, about 47% of respondents affirmed to worry at least sometimes.

An interesting finding was that participants believe it is hard to know what behavioural changes would be effective for protecting personal data. Also, knowledge about what and when information is being collected is often lacking. Consequently, some voiced the need to have greater transparency. A considerable number of participants expressed the idea that they *would like to be able to control* what information they reveal through their use of SOSTs *but don't know how to do so*. Some examples are:

> *"Those that are not tech-savvy have a hard time knowing how to defend themselves from these things… But it's hard also for experts" - Middle-aged woman, university lecturer*
>
> *"It is necessary to have rules that are simple to understand" - Middle-aged man*
>
> *"I used to think about this stuff but then I gave up trying to control my information… it's too complicated" - Biometrics table*
>
> *"I don't change my behaviour because I am not aware of what information is being collected" – 2nd CCTV table*

A minority of citizens reported that privacy concerns affect their behaviour when using the Internet, some examples being: using social networks sensibly, changing passwords frequently, browsing anonymously, and avoiding certain banking operations. Others, however, do not change approach. One participant noted that people tend to pay more attention to privacy in the aftermath of shocking news (e.g. the NSA scandal), but afterwards they slip back into their old, careless habits (first CCTV table). Another participant (drones table) formulated the interesting opinion of a trade-off between convenience and surveillance:

> *"I use SOSTs and do not change my behaviour although I am aware that by doing so I am giving up part of my freedom – it is a trade-off against convenience".*

A major concern citizens expressed was that their *data might be misinterpreted or manipulated*:

> *"I am worried that my actions may be misunderstood" - Drones table*
>
> *"I am scared about data being manipulated, how it is used, who interprets it and how" - Biometrics table*

Some participants stated that they never worried because they *don't care* about what information is gathered about them. A couple of citizens furthermore stated that they have "*nothing to hide*".

Additional concerns that participants pointed out regarding the use of SOSTs are: giving their information when they register for an online service, information posted on Facebook and other social networks, and (frequently) online banking and credit card information.

6.2.3 Privacy in the Italian culture

6.2.3.1 Interpretation of privacy

There was a fair degree of homogeneity across tables and participants as to what a possible definition of privacy could be. The general idea that got through is that privacy means to respect an individual's freedom to choose what is exclusively private. Definitions seem to include both the confidentiality of personal data and the intimacy of private life (that is, both rights to the respect for private and family life and the protection of personal data[19]). The words *respect* and *freedom* recurred across tables a significant number of times (8 and 6 citizens respectively). The latter suggests that some citizens saw privacy as an inherently individual right. Some examples are:

> *"[Privacy is] the freedom to think and act without being observed" - Middle-aged woman, first CCTV table*
>
> *"It means to respect each individual" - Drones and 1st CCTV table (exactly the same words were reported)*
>
> *"[Privacy is] the freedom to be oneself" - DPI table*

Also, many thought of privacy as the possibility to create boundaries that entitle them to a *private secluded sphere*:

> *"It means to have a place in which I can be alone or with those I love" - SLT table*
>
> *"It means to respect people's intimate sphere" - drones table*
>
> *"It is the power of citizens to decide where private boundaries are traced" - young man, biometrics table*
>
> *"It means to be in charge of what others can know about me and to decide what is, instead, private" - DPI table*

Furthermore, *legal protection* of private data was mentioned as an important component of privacy. A participant stated:

> *"Privacy means making personal information accessible only for substantiated legal reasons" - DPI table*

SOST	Words used to define privacy
DPI	Freedom to be oneself; respect; secret; what I want to keep for myself; right to behave as I believe in; a burden (a false privacy): I wished it had a real weight.
Smart CCTV 1	Defence/offence; to act and think shielded from external observers; respect of the individual; to disclose only what I want; unavailability of one's information, unless requested by judicial authority; reciprocal agreement not to damage others' information.
Drones	Respect of one's opinions and of the person; right to have a private life; protection of sensitive data; personal data processed for necessary and limited purposes.
Biometrics	Not to have my data manipulated; we have no choice, we are forced to consent to the use of data; some sensitive data should not be collected; a convention of what we decide to disclose about ourselves; the citizens' powers to establish their boundaries.
SLT	Utopia; protection of private life, confidentiality; protection of all personal data; a space where you can enjoy solitude or family life; freedom > privacy (verbatim);
Smart CCTV 2	Fundamental right; respect (twice); confidentiality and liberty; decide if and to whom to disclose information on personal habits; liberty; keep silent without this raising suspicions.

Table 1: The meaning of privacy for participants

[19] As defined in articles 7 and 8 of Charter of Fundamental Rights of the European Union, Official Journal C 303/1, p. 1–22, 14 December 2007.

6.2.3.2 Concerns about to mass surveillance

A majority of participants indicated that they were either very worried or worried about SOSTs' impact on privacy (62%). One participant that declared not to be worried said:

> *"My personal information is not interesting, so I'm not worried" – 1st CCTV table*

Another citizen (fatalistically) believed that there is no reason to worry because she believes that privacy cannot exist:

> *"I am not worried for my personal privacy – privacy has become a utopia on which individuals have no control. At this stage, it is better to have less privacy and more security" - Middle-aged woman*

One of the participants that declared to be worried stated that his main concern was the unforeseeable future developments of SOSTs (first CCTV table).

Citizens were also asked to assess if their level of concern would be different according to whether they looked at the issue form an individual or a societal point of view. At two tables citizens agreed that their opinion would indeed change (to privacy's disadvantage):

- DPI table: in certain public settings (i.e. stadiums) surveillance should be more important than privacy;
- First CCTV table: the "common good" is more important than individual privacy.

On the other hand, at other two tables (biometrics and the second CCTV table), participants said that their level of concern was the same whether an individual or societal perspective was adopted. In particular, at the biometrics table, a citizen stated that: "a good management of individual privacy leads to a good management of collective needs".

6.2.3.3 The inviolable core of privacy

Participants believed that "sensitive" data should never be subject to intrusion. This includes: information on health; sexual orientation; political and religious beliefs; generic sensitive data; one's thoughts; and personal communications. Furthermore, attendees stated that the inviolable core of privacy should be such that fundamental rights and the possibility to act freely need to be guaranteed (DPI table).

A few people mentioned data regarding vulnerable individuals (also on social networks) as the inviolable core of privacy:

> *"Data concerning children, people with health problems, and foreigners need to be particularly protected" - middle-aged unemployed woman*

Lastly, citizens sitting at the second CCTV table agreed that the inviolable core of privacy is made up of family life, what happens within private homes, and everything concerning people's intimate sphere.

6.2.4 Regulation and control around SOSTs

Regulation and control of SOSTs was the last topic discussed in the first session of the citizen meeting. Participants were first asked about their level of awareness of the applicable law and the safeguards already in place, as well as their desire to learn more and additional information (5.1). They were further asked about the extent to which they would like to gain additional control, and what legal safeguards there ought to be when SOSTs are used by security agencies.

6.2.4.1 Awareness and a need for more information

The level of awareness regarding who controls SOSTs and how they are regulated is rather low. In fact, 51% of participants stated that they had only some knowledge of these issues and 32% declared that they knew nothing or very little. Those that had a higher level of awareness generally said that they gained it thanks to their professional expertise.

In general, participants were interested in learning more about regulation and control of SOSTs (as emerged earlier when discussing surveillance) used both by public and private institutions. In particular, citizens sitting at the DPI table had articulated a wide range of questions:

- How do 'they' gain access to my personal data (e.g. also the mobile phone)?
- Are my data sold?
- How can I avoid it?
- What can I do if I'd like to keep certain information private?
- How do I find out what is the applicable law on data protection?
- How do laws regulate this field? Are they in contrast with other states' laws?
- How can an average citizen be protected?
- For how long personal data be kept?

A citizen at the DPI table was interested in knowing:

> *"Who are they [people that use personal data]?...Who is Google?".*

This sentence is a good example of citizens' frequent use of the word 'they' (also highlighted above), understood loosely as anyone who can access and process technology-generated data. This semantic choice seems to reinforce the finding mentioned earlier: citizens are not particularly aware of who can control their data and where it ends up.

Who should provide more information?

Most citizens said that the responsibility of providing more information lies in the hands of *public institutions*. Among those cited there are: the government, the police, the ministry of interior, the data protection authority, public administration, and municipalities. With regard to children, a couple of citizens mentioned schools. One participant said:

> *"The schooling system is responsible for providing this information to children, while the state should do so for everyone else" – drones' table*

Furthermore, many mentioned the *media*. In particular, sources such as newspapers, TV channels, Internet, leaflets, public institutions' websites, and even YouTube were proposed. Several participants stressed that it is essential to make communication on these issues *clear* and understandable for the layperson. At the second CCTV table, citizens said that a project like SurPRISE is a good way to raise awareness among the public.

6.2.4.2 Expectations towards legal safeguards

Citizens' control over their personal data

The vast majority of participants believed that citizens should be able to control their personal data and information. 66% said this was very important while practically everyone (94%) indicated that it is either important or very important.

Generally, citizens indicated that a precondition for tighter controls is gaining knowledge as to what information was gathered about them. Some mentioned the "Do not call" registry. Others pointed out that it would be useful if there were websites in which they could check what personal data were collected about them. Additional suggestions include databases, cloud-based and password-protected public registries. Also, several citizens expressed the wish to be able to delete the information that they do not want to share. The right to be forgotten was explicitly mentioned at the biometrics table. A couple of participants said that they ought to be notified whenever information about them is being collected, and that transparency is essential. As formulated by one citizen:

> *"It [data collection] needs to be regulated: as soon as my information has been registered somewhere they need to inform me and allow me to delete my data" – 1st CCTV table*

Expected legal safeguards

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 ex post verification of correctness. Most citizens said there ought to be a medium-high to high level of protection of their personal data.

In particular, when asked if they believed there should be a judicial authorization to get access to personal information, most (57%) said that they expected there to be a judicial authorization without hearing. However, a third of citizens (32%) stated that a hearing should be necessary. With regard to the protection of personal data being processed, most citizens (62%) expected that they should be subjected to the DPA's active control *and* that they should be accessible to the interested data subject. Finally, citizens were asked how the verification of a correct data processing data should take place. The most common answer (66%) was that the fulfilment of the principles of necessity, appropriateness, and proportionality should be assessed by means of judicial review.

It is important to note that *none* of the participants declared that public security agencies (as defined in note 5) should be forbidden to access data generated by SOSTs.

6.3 Second session of the citizen meeting (SOST-specific)

This section focuses on the results of the second session of the citizen meeting. There, each table was associated with a SOST (Smart CCTV being analysed twice) which was unpacked from several angles: pros and cons, effectiveness and intrusiveness (6.3.1); use by security agencies and related legal safeguards (6.3.2); potential trade-offs (1.3.3); and alternatives (6.3.4). Participants were asked to reach a conclusion ('recommendation', 6.3.5) for each of these themes participants assessed the consensus reached.

6.3.1 Differences and similarities in the perception of particular SOSTs

The following paragraphs include considerations regarding: how acquainted participants are with each technology; their pros and cons; whether they are a useful tool to promote security; and how intrusive they are.

6.3.1.1 Deep packet inspection

None of the participants at the table had any familiarity with DPI except for one citizen that declared to have seen it rarely. Also, it was one of the least well known among the SOSTs discussed.

Citizens sitting at this table suggested that the main use for this technology could be within the context of judicial investigations. In fact, they pointed out that it could be useful to look into criminal activity and child pornographers online. Also, some signalled that DPI made everything traceable and more transparent. Participants disagreed on whether DPI can be an effective way to protect personal and national security. Some said they could only judge on a case-by-case basis. One citizen specified that this depended also on how "righteous" the government is and if fair and effective regulations are in place.

However, all participants were very worried about the negative impact this technology could have on individual privacy. Some specific concerns were that this SOST could limit freedom of thought and that personal data could be manipulated, modified or interpreted out of context (participants suggested that other tools are needed to interpret the data). Also, participants believed that clear boundaries had to be drawn to limit the use (e.g. by governments) of such a potentially intrusive technology.

6.3.1.2 Smart CCTV

Given the unexpectedly high number of participants in the citizen meetings, two tables for CCTV were set up. Interestingly, most citizens sitting at the first table had no familiarity with CCTV, while at the second table, *all* participants stated that they had often seen CCTV cameras. Besides this discrepancy, however, answers given at the two tables were remarkably similar. It should be noted that it is not always clear whether citizens were discussing about the smart or simple version of CCTV cameras.

(Smart) CCTV was one of the most positively rated SOSTs among participants. As for pros, at both tables, it was pointed out that (smart) CCTV could be more successful and more cost efficient than human control (however, nobody raised the issue of maintenance). In fact, participants stated that humans could be more distracted and less impartial than (smart) CCTV. Also, they said that it is easier to manage a large amount of information using technology. Citizens identified crime prevention as one of the key positive aspects of (smart) CCTV. In fact, they emphasized that CCTV can immediately detect illegal or dangerous behaviour and deter people from engaging in it. Furthermore, citizens agreed that CCTV has the potential to be a useful technology to enhance individual and national security. However, they specified that it "has to be used properly" and that it cannot entirely substitute human supervision.

On the cons side, citizens were mostly worried that data could be misused. At both tables, the possibility of "false positives" and "fake alarms" was evoked. Also, some participants mentioned that technology can be imprecise and cannot contextualize actions. Moreover, attendees acknowledged that CCTV could break down or be vandalized. One citizen also said that being controlled could, on the contrary, make citizens feel insecure. However, most participants agreed that this is the least intrusive SOST. At both tables, it was stated that whether CCTV is intrusive or not depends on *how* it is used:

> *"It depends on what purposes it's used for" – 1st CCTV table*
>
> *"If the objective for which it is used is to improve services for citizens, it is not intrusive" – 2nd CCTV table*

6.3.1.3 Drones

All participants at this table declared that they had never seen drones.

Citizens believed that drones could be useful to monitor large areas and intervene quickly when people are in danger. Accordingly, someone gave the example of emergencies (e.g. a fire, rescuing missing people) as a situation in which drones could be useful. In general, participants stated that drones could promote national and personal security when used correctly.

On the other hand, participants stated that an important downside of drones is their reduced visibility, which increases the perception of intrusiveness (a few participants, in fact, suggested that they should be signalled). In particular, a citizen was wary about drones monitoring private areas and said "tapes should be destroyed". Moreover, it was suggested to create a registry of privately owned drones.

6.3.1.4 Biometrics

Most of the citizens sitting at this table stated that they rarely saw or had any contact with technology capturing biometrics.

Participants pointed out that biometrics can be particularly useful in the context of investigations or to ensure security in the workplace or while traveling. Also, another proposed advantage is that biometrics speeds up control procedures. This could make people feel more secure and be a deterrent for criminals.

Most citizens believed this technology is very intrusive. In particular, they reported being worried about potential errors that could occur when identifying someone. Two citizens emphasized the risk of personal identity being forged. Furthermore, some were worried that – when combined with other technologies – biometrics could be revealing "too much" personal information. Participants were in fact particularly interested in knowing how much information could be gathered using biometrics. It was suggested to limit the authorization to access biometric data.

6.3.1.5 Smartphone location tracking (SLT)

This is the technology the citizen meeting's participants were most acquainted with. In fact, most participants sitting at the SLT table said they were exposed to it all the time. Overall, citizens agreed in considering SLT a rather convenient technology. Some of the advantages mentioned included getting information quickly and finding places easily. Also, participants said that SLT makes them feel more secure because people "can be tracked down easily if they're in need of help". One citizen said that it could be a useful tool for the police. Conversely, however, a participant pointed out that dependence on this SOST could *decrease* personal security:

> *"These technologies can diminish people's autonomy and this, in turn, could be an obstacle to their personal security".*

Some of the negative aspects that were brought up are that the data gathered could be used inappropriately and that people may become overly reliant on it:

> *"Young people do not have a sense of direction anymore!"*

Attendees did not consider SLT particularly intrusive. However, once again, the importance of transparency was remarked. There was a general consensus around the statement: "it is intrusive if I do not have the possibility to decide whether I am geo-localized". Furthermore, a citizen lamented that people nowadays are "forced" to use this technology because of its convenience and therefore have to accept whichever level of intrusiveness. In general, in the discussion on SLT, a trade-off between convenience and privacy seemed to emerge.

6.3.2 Security agencies and legal safeguards

An overwhelming majority of respondents (87%)[20] stated that security agencies (that use SOSTs in Italy) are trustworthy. A similarly high rate (66%) of voters[21] disagreed or strongly disagreed with the statement whereby security agencies (that use SOSTs in Italy) abuse their power.

Such results depart from the outcomes of the large-scale event, where a strong majority doubted that security agencies do not abuse their powers when using SOSTs[22]. Not only is the level of trust in security agencies in line with other studies[23], but also fear of abuses might decrease vis-à-vis the scepticism surrounding the commercial usage of personal information. Indeed, some citizens said that they trusted public security agencies more than private companies (biometrics table) when it came to processing of their own personal data.

In general, citizens' trust is not unconditional, and many felt that discretion should be limited. One participant said that he is worried about "impunity if there are abuses of power" (1st CCTV table). At the drones table, participants agreed that they trusted security agencies but that their actions should be traceable and that they shouldn't have unfettered discretion.

As for the 30% of voters who feared abuses, a possible explanation, also hinted at in discussions, may be linked to the ignorance surrounding SOSTs' regulations and to how information can be used (rather unsurprising in Italy[24]). Instances of statements in this sense include:

> *"We need to have more information on how public authorities use personal information" – SLT table*
>
> *"How do they use information? We don't know!" – 2nd CCTV table*

[20] 33 responses over 38 voters. The voting results of one table are missing.
[21] Over 38 voters. The voting results of one table are missing.
[22] Porcedda and Zorzi (2014).
[23] Ibid.
[24] Ibid.

6.3.3 Reflections on the "trade-off" concept

Participants were asked to answer the question: "Security is often thought to be inversely proportional to privacy: it is only possible to get a higher level of one of the two by sacrificing the other. Do you agree with this opinion?". Rather than agreeing or disagreeing with the statement, many participants across different tables simply stated how much privacy they were willing to give up in exchange for more security. On the one hand, their response may indicate that they bought the trade-off model. On the other hand, they might have simply been induced to think this way by the question asked.

Among those that answered the question precisely, mixed opinions emerged. The most common view was that a trade-off between security and privacy is not necessary if clear and fair rules are in place:

> *"There is compatibility [between security and privacy] if access to data is properly regulated" – drones table*
>
> *"If there is a good regulation, it is possible to have more security without giving up privacy" – 1st CCTV table*

The important role played by clear rules in engendering a fair relation between security and privacy was reaffirmed in most tables, suggesting that many do not adhere to the trade-off model. At the DPI table participants shared a rather articulated view. In particular, although in the short run it may be necessary to give up some privacy to have more security, this might not hold true in the long run:

> *"A better quality of life could lead to more security without affecting privacy; it would no longer be necessary to control people to ensure security. Security would, instead, be a natural result of collective wellbeing."*

They furthermore stressed the importance of citizens' active participation in society and of promoting solidarity and culture.

Citizens' answers throughout the citizen meeting hint at different possible interpretations. Some participants seemed to reject the trade-off model altogether, but only because the problem is identified in regulation or society. Very few participants would openly challenge SOSTs for the sake of privacy. Others might have adopted the trade-off approach during the event itself, having been influenced by the formulation of questions (which often focused more on SOSTs than on privacy). Moreover, as pointed out in previous sections, another trade-off emerged during the small-scale event: that between convenience and privacy. This is particularly true for the technology participants are most acquainted with, SLT.

6.3.4 Alternatives

The main alternatives to SOSTs pointed out in the citizen meeting were improving *social cohesion* and *wellbeing*. These concepts, although declined slightly differently, emerged in four out the six tables. At the DPI table, citizens confirmed what was said previously on trade-offs: security can be enhanced by promoting *culture*, moral *values*, a more *active citizenship*, and in general, higher standards of living. Participants sitting at the first CCTV table also said:

> *"It is necessary to promote stronger social and community ties and to form active citizens".*

Along the same line, at the drones' table participants highlighted the importance of social wellbeing (including more economic security) and civic and democratic awareness. Also, they added that social and civic ethics should be taught in schools. Also, citizens at the biometrics table pointed out that connectedness, employment, and social inclusion could be essential measures to *prevent* crimes. In fact, they remarked that these processes do not necessarily exclude the use of SOSTs, but rather they could be complementary measures focusing on prevention.

It should be noted that the lack of social cohesion and the decline in civic and moral values were also among the main threats to security that citizens pointed out at the beginning of the event. The fact that these issues are brought up once again towards the end of the event proves the importance attributed to them.

Other participants focused on the need to *integrate* SOSTs with traditional means of surveillance. In particular, a participant at the first CCTV table said:

> *"Security agents should be trained to be able to correctly use SOSTs so that they can minimize technologies' negative effects".*

6.3.5 Recommendations and messages for European and national politicians

In this section we cluster the recommendations formulated by the six tables around the main themes (6.3.5.1.) and we report verbatim the content of postcards filled in and delivered by participants at the end of the event (6.3.5.1).

6.3.5.1 Effective use of SOSTs

Table: DPI

Title: /

Recommendation/message: DPI is useful as a forensic tool, but it can bear substantial negative consequences. It should be used only for terrorism and child pornography. Commercial purposes must be prohibited. There must be complete transparency about its use. There must be complete guarantees.

Table: 1st Smart CCTV

Title: Better technology in real time

Recommendation/message: 1) Let's improve technology to avoid false positives and limit the malfunctioning and risks of sabotage. 2) A hit must lead to an immediate and contextual intervention; data can only be used for a limited time span.

Table: Drones

Title: /

Recommendation/message: Public and private use of drones must be regulated. The use of drones beyond investigations must be adequately publicized and disciplined.

Table: 2nd Smart CCTV

Title: Technology and law

Recommendation/message: The tools should be used for collective and individual prevention purposes. The SOSTs should be used in a legal and responsible manner for all security threats. Draft a European ethical code applicable in all countries.

Table: 1st Smart CCTV

Title: A supplement

Recommendation/message: This technology cannot substitute human intervention. It must be seen as a supplement.

Table: Biometrics

Title: Effectiveness depends on the conditions of use

Recommendation/message: Effectiveness varies according to the specific use. It can be useful during investigations, but also to speed up transports. It can be useful for security purposes, assessed on a case-by-case basis.

Table: 2nd Smart CCTV

Title: Integrated and shared system

Recommendation/message: It's unreliable alone; it must be part of an integrated system encompassing several technologies, including human control. Effectiveness depends also on the shared and widespread knowledge of the strategies informing actions.

6.3.5.2 Proposed strategies for use by public security authorities

Table: SLT

Title: Effectiveness and technological security

Recommendation/message: Technology must serve citizens' security, and it must be combined with the action of public security authorities. Technology alone is ineffective (and does not convey a feeling of security). It is effective if used efficiently by the police.

Table: DPI

Title: Potential trust in public security authorities

Recommendation/message: Let’s create a unique database so that data can be shared by various public security authorities for the sake of national security (criminal investigations, corruption, evasion). The use of DPI can be authorized depending on the specific cases and investigations. It’s OK if authorized by a judge. People using DPI should be controlled and surveilled.

Table: 1st Smart CCTV

Title: In part

Recommendation/message: Training of those who use it must be improved; impunity of those who commit mistakes when using it must be eliminated.

Table: Biometrics

Title: Trust because norms are in place

Recommendation/message: Public security authorities deserve to be trusted, because they are autonomous bodies regulated by norms and controlled by judicial authorities. When biometrics is used, one expects that data remain within the public security bodies, and are not transferred, sold etc.

Table: 2nd Smart CCTV

Title: /

Recommendation/message: Plan a smart use of the SOST to prevent petty crime.

Table: 1st Smart CCTV

Title: preventing instead of foreseeing

Recommendation/message: We should prevent (i.e. use algorithms that analyse the presentand are interpreted by a person) rather than foresee (i.e. perform historical analysis over the data, or create pre-set profiles for future searches). Let's train the police to use the technologies efficiently.

6.3.5.3 Regulation and control

Table: DPI

Title: Transparency and control concerning the use of DPI

Recommendation/message: There should be a common European policy and regulation on the use of DPI, to address the problem of data transfers abroad.

Table: DPI

Title: Let’s limit the use of DPI

Recommendation/message: Let’s limit the scope of usage of DPI. Sexual life, political beliefs, religion must be safeguarded. As a challenge: DPI’s fine, as long as it is applied on everyone.

Table: Drones

Title: Wise control

Recommendation/message: There cannot be an indiscriminate use of the SOST, and there must be records of its use.

Table: Drones

Title: Technology and privacy

Recommendation/message: the use by private parties should be limited and controlled.

Table: 2nd Smart CCTV

Title: Watch, but not too much

Recommendation/message: Use the SOSTs correctly, legally, and for purposes connected to security and prevention. It shouldn’t be used to control individuals (e.g. daily habits) or groups.

6.3.5.4 Information and transparency

Table: SLT

Title: Information

Recommendation/message: To inform users thoroughly and clearly, so as to let them have the power to choose.

Table: SLT

Title: /

Recommendation/message: We demand that public authorities communicate clear objectives and more information.

Table: SLT

Title: Information (2)

Recommendation/message: We recommend to be informed as to when and how users are geolocalized, and who and how uses such data.

Table: SLT

Title: /

Recommendation/message: Using SLT more transparently to limit privacy infringements.

6.3.5.5 Trading privacy for security?

Table: 1st Smart CCTV

Title: Regulating, fostering integration, and communicating clearly

Recommendation/message: If appropriate regulation is in place, it is possible to increase security without affecting privacy. Clear rules should be adopted. We should complement traditional methods by using new technology. Rules should be drafted clearly, so as to be understandable for the layperson.

Table: Drones

Title: Equilibrium

Recommendation/message: Security and privacy should be in a balanced relation thanks to more information to the citizens.

Table: Biometrics

Title: Quite intrusive

Recommendation/message: It's highly intrusive. Negotiation plays a crucial role: to what extent we accept the intrusion for the sake of greater security. It is important to evaluate how much information can be distilled from biometrics. If the data that can be derived from it are limited, then it's ok, but if it unveils a wealth of data, it undermines privacy.

Table: biometrics

Title: We need clear rules

Recommendation/message: There must be a public discussion of the legal implications of biometrics. The assessment has to be done on a case-by-case basis: sometimes security should prevail; other times, privacy should have more weight. It should be the object of regulation at constitutional level with a view to clarify the approach to fundamental rights.

Table: 2nd Smart CCTV

Title: It can be done!

Recommendation/message: If we adopt the definition provided by the SurPRISE project, security can only be reached at the expense of privacy. If precise and stringent norms are respected, the concept of security can be widened at the expense of privacy.

6.3.5.6 The alternative is civic engagement

Table: DPI

Title: Ethics, participation and solidarity

Recommendation/message: Let's rediscover ethics and solidarity, education, culture so as to avoid that surveillance becomes the only way to control. A society culturally and socially wealthier would help reduce the use of SOSTs. Let's foster participation and dialogue.

Table: DPI

Title: Increasing the quality of life; culture as an alternative to SOSTs

Recommendation/message: Public participation, events that stimulate citizens and their public conscience with regards to security issues. Increased awareness and respect for others. Information should be used all over the territory. Well-being understood in moral and cultural sense. Let's make technology human.

Table: 1st Smart CCTV

Title: Integration

Recommendation/message: Develop and use SOSTs, but in addition to and as a support to traditional methods. We should complement traditional methods by using new technology. Let's foster active citizenry, by improving relations within our community. Train police properly to limit the negative effects of the SOST.

Table: Drones

Title: An upright society

Recommendation/message: Whenever possible we hope that alternative security measures can be put in place, which can increase social wellbeing and civic sense. We should build smaller communities. We should teach civic education in schools. We should create more jobs and increase welfare. An upright politics. Punishment must be certain.

Table: Biometrics

Title: Strengthening social cohesion

Recommendation/message: SOSTs and alternatives are not incompatible, but social cohesion should play a primary role in crime prevention.

Table: SLT

Title: Civil life

Recommendation/message: Relying on a single tool is wrong. We must instead increase the level of civic engagement, and regain public spaces.

Table: 2nd Smart CCTV

Title: Surveillance, but not only

Recommendation/message: We recommend an integrated system. SOSTs are not the only answer.

6.3.5.7 Individual recommendations (postcards)

The table below reports the translated version of participants' postcards delivered at the end of the citizen meeting.

"I would like to add…"	
1	I hope that surveillance will not neglect humanity and the respect for each individual.
2	No matter what surveillance measures are adopted, they must respect citizens' dignity.
3	Citizens should only be surveilled following a judicial authorization foreseeing a hearing. The person whose data are collected by governments or private parties, should always be able to access it.
4	New and future security technologies must be chosen carefully and according to set criteria.
5	To take into serious considerations citizens' proposals, which are at the heart of any democracy. To improve communications concerning technology, since I believe that there isn't sufficient information about this topic. Ignorance helps nobody.
6	Very good project. It'd be crucial to consult citizens on other topics as well. For instance, why doesn't Europe pay more attention to the problem of seaborn migration in Italy? I hereby ask that Italy be helped to address this problem and help people. Thank you.
7	An all-encompassing policy, in particular concerning the protection of privacy and security; clear and simple norms drafted with the active cooperation of citizens.
8	An agency in charge of collecting data does not necessarily invade privacy, provided that irrelevant data are deleted. Security > privacy (verbatim).
9	Attention must be paid to each human being and his or her personal liberties. Powerful surveillance tools require strong regulation.
10	Work towards building the United States of Europe based on shared laws beyond commercial practices.
11	Clear and up-to-date laws should be adopted that regulate both security technologies and the processing of the data they collect, so as to limit the erosion of privacy, and their commercial exploitation.
12	I recommend taking into serious account the outcomes of the citizen meeting, by correcting the currently inadequate applicable law.
13	I'd like to add that the greatest resource of Earth are men and women, the greatest resource for the resolution of all problems is their brotherhood, friendship and sharing. Only by attaining such conditions we may be able to start life anew.
14	If one invests in culture and the environment, and takes measures to support social cohesion, one will decrease security issues.
15	Let's support cooperation and solidarity projects. Migrants are a fact. They are displaced people against their wishes. Do not return them forcedly.

Table 2: Individual Recommendations (postcards)

6.4 Process design

The Italian SurPRISE citizen meeting took place on June 17th, in Florence[25]. The setting was "Villa Schifanoia", seat of the European University Institute's Department of Law. The event started at 5:30 PM with registration and a welcome coffee. We began the event by showing the movie of the Italian citizen summit, the purpose being to show the importance of the citizen meeting as the continuation of a process started earlier. The two working sessions lasted for three hours, interrupted by a short break in between. Both sessions were guided by a web-based decision support system developed specifically for the citizen meeting. At the end of the second working session, participants and moderators alike were asked to fill in the questionnaire, and when they handed it in, they received a small gift[26] for their participation, together with a return bus ticket to compensate for travel expenses. Each table was then given the opportunity to illustrate their main conclusion in the plenary. The event ended with a small reception on the terrace of Villa Schifanoia.

6.4.1.1 Recruiting citizens

The recruitment process started on May 19th and was carried out by the company "*Contesti e Cambiamenti*" using a recruitment method known as "outreach". This method consists of approaching people in an unstructured way using informal communication. People were approached in several public areas close to where the event took place. Later on, they were contacted via email and phone calls. At the same time invitations were sent to several associations in order to contact typologies of people that were otherwise difficult to reach. Overall, 47 citizens[27] showed up, out of 65 overall invitees (to account for no-shows[28]). All participants signed a consent form for the processing of their personal data both upon invitation and on the day of the event.

The sample of citizens that participated in the event was fairly representative with respect to gender, while older citizens were slightly over represented (citizens under age 30 where often unable to attend due to professional commitments). There is a somewhat stronger education bias in the sample since 66% of participants have a university degree (compared to 22% of the Italian population); people with lower levels of education, in fact, often declined the invitation to participate.

[25] Sincere thanks to all that contributed to the success of the Italian citizen meeting. Melissa Zorzi for having taken care of the main organizational aspects, and having been an irreplaceable colleague; Professor Martin Scheinin, responsible for the SurPRISE project at the EUI; Serena Bürgisser, (Vice Director, EUI Communications Service) and Gianni Palazzo for their media support; Jonathan Andrew (team SURVEILLE), Claudia De Concini (team SURVEILLE/SurPRISE), Martyn Egan and Matteo Rocchi for logistics, troubleshooting and invaluable moral and practical support; Paolo Martinez (FUTOUR) for his brilliant head facilitation; Provincia di Firenze, Comune di Firenze and Comune di Fiesole, for their moral sponsorship; Contesti e Cambiamenti for the very professional sampling and recruitment of participants; great table moderation and handling of the decision support system (DSS): Ginevra Avalle, Sandro Buggiani, Nicolò Caciotti, Luca Caterino, Lapo Cecconi, Giulia Ciampi, Marco Algimiro Fusaro, Carlotta Iarrapino, Valeria Maione, Marco Scarselli, Antonio Volino and Alberto Zinanni.

[26] Participants received a voucher for a complimentary dinner at a local restaurant (Runner Pizza) as well as a discount for accompanying guests.

[27] The target of the SurPRISE citizen meetings was of 40 people, but the EUI aimed to invite more to compensate for the lower participation of the large-scale event held in October. Porcedda and Zorzi (2014).

[28] The 28% of no-show is within the expected rate of 30%. It should be noted that all the available citizens that did not end up participating informed the organizers beforehand.

Demographics of the total sample		
Place of residence	**N**	**%**
Florence	42	65%
Province	23	35%
Gender	**N**	**%**
Male	29	45%
Female	36	55%
Age	**N**	**%**
18-30	10	15%
31-45	25	38%
46-65	30	46%
Education	**N**	**%**
Elementary / lower middle schools	3	5%
High school diploma	19	29%
Laurea e post laurea	43	66%
Employment status	**N**	**%**
Employed	21	32%
Self-employed	21	32%
Unemployed	3	5%
Stay-at-home parent or carer	4	6%
Student	8	12%
Retired	8	12%

Table 3: Demographics of registered participants

Besides the recruitment process, the firm *Contesti e Cambiamenti* also took care of the disposition of participants at tables. In addition, since more people than expected showed up, an extra table for CCTV was set up.

6.5 Evaluation of the event

6.5.1 How citizens assessed the meeting

6.5.1.1 Positive features

The majority of participants agreed that the event was overall a pleasant and positive experience. Citizens were interested in learning how a citizen meeting exactly works and to confront themselves on the topics dealt with. There was an active and productive exchange of opinions through citizens' spontaneous and positive interaction. Thanks to the decision support system used, participants had the chance to discuss actively with each other about relevant topics, sharing food for thoughts. The findings brought forward more extensive awareness of SOSTs' security benefits and privacy risks. The citizen meeting turned out to be an enjoyable social gathering, thanks to the quality of the organization and the availability of both staff and participants.

6.5.1.2 Negative features

Doubts emerged regarding the tempo of discussions. Often, time limits were considered to be rather stringent and hard to respect. Moreover, some participants were puzzled by the overall length of the event. Another issue concerned the voting system: participants believed that it might have influenced citizens' final opinion. In addition, some questions could have been transformed in Likert scales questions while others - that were indeed based on Likert scales - required much more detailed answers. Some of the options given in Likert scale-based questions were perceived as being inadequate with regard to the question asked, whereas some questions were considered too complex. Finally, some participants complained about the room being too small and the ensuing noise.

6.5.2 Evaluation of the DSS by the research staff

6.5.2.1 Positive features of the DSS

Moderators appreciated the speed and simplicity of the DSS. Moreover, they found it made it easier for participants to express themselves and confront ideas on different topics.

6.5.2.2 Negative features of the DSS

Moderators complained about the DSS' tight time schedules imposed on each discussion. In fact, the lack of time was seen as a major obstacle; having to save manually the discussion session was also a time consuming effort, for which moderators suggested introducing an automatic saving mechanism. Another negative element was the lack of coherence between questions and answers and occasionally, their limited clarity.

6.5.3 The role of information debate and group dynamics in citizens' acceptance of SOSTs

Citizens' open dialogue contributed to well-thought and unconventional recommendations. Discussions featured concrete and real examples, which helped establishing clear stands on the themes dealt with during the event. Ideas were effected through constructive table discussions; the interaction was very productive especially during the second session. Using the DSS, citizens were given the opportunity to define a shared consensus on single statements and remain focussed on the discussion at hand.

> *"Unrestrained discussions among people with very different opinions helped to elaborate concise and original ideas, for example, on the topic of public security authority. "* - *a moderator*

7 Country report of Denmark[29]

7.1 Executive Summary

The Danish SurPRISE small-scale event took place on two separate occasions. The first was on the small island of Bornholm on June 14th, where 16 citizens showed up to discuss security technologies and aspects of surveillance, privacy and security. With only 16 citizens it was immediately decided to address only two security technologies and host another event on the 15th of August, this time in Copenhagen. At the second meeting 27 citizens participated in an engaged discussion on the remaining three security technologies.

The participants were happy to engage in the discussion and expressed that it was an important subject to debate in public. The participants didn’t feel insecure in their country or their daily life. However, they were quite concerned about how the technology would develop in the future, and many already felt that it had come too far in some areas. They were particularly worried about how mass surveillance could influence democratic society and the feeling of personal freedom. A majority didn’t feel that blanket surveillance could be justified even if it was to improve national security.

One of the most frequent recommendations was more or better regulation and control and the suggestion for a 'data ombudsman'. Many participants pointed to the need for an independent body on the national or European level to ensure control over the institutions and/or firms that administrate data and data retention.

Many participants also suggested that education and information in technology should be an integrated part of public information and elementary school in the future.

Overall the Danish participants assessed the technologies as a combination of convenient and practical commodities and surveillance tools outside democratic control. This led to a lot of concern about the future development and consequences of further implementation and a call for transparency and democratic control.

[29] The authors of this chapter: Jacob Skjødt Nielsen, Anne Kirstine Smith Lygym, Nicklas Bang Bådum from DBT

7.2 Perception of security and insecurity

7.2.1 Safety

The vast majority of participants at both meetings expressed a feeling of safety and security in their daily life. Many emphasised a feeling of security in public areas such as train stations, and many mentioned that they rarely feel insecure at night-time, even if they walk alone. In regard to this, it should be pointed out that the young people at the meetings in general felt safer on the streets than the elder participants. Several citizens mentioned that they personally had no experience with unsafe situations. On the other hand, all groups mentioned the national and international security situation as a different matter.

> *'Danish participation in war affects my general feeling of security'.*
>
> Young male student

7.2.2 Main security challenges

Although the overall attitude among the participants was a feeling of relative safety and security, all the tables did give examples of things that affected the perception of security. The main security challenges can be roughly categoriSed under the following headlines:

Personal safety

Matters that affected the safety of the participants personally or someone they knew. There were two aspects of perceived personal insecurity: physical safety and digital safety. The former related almost solely to the notion of violent crime and attacks. Only a few identified terrorism or organised crime as a source of personal perceived insecurity.

Digital safety or lack thereof was a more commonly shared source of insecurity. This issue was often repeated by participants after first being named as a cause of insecurity. Examples of this were Internet surveillance, invasion of privacy and (unlawful) collection of personal data. The latter was especially emphasised, and arguments involved recent media coverage on Edward Snowden and documentation of NSA surveillance activities in Denmark and other countries.

Societal risk and insecurity

Several participants named the current economy as a main security challenge in Denmark. Since the economic crisis, unemployment and changes in the social safety system (welfare) have affected the feeling of safety among the participants. This was emphasiSed by participants who were unemployed or otherwise outside the workforce.

> *'I'm beginning to feel insecure…The Danish social safety net is changing for the worse'.*
>
> Male in his 40s

The feeling of increased insecurity with regard to economy was twofold: first, how it would affect the participants personally, and second, how an increased gap between the wealthy and the poor could lead to a less stable society and more unrest and crime.

International relations

Danish involvement in conflicts and warfare has affected the participants' feeling of security. Some participants pointed to the change in foreign policy in 1990 to what is known as 'Danish foreign policy activism', which means that the Danish military has taken part in international conflicts ever since and has been one of the most (relative to its size) active supporters in the fight against terrorism. This makes Denmark a potential target for international terrorism, and the participants pointed to the international crisis with IS and Afghanistan and the fear of terrorism in general as security challenges for Denmark. Social and economic inequality on a global scale was another issue that affected the participants' overall feeling of security. The sentiment was that our Western lifestyle has created a global economic imbalance, another reason some participants regarded their lives as less secure than before.

7.3 Opinions on surveillance-based security solutions in general

Many participants overall perceived surveillance-oriented security technologies (SOSTs) as positive instruments for ensuring safety and security at airports and government buildings. There was also an overall positive attitude towards the use of SOSTs as tools for monitoring traffic and alerting authorities in case of traffic jams or emergencies. Many appreciated the positive benefits of biometrics, closed-circuit TV cameras (CCTVs) and smartphone location tracking (SLT) as tools for enabling a flow at places with many people present, e.g., airports and highways.

There was also a generally positive attitude towards the use of SOST to help find missing people, children and people with dementia. Many participants highlighted SLT as a SOST they actively enjoy in their daily life. Participants in their 20s especially have grown accustomed to the GPS and location-finding tools integrated in smartphones. As regards SLT, many groups discussed its use in police investigations. The general opinion among the participants was that the SOST was a practical tool for locating criminals, and it also could be used to prove innocence. Some participants raised the argument that reasoned suspicion must be the basis for all government use of SLT technology.

The SOST participants felt most concerned about was deep impact inspection (DPI). According to the summaries of the discussion rounds, most criticism of DPI is related to a fear of losing privacy. This is seen in relation to the participants' definition of privacy and their homes. (This will be elaborated in 2.4.3.)

Overall the participants approved of the use of SOST, if it can be proven to be effective. Many participants felt concern about unnecessary use of SOST, primarily because of a fear of their movement and activities being logged. Thus there was a general concern about data retention. At several tables the EU ruling on 'the right to be forgotten' (13 May 2014) was mentioned in positive terms.

7.3.1 Appropriateness and necessity

Most participants found the use of SOSTs appropriate in the matter of national security issues and in situations where the technologies could actively save lives, as in traffic surveillance. In addition, the use of SOST to optimise infrastructure was generally viewed as reasonable. Several participants mentioned SOST as an effective tool for generating knowledge in urban planning. With regard to this topic, it was suggested the data be anonymised.

7.3.2 Awareness of the kinds of information gathered

Most participants agreed they lacked of information as to when surveillance is present and to what degree the data is being used.

> *'I'm more certain that I'm being monitored than the opposite'.*
>
> Woman in her 30s.

There was general agreement that the public needs more information about both the degree of surveillance and who gathers and uses the information. The participants also expressed the desire to get education in taking personal precautions, and many recommended the need to inform children and youngsters about 'digital behaviour'.

The uncertainty of *when* data and information is being gathered was a recurring topic at most tables. This especially related to Internet surfing and the use of smartphones. However, many participants also mentioned uncertainty about when and where the public is being surveilled by CCTV.

Almost every table agreed that there is a need for more transparency and knowledge about data gathering and data retention. There was also a general wish for more influence over the gathered personal information and for the possibility of making a statement of opposition should the information be wrong.

7.3.3 Effect of surveillance on everyday life

The use of SOST in Denmark has had an effect on the daily life of the participants. Some stated that they rarely think of the presence of SOST, and some also stated that they never change their behaviour on account of this technology. But most of the project participants related how they, in different ways, actively adapt their activities because of the technology. Some participants informed us that they avoid changing rooms at clothing stops because of the fear of CCTVs; several participants related incidents in which they had either turned off their smartphone or left it at home on purpose owing to the fear of being tracked. In most cases the choice was made before participating in political demonstrations, but one participant, a young male student, had turned off his phone before our citizen summit. As he explained, he felt it was a controversial topic, and he was concerned that his participation could lead to suspicion about his political views in general.

DPI was by far the SOST with the biggest effect on citizens' everyday lives. Several participants reported that they actively changed their behaviour because of their knowledge of the potential for surveillance through the Internet. Some changed browsers before surfing certain topics, and many expressed belief that no activity on their computer was personal or private.

7.4 Privacy in Danish culture

7.4.1 Interpretation of privacy

Privacy was often described as something personal or defined as activities performed alone. Several participants defined privacy as something they 'don't tell anybody about' or as something 'confidential'. As one participant said, 'Everything else is in theory everybody's property'. It was also mentioned several times that privacy has something to do with self-determination regarding who, if anyone, should have information about and knowledge of the private activity.

> *'Privacy is the personal freedom to make a free choice'.*
>
> Woman in her 20s

Many also expressed a feeling that the public sphere is increasingly moving into the personal sphere. As one citizen said:

> *'Technology is changing my perception of "private activities"'.*
>
> Male in his 60s

This indicates that the perception of privacy may be moving towards a narrower definition and into a narrower space, both spatial and mental.

7.4.2 Concerns about mass surveillance

There was a strong tendency in all five groups towards a concern that the use of surveillance-oriented security technology in general is eroding privacy. This was even more true when expectations about how technology will develop in the future are taken into account. Furthermore, the majority 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 have concerns about its development in any case.

Thus concerns about mass surveillance did increase significantly when the respondents thought about the future and other people who might be the target of mass surveillance.

Another strong tendency in the replies was how much importance the respondents placed on control over the data and information collected about them. One line of reasoning was that people should be in control of their own data; another was that a third party, e.g., an independent regulatory institution should be in charge of controlling access to private data.

7.4.3 The inviolable core of privacy

The participants' definition of privacy was varied. Still, there seemed to be a tendency towards describing privacy in words related to home and freedom.

> *'It's when I'm home and close my door'.*
>
> Young female student

The word "thoughts" was mentioned several times in defining the core of privacy. Many participants also mentioned "conversation" – oral, by letter and by email. Concerning this, several participants stressed that they found DPI highly intrusive especially because of its potential for reading and altering personal messages sent via the Internet. Conversations with doctors and psychiatrists were also mentioned at several tables.

7.5 Regulation and control around SOSTs

Most citizens assessed their knowledge of the regulation and control of SOSTs as sparse. Many expressed frustration with Danish regulations, and those who claimed to have some knowledge stated that the laws on the subject are outdated in relation to contemporary technological development and possibilities. Very few respondents were specific about the actual laws and regulations at the national or EU level. Some mentioned the data protection agency but were unclear as to what extent the Danish DPA took active part in regulating and controlling use of surveillance-oriented security technology.

7.5.1 Need for awareness and information

In general the participants felt they lacked knowledge about rules and legislation, both as regards government regulation and citizens' rights. Many participants requested international or European regulation in place of or as a supplement to national or even local regulation and control.

In addition there was a general demand for more information. Many answered the question with questions. A typical response was:

> *'What are my rights in regard to getting insight into data retention?'*
>
> Male in his 30s

The small-scale event revealed citizens' concerns about rules and regulations and a great lack of knowledge about the potential for public access to documents and data.

A few citizens did in fact have knowledge about the topic of legislation, regulation and control and stated that they had investigated the topic themselves. They didn't feel that the public in general was well informed.

7.5.2 Expectations about legal safeguards

Many participants felt that legal safeguards should be required to inform citizens of legal practices as well as the gathering of information. Many tables agreed that private companies should be further controlled and that customer information, particularly in 'terms and conditions', should be more transparent and written in more comprehensible language.

In line with the recommendations from the large-scale event, the participants desired that a new independent organisation be put in place to better advise, regulate and control the use of surveillance-oriented security technology. They felt this should be a European or international regulatory body and should itself be guarded with extensive democratic control.

7.6 Differences and similarities in perception of particular SOSTs

When group discussions in the second event were dedicated to specific security technologies, the participants discussed positive and negative elements of the chosen technology and made assessments of its effectiveness and intrusiveness and of the technology as an effective national security measure.

7.6.1 Deep packet inspection

Deep Packet Inspection (DPI) and surveillance on the Internet was a difficult concept to discuss for most participants. Recent media coverage of how the NSA has used DPI to monitor Internet information and its possible collaboration with Danish security organisations had raised the awareness of some of the participants. The potential limitations and outreach were nonetheless still debated among the citizens, showing that DPI is still considered a dubious technology.

The participants didn't find DPI to be a very effective tool for improving national security and a personal feeling of security. They did describe it as a tool for statistics on the Internet and in favourable situations for criminal investigation by detectives or public security authorities.

Many participants did regard DPI as intrusive to privacy. They mentioned challenges concerning the possibility of misinterpretation of data and change in behaviour.

The trust in security agencies using DPI in Denmark was somewhat lower than for other SOSTs. The main reason for this was possible collaboration with the NSA, as mentioned earlier.

When asked, the participants didn't believe in this trade-off within the context of DPI. This was mainly ascribed to the fact that they considered DPI to be very intrusive, as it targets everyone. Alternatives to DPI should be given higher priority, was the group's general feeling.

> *'We have no idea what is really going on. It makes it impossible to exercise democratic control. You cannot form opinions when you do not understand what technology means'.*
>
> Male in his 20s

7.6.2 Smart CCTV

Denmark has implemented many CCTV cameras for security agencies and private operators alike. Some reports show that Denmark currently has the highest number of CCTV cameras in the world per inhabitant. Smart CCTV is still a new technology and has limited use as a national security measure.

The participants in general were not convinced of the effectiveness of this technology, but a few of them mentioned positive aspects. These mainly related to increased perceived personal safety. The notion was that smart CCTV would discourage criminals in relation to petty crime. Other positive aspects mentioned included license plate recognition for vehicles, assistance in shops and so on.

Smart CCTV was considered intrusive if it included biometric recognition such as facial or iris recognition. Some participants didn't find the camera itself to be intrusive, using the 'nothing to hide' argument. However, there was some debate as to whether the knowledge of being under surveillance would still affect behaviour, even subconsciously. The majority didn't find smart CCTV to be an improvement in national security. Trust in security agencies using advanced CCTV was limited, the argument being that people are operating the systems and that the systems themselves – advanced or not – are still subject to technical faults.

The participants didn't feel that CCTV could only be implemented at the expense of privacy. They pointed to regulation, control and data security as alternative methods to blanket surveillance. Even with these in place the participants all felt that alternative approaches should be given higher priority.

> *'The potential for misuse is enormous. Imagine the apartheid regime with black/white camera recognition. The majority of people live in authoritarian states, which is a problem. For the authorities it is a weapon and a potential for constant surveillance by authorities at meetings'.*
>
> Male in his 40s

7.6.3 Drones

Not many participants were aware of drones being used as a security technology in Denmark, and many still regard drones solely as a military technology. There has been debate about their possible implementation by police, firefighters and security companies in the media, but this did not make the participants consider drones as an improvement in national security or their personal feeling of security.

Drones were considered intrusive to privacy especially when it comes to private and illegitimate use. Examples were celebrities being surveilled by paparazzi or neighbours filming through windows or gardens. This was felt to be highly intrusive to privacy as it is a clear violation of personal space and uncontrolled. The use of drones must therefore be regulated so that abuse can be limited or even prevented.

The group also named several positive aspects of drones, for example in search and rescue as a substitute for putting people in hazardous situations, as in the case of radiation or fires. A drone can provide an overview that will help firefighters and rescue personnel.

In general the participants expressed mistrust in security agencies using drones, but it was also unclear to most participants for whom and to what extent this is already a reality. This answer was influenced by the military application of drones and how they are often portrayed in the media.

As with most other groups, they found that alternative approaches should be given higher priority, but examples were scarce as the concrete purpose of drones was unclear.

> *'It can be an expensive solution and create a false feeling of security. I do not believe it changes anything for those who want to do a bad thing. It is treating the symptoms rather than the real problem'.*
>
> Woman in her 30s

7.6.4 Biometrics

The group that discussed biometrics considered them to have properties that could improve national security and the feeling of security. This was primarily based on the idea that biometrics are already in use to identify criminals with a high level of certainty. What the group didn't support or endorse was the notion of a national or international database with biometric data. A worldwide database with biometric information would be highly intrusive though also potentially efficient in solving crimes, but the violation of privacy and personal freedom made this database unthinkable. Another question that arose in the group was who would have access to biometric monitoring and what could it be used to do. The consequences of misuse could be dire and could entail identity theft and the like.

Biometrics is a technology that requires resources and knowledge to use properly. The group that discussed biometrics was the only one that trusted in security agencies that use biometrics. The group identified the police and the police intelligence service as users but not the municipalities that currently issue passports with biometric information on the chip. The other group didn't find a trade-off necessarily to be the case with biometrics, believing that security and privacy can be increased independently of each other.

Alternative approaches could be given higher priority, but in some cases the group didn't consider alternatives to be realistic, as biometrics is unparalleled for investigative purposes.

> *'Those with power and money will have the opportunity to exploit the technology'.*
>
> Women in her 20s

7.6.5 Smartphone location tracking

All participants had smartphones and knew about smartphone location tracking technology. The concept of GPS led easily into a basic understanding of consequences and challenges concerning location tracking technology. On top of that the participants used apps that employed location tracking on their smartphones.

They did not find smartphone location tracking to be a very useful tool for improving national security, even though they were aware and identified cases and situations in which this technology had been used successfully as a part of criminal investigation.

The group did however agree that the use of smartphone location tracking was highly intrusive to privacy, both as blanket surveillance and when it used to target people in specific areas without a court order or something similar.

The participants discussing smartphone location tracking only partially trusted security agencies that use this technology in Denmark. Of great concern was the potential misuse of location tracking by companies and third-party operators from other countries. This could be a problem because legislation has not followed technological development and because users of smartphone apps do not check consent forms before installing them.

This group also didn't believe in the trade-off idea. They felt that legislation could be improved, that regulation and control could ensure lawful use and that software companies would provide location apps without privacy infringement given the right incentives.

On the question of alternative approaches, the group was somewhat split, for the reason that they didn't feel an alternative to smartphones as such was realistic, but on the other hand apps should become fair and privacy friendly.

> *'An outcome of this form of surveillance could be to prevent revolutions'.*
>
> Women in her 40s

7.7 Security agencies and legal safeguards

In all discussions about the trustworthiness of security agencies that use surveillance-oriented security technology, it was evident that most participants didn't trust all employees in any given security agency, but this was primarily because of potential weakness in the individual employee.

A minor group of participants moreover didn't trust the security agencies as institutions, arguing that the policies of said institutions didn't follow official policies or legislation but were in fact a product of undisclosed collaboration among selected security agencies.

The somewhat abstract question regarding security agencies and abuse of their power caused many participants to answer in a similar manner: all security agencies abuse their power to some extent at some point in time. The underlying tendency, however, is clear enough: extended-use surveillance-oriented security technologies increase the risk of abuse.

When it comes to trust in private companies, almost all respondents placed less or no trust in the motives of private agencies working on a commercial basis. The participants were certain that these companies were abusing the data they collected.

7.8 Reflections on the 'trade-off' concept

The participants in general were quite sceptical about the concept of trade-off between privacy and security. Two of the five groups didn't see it as a trade-off at all, and the remaining three groups answered 'not really'. The respondents felt that a society can be secure and at the same time protect the citizen's right to privacy. In the words of one of the participants:

> *'What is the purpose of security? A prerequisite for security is, of course, privacy…it is not a trade-off; it's a prerequisite to have both'.*

> Male in his 50s

Typically the participants agreed that the development of security technologies should take into account both respect for privacy and data protection legislation.

7.9 Alternatives

Many of the recommendations suggested non-technological solutions and focused on social action and responsibility instead. Many emphasised crime prevention, such as social work or education.

7.10 Recommendations and messages for European and national politicians

The suggestion of a data ombudsman was the most frequent recommendation. This was the case at the large-scale citizen summit, and the small-scale summit confirmed this. Many also suggested an independent body to ensure that an organ controls the institutions and/or firms that administrate the data and data retention.

Many participants suggested that education in Internet praxis should be a part of elementary school, in regard to both precautions concerning privacy and information about how the technology actually works. These recommendations also reflect the lack of knowledge about SOSTs and their functions that many participants expressed. The combination of technology as a convenient and practical tool commonly used in daily life and the lack of understanding of the consequences of its use creates an unreflective adaptation and acceptability of SOSTs in society.

7.10.1 Drones

Table: Drones

Title: Data ombudsman

Recommendation/message:
- It must always be judged as to whether it's necessary

- It must be used when it's appropriate.

- Democratic insight is important. The opportunity to pull the emergency brake must be present. There could be a whistle-blower solution.

- An extra effort in control from an authority

Table: Drones

Discussion phase: Positive and negative assessment

Title: Transparency and opportunity for objection

Recommendation/message:
- The registered data has to be publicly available and editable if it is wrong.

- The EU court has just ruled, that anyone can apply to delete incorrect information about them.

- It is important to be notified when there is registered information about you – and then anyone should be able to make objections.

- You don't know if the data is erroneous if there isn't transparency

Table: Drones

Discussion phase: Intrusiveness

Recommendation/message:

- Don't increase it. Restrict it to a limited degree. Use it only when necessary.
- It must be continually evaluated whether it's necessary.
- It shouldn't be there when it has been proven ineffective and doesn't solve the problem

Table: Drones

Discussion phase: Security agencies and legal safeguards

Recommendation/message:

- Control from an external authority

Table: Drones

Discussion phase: Transparency and supervisory body

Recommendation/message: Privacy and security are not complementary. Not a trade-off. A precondition for safety is privacy.

Table: Drones

Discussion phase: Alternatives

Title: We need to do what actually works

Recommendation/message:
Rethink the approaches and start from scratch; insecure and fearful citizens create the need for surveillance. Think in a bigger context and include integration, rehabilitation, etc. Include architects, artists, etc., in making public spaces safer. Lights at every bus stop, etc.

7.10.2 Smart CCTV

Table: Smart CCTV

Discussion phase: Main positive and negatives

Recommendation/message: The potential is huge; that's positive. We need to concentrate on limiting potential abuse of the technology (which is huge). The fact that Facebook can recognise your face and cameras can catch your number plates is exciting, but the technology needs to be controlled safely.

Table: Smart CCTV

Discussion phase: Effectiveness

Recommendation/message: It's possible that it works and improves national security, but it's a lazy and cheap way of solving societal problems. You can't improve security with only preventive initiatives such as SOST.

Table: Smart CCTV

Discussion phase: Intrusiveness

Recommendation/message:
- You need to be very cautious with your information if you as a Danish authority want to develop it more.

- There are possible breaks as soon as you communicate through the Internet; it is important to be aware. When the plane was invented, the plane crash was invented. It will go wrong. We should focus more on who's using the data than how to collect it. We need to see who is using it and how, rather than either/or as it is now.

Table: Smart CCTV

Discussion phase: Trade-off

Recommendation/message:
In some cases there can be a trade-off. Less privacy is a cheap price to pay for more security, though.

Table: Smart CCTV

Discussion phase: Security agencies and legal safeguards

Recommendation/message:
- We should be very cautious about outsourcing information. Anyone can be paid off for information. It is a vacuum until more advanced technology is introduced. With advanced surveillance it is possible to ensure that you don't continuously collect random information but only target persons who are wanted. Criminals have to accept less privacy.

Table: Smart CCTV

Discussion phase: Alternatives

Recommendation/message:
Prevention should be employed to a greater extent; if it concerns terror then teach people about religious understanding; if it's Facebook then teach the users how to behave safely on social media. Cameras and other technical inventions can't be the solution – you need to know the reason the problems occur.

7.10.3 Deep packet inspection

Table: DPI

Discussion phase: Main positives and negatives

Recommendation/message:

More information and information about the technology and its potential – it's difficult to have a public debate otherwise.

Table: DPI

Discussion phase: Effectiveness

Recommendation/message: SOSTs are far from enough. Criminals can just step out of the digital world if they want to exercise terror.

Table: DPI

Discussion phase: Intrusiveness

Recommendation/message:
- There should only be DPI in the most critical locations. Only use it when there have been worrying or unusual events. No general surveillance of data. There has to be a search warrant from a judge.
- Communicate about it; it is difficult to understand and have an opinion about.
- The technology has to operate within a normal democratic practice: division of power, legal rights, etc.

Table: DPI

Discussion phase: Security agencies and legal safeguards

Recommendation/message:
- Yes, but mostly/only public authorities. Private companies have economic interests, etc., and are more difficult to control. Governments/public authorities are responsible for public interests and morale.

Table: DPI

Discussion phase: Trade-off

Recommendation/message: Yes, they are complementary. It's a balance. Don't put the surveillance camera up before there's a serious motive.

Table: DPI

Discussion phase: Alternatives

Recommendation/message: It's important to look at alternatives. The reason for the threat doesn't disappear because of a surveillance camera.

7.10.4 Biometrics

Table: Biometrics

Discussion phase: Positive and negative assessment

Title: Biometric methods are good

Recommendation/message: Crime: It's okay that cameras can recognise faces. To connect information on your biometric, eye scan in a bank reduces scam with credit cards. It's an advantage to gather information while fighting against diseases. You can track those who are predisposed to certain conditions.

Recommendation: Safer ways of paying.

Table: Biometrics

Discussion phase: Effectiveness

It can be used for registration of entry in countries.

- Crime.
- The health care sector.
- Research in science – predisposition to diseases.

Table: Biometrics

Discussion phase: Intrusiveness

Recommendation/message: Storage of biometric data is not beyond measure anymore. It's better than computer surveillance because you can recogniSe the person.

Table: Biometrics

Discussion phase: Security agencies and legal safeguards

Recommendation/message: Yes, there is much confidence on the part of the public. To politicians: tell the secret services to do things right.

Table: Biometrics

Discussion phase: Trade-off

You need to consider what makes people happy. The way we understand privacy is very individual. It is easier to generalise security. Maybe you are safe, but it's more important that you *feel* safe.

Table: Biometrics

Discussion phase: Alternatives

Title: Creating trust

Recommendation/message: The alternatives have to be top-prioritised for us feel safe. We have to consider a broader perspective: Are the circumstances for people who drop out of the system good enough? What is the level of education and job frequency? etc.

7.10.5 Smartphone location tracking

Table: Smartphone location tracking

Discussion phase: Positive and negative assessment

Recommendation/message.
- The effectiveness has been beneficial for social life. It has changed social behaviour. It can be a serious stress factor, though. Teenagers go out a lot and they need to be contactable. It prevents revolutions.

Table: Smartphone location tracking

Discussion phase: Effectiveness

Recommendation/message:

We fear the Panopticon society. We need to know more, get more information.

Knowledge about what is under surveillance: access to documents, possibility of getting your file deleted. We have a right to be forgotten.

Table: Smartphone location tracking

Discussion phase: Intrusiveness

Recommendation/message It is difficult to control. We need a lot of supervision and control as well as encryption of identities. Denmark should follow the EU ruling about logging.

Table: Smartphone location tracking

Discussion phase: Security agencies and legal safeguards

Recommendation/message: No confidence. More access to documents and external supervision.

Table: Smartphone location tracking

Discussion phase: Trade-off

Rather privacy than security. Safety is problematic.

Table: Smartphone location tracking

Discussion phase: Alternatives

Technology is fine but not surveillance technology. We like old-school security technology for personal safety

7.11 Process design

DBT arranged two small-scale meetings because there were not enough participants for the first one. The first was held on the island of Bornholm during a large meeting, 'Folkemøde', where citizens and politicians met over four days to discuss various topics of political relevance.

DBT should have used the citizen panel from the municipality of Bornholm to recruit the participants. However, this arrangement was cancelled just before the invitations were to be sent out to the citizens of Bornholm. After that DBT tried a last-minute recruitment strategy using newsletters, Facebook, newspapers, media partners and face-to-face recruiting.

In the end only 16 participants showed up, and the managers decided to go through with only two of the five SOSTs. The evaluation showed that a small-scale event was probably too long for the Folkemøde, in which the events are typically limited to 1-1½ hour maximum.

The participants were an even mix of women and men, aged between 26 and 64, and the majority had a medium or high level of education.

The second meeting was held in Copenhagen in August. Participants in this event were recruited using a host of channels: email lists for university study programmes, DBT's social media accounts on Facebook and Twitter, the DBT newsletter (TeknoNyt) and the DBT website. The participants were asked to sign up via email or a WebForm.

The process started more than a month prior to the event in order to give people a chance to react to it, and a number of reminders were posted via each of the communication platforms utilised.

When the day of the event came, 34 had signed up, but a couple had to cancel and some didn't show up, so the final number of participants was 27.

The participants were fairly evenly divided, with 15 women and 12 men, most aged between 20 and 31, but with six outliers (15, 17, 18, 46, 51 and 82). The majority of the participants were university students.

Given that the event was held in central Copenhagen, it is unsurprising that all participants were inhabitants of Copenhagen or the immediately surrounding suburbs.

The event took place in DBT's conference room in central Copenhagen, which is easily accessible via public transport or by bike. The locale featured ample space for the 27 to be seated at three separate tables without disturbing each other and satisfactory WiFi and media infrastructure.

7.12 Evaluation of the event

7.12.1 How citizens assessed the meeting

The immediate reaction from the participants at both meetings was very positive.

They considered the event to have been very well organised and well executed. The participants on Bornholm didn't mind the somewhat smaller setting, as the table discussions went well in any case.

Of particular frequency was the mention of the topicality of the subject, considering the public debates and news stories in the preceding year.

The participants especially enjoyed the opportunity to carry on an informed debate about a topic of current interest that would lead to a substantial report, giving the participants the opportunity to let their voices be heard by their politicians and to give direct recommendations.

That being said, a majority of the participants did consider some of the questions to be too nonspecific. The questions regarding legal safeguards and security agencies especially were basically incomprehensible to most participants, who would lose track of the question and options halfway through.

In terms of the informational material, it was clear that few had read it all and most had only skimmed parts of it. Especially in the biometrics group, it was evident that the participants were not initially aware of the concept of biometrics as related to surveillance technology; neither were they aware of the ways in which it could be used as a SOST. In other groups, especially Smartphone location tracking, knowledge of the matter was very high for many of the citizens.

7.12.2 Evaluation of the DSS by the research staff

Overall the moderators and minute takers were satisfied with the procedure and the decision support system. One was completely satisfied, two were rather satisfied, one was neither/nor and one was rather dissatisfied.

Three moderators responded that some of the questions were too complex for the participants, especially the ones about regulation. All in all the procedure and DSS were easy to understand and to progress simultaneously throughout the event. Two suggested fewer questions, and two would have liked to have more time for discussion and recommendations. They all agreed that the participants had a good time and interesting discussions.

7.12.3 The role of information debate and group dynamics in citizens' acceptance of SOSTs

Overall the participants had a good dialogue. The 'sceptical' side was somewhat dominant among the participants at most tables, so the moderators had to help the more 'technology-friendly' participants have their say in the debate. This was also a challenge in the recommendation round where the marginal voices were less likely to be heard. The discussions were heavily influenced by recent media coverage of surveillance and a media scandal in Denmark.

The voting booklet was easy to use and got the discussion going around the table. Some of the citizens clearly had almost expert knowledge in some areas, while others hadn't even read the entire informational booklet. The latter was a problem at the biometrics table, where several of the participants had a hard time grasping the implications of biometric technology.

8 List of Tables

9 List of Abbreviations

Abbreviation	Definition
BOE	Boletín Oficial del Estado (“official state bulletin”)
CCTV	Closed circuit television
D1.4	Deliverable 1.4 – Method description decision support test cases
D6.4	Deliverable 1.6 – Final report on security classification
D7.3	Deliverable 7.3 – SurPRISE decision support web-tool
DNA	Deoxyribonucleic acid
DPA	Data protection authority
DPI	Deep Packet Inspection
DSS	Decision Support System
EEA	European Economic Area
EU	European Union
GPS	Global Positioning System
NSA	National Security Agency
SLT	Smartphone Location Tracking
SOST	Surveillance-oriented security technology
TeknoNyt	Name of the DBT newsletter
WP2	Workpackage 2 – Framing the assessment
WP3	Workpackage 3 – Exploring the challanges
WP5	Workpackage 5 – Participatory data gathering
WP7	Workpackage 7 – Decision support testing

10 Appendix

10.1 Screening questionnaire

Screening questionnaire – WP7 small-scale event	
Good morning! I am …………… and I work for ………….. We have a research project about how surveillance-based security solutions like CCTV, civil drones, smartphone location tracking, internet surveillance and biometrics affect the privacy of citizens. If you are interested in a possibility to learn about these things and to share your opinion with others about this topic, I would like to ask a few questions.	
1. GENDER *QUOTA: 50% MALES – 50% FEMALES!*	1 – male 2 - female
2. Which age group do you belong to: *QUOTA: 33% 18-35 – 33% 36-50 – 33% ABOVE 50!*	1 – below 18 *CLOSE!* 2 – 18-35 years old *QUOTA!* 3 – 36-50 years old *QUOTA!* 4 – above 50 *QUOTA!*
3. What is your highest education? *QUOTA: approximate quota should be set based on national statistics:* *PRIMARY – SECONDARY - HIGHER!*	1 – primary *QUOTA!* 2 – secondary *QUOTA!* 3 – higher *QUOTA!*
4. What is your employment status: *MAXIMUM NUMBER OF UNEMPLOYED PEOPLE IS 5!*	1 – work (employee/self-employed) 2 – unemployed 3 – retired 4 – student 5 – other:…………………………
5. What is/was your profession? *A GOOD MIX IS REQUIRED!*	………………………………………
6. Where do you live? *IF POSSIBLE, INVOLVE PEOPLE OUTSIDE [include the city]!*	………………………………………
7. Did you participate in the citizen summit organised about security technologies in [include the month of the large-scale summit**]?**	1 – yes *CLOSE!* 2 – no *GO ON!*
8. How often do you read newspapers or books printed or online for at least 30 minutes?	1 – every day *GO ON!* 2 – a few times a week *GO ON!* 3 – once a week *GO ON!* 4 – more rarely *CLOSE!*
9. In order for you to formulate an informed opinion in the discussions, we shall provide you with an approx. 25-page magazine containing interesting information on the topics we cover. It is very important that you read this material prior to coming to the meeting. Do you agree to read this magazine?	1 – yes *GO ON!* 2 – not sure *CLOSE!* 3 – no *CLOSE!*

10.2 Evaluation questionnaire for participants

I. Please mark with an X in the square beside your answer to indicate how much you agree or disagree with the following opinion:
I have gained new insight by participating in the citizen meeting

☐ Strongly agree
☐ Agree
☐ Neither agree nor disagree
☐ Disagree
☐ Strongly disagree

II. Please mark your agreement or disagreement again:
I believe the citizen meeting has generated valuable knowledge for politicians

☐ Strongly agree
☐ Agree
☐ Neither agree nor disagree
☐ Disagree
☐ Strongly disagree

III. Has this experience changed your attitudes regarding security-oriented surveillance technology? Mark your answer

☐ Yes, they are now more positive
☐ Yes, they are now more negative
☐ No, they are the same as before the meeting

IV. What did you especially like in the process of this citizen meeting?

....

....

....

V. What did you especially dislike in the process of this citizen meeting?

....

....

....

10.3 Evaluation questionnaire for moderators

I. Please mark with X in the square beside your answer to indicate, overall, how satisfied you were with the DSS?

□ I was completely satisfied
□ I was rather satisfied
□ I was neither satisfied nor dissatisfied
□ I was rather dissatisfied
□ I was completely dissatisfied

II. What do you regard as the main strengths of the DSS?

....

....

....

III. What do you regard as the main weaknesses of the DSS?

....

....

....

IV. How did the interaction between the citizens during the event contribute to the formulation of messages and recommendations for the European politicians? Please include examples.

....

....

....

....

....

....

....

....