



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 – Italian citizen meeting

Lead Beneficiary: Medián Opinion and Market Research

Author(s): Maria Grazia Porcedda and Teresa Talò

Dissemination Level: Public









Version: final



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 / Oesterreichische Akademie der Wissenschaften Coordinator, Austria	ITA/OEAW	
Agencia de Protección de Datos de la Comunidad de Madrid*, Spain	APDCM	
Instituto de Políticas y Bienes Públicos/ 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	

This document may be freely used and distributed, provided that the document itself is not modified or shortened, that full authorship credit is given, and that these terms of use are not removed but included with every copy. The SurPRISE partners shall all take no liability for the completeness, correctness or fitness for use. This document may be subject to updates, amendments and additions by the SurPRISE consortium. Please, address questions and comments to: feedback@surprise-project.eu

*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

Table of Contents.....	i
1 Country report of Italy.....	1
1.1 Summary.....	1
1.2 First session of the citizen meeting (SOSTs-neutral)	3
1.2.1 Perceptions of security	3
1.2.2 Opinions on surveillance-based security solutions in general.....	5
1.2.3 Privacy in the Italian culture	7
1.2.4 Regulation and control around SOSTs.....	8
1.3 Second session of the citizen meeting (SOST-specific)	10
1.3.1 Differences and similarities in the perception of particular SOSTs	10
1.3.2 Security agencies and legal safeguards	12
1.3.3 Reflections on the “trade-off” based thinking.....	13
1.3.4 Alternatives.....	14
1.3.5 Recommendations and messages towards the European and national politicians	14
1.4 Process design.....	20
1.5 Evaluation of the event.....	21
1.5.1 How citizens assessed the meeting	21
1.5.2 Evaluation of the DSS by the research staff	22
1.5.3 The role of information debate and group dynamics in citizens’ acceptance of SOSTs.....	22

1 Country report of Italy¹

This chapter² 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 biometrics³, 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.

1.1 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 outcomes⁴. 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 sociodemographic 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

¹ The authors of this chapter: Maria Grazia Porcedda (EUI, SurPRISE) and Teresa Talò (EUI).

² The authors wish to thank Claudia De Concini and Bart Provoost for their help in drafting this report.

³ 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).

⁴ The results of the large-scale event form part of a different report: Porcedda and Zorzi (2014).

- **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.
- **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?** Citizens identified the core as made up of: medical data, vulnerable people's data, religious and political beliefs, sexual orientation, and personal communications.

During the citizens 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 agencies⁵ fairly high, but not unconditionally. Institutions should be accountable;

⁵ 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.

- **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.

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.

1.2 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 (1.2.1); perceptions on surveillance-oriented security solutions (1.2.2); the meaning of privacy (1.2.3); the role of regulation and safeguards (1.2.4). We discuss the outcome of the debate on each topic in sequence.

1.2.1 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.

1.2.1.1 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.

1.2.1.2 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.

1.2.2 Opinions on surveillance-based security solutions in general

1.2.2.1 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 pedophile 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.

1.2.2.2 Awareness of what kind of information are 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.

1.2.2.3 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.

1.2.3 Privacy in the Italian culture

1.2.3.1 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 data⁶). 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

⁶ 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.

raising suspicions.

Figure 1: The meaning of privacy for participants

1.2.3.2 Concerns with regards 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 from 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".

1.2.3.3 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.

1.2.4 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.

1.2.4.1 Awareness and information need

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.

1.2.4.2 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 fulfillment 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.

1.3 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 (1.3.1); use by security agencies and related legal safeguards (1.3.2); potential trade-offs (1.3.3); and alternatives (1.3.4). Participants were asked to reach a conclusion (‘recommendation’, 1.3.5) for each of these themes participants assessed the consensus reached.

1.3.1 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.

1.3.1.1 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 signaled 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.

1.3.1.2 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 behavior 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

1.3.1.3 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.

1.3.1.4 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.

1.3.1.5 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.

1.3.2 Security agencies and legal safeguards

An overwhelming majority of respondents (87%)⁷ stated that security agencies (that use SOSTs in Italy) are trustworthy. A similarly high rate (66%) of voters⁸ 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 SOSTs⁹. Not only is the level of trust in security agencies in line with other studies¹⁰, but also fear of abuses might decrease vis-à-vis the skepticism surrounding the commercial usage of personal information. Indeed, some citizens said that they trusted

⁷ 33 responses over 38 voters. The voting results of one table are missing.

⁸ Over 38 voters. The voting results of one table are missing.

⁹ Porcedda and Zorzi (2014).

¹⁰ Ibid.

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 Italy¹¹). 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

1.3.3 Reflections on the "trade-off" based thinking

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.

¹¹ Ibid.

1.3.4 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 of 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”.

1.3.5 Recommendations and messages towards the European and national politicians

In this section we cluster the recommendations formulated by the six tables around the main themes (1.3.5.1.) and we report verbatim the content of postcards filled in and delivered by participants at the end of the event (1.3.5.1).

1.3.5.1 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.

1.3.5.2 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 analyze the presentand are interpreted by a person) rather than foresee (i.e. perform historical analysis over the data, or create preset profiles for future searches). Let's train the police to use the technologies efficiently.

1.3.5.3 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.

1.3.5.4 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.

1.3.5.5 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.

1.3.5.6 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.

1.3.5.7 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 seaborne 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 forcibly.

Figure 2 Individual Recommendations (postcards)

1.4 Process design

The Italian SurPRISE citizen meeting took place on June 17th, in Florence¹². 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 citizens 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 gift¹³ 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.

1.4.1.1 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 citizens¹⁴ showed up, out of 65 overall invitees (to account for no-shows¹⁵). All participants signed a consent form for the processing of their personal data both upon invitation and on the day of the event.

¹² 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 Avalue, Sandro Buggiani, Nicolò Caciotti, Luca Caterino, Lapo Cecconi, Giulia Ciampi, Marco Algimiro Fusaro, Carlotta Iarrapino, Valeria Maione, Marco Scarselli, Antonio Volino and Alberto Zinanni.

¹³ Participants received a voucher for a complimentary dinner at a local restaurant (Runner Pizza) as well as a discount for accompanying guests.

¹⁴ 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).

¹⁵ 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.

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 were 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.

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%

Figure 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.

1.5 Evaluation of the event

1.5.1 How citizens assessed the meeting

1.5.1.1 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.

1.5.1.2 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.

1.5.2 Evaluation of the DSS by the research staff

1.5.2.1 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.

1.5.2.2 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.

1.5.3 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