"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 6.12 – Workshop Report

Lead Beneficiary: ITA/OeAW

Author(s): Stefan Strauß (ITA/OeAW)

Due Date: September 2014

Submission Date: December 2014

Dissemination Level: Public

Version: 1

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

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

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

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

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

Table of Contents

About SurPRISE i
1 Introduction 1
1.1 Purpose and setting of the stakeholder workshop 1
2 Background information 2
2.1 Citizen participation in SurPRISE 2
2.2 Large-scale participation with the citizen summits 2
2.3 Small-scale citizens meetings 3
3 Agenda 4
4 Presentations at the workshop 6
4.1 Introduction to the Expert & Stakeholder Workshop 6
4.2 Presentations of the results of the participatory events 10
5 Participants 46

About SurPRISE

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

A core objective of SurPRISE is to re-examine the relationship between security and privacy. This relation is commonly positioned as a 'trade-off', accordingly infringements of privacy are sometimes seen as an acceptable cost of enhanced security. This common understanding of the security-privacy relationship, both at state and citizen level, has informed and influenced policymakers, legislative developments and best practice guidelines concerning security developments across the EU. However, an emergent body of scientific work and public scepticism questions the validity of the security-privacy trade-off. In response to these developments, SurPRISE investigates the relation between surveillance, privacy and security from a scientific as well as citizen's perspective. A major aim of SurPRISE is to identify criteria and factors, which contribute to the shaping of security technologies and measures as effective, non-privacy-infringing and socially legitimate security devices in line with human rights and European values.

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

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

1 Introduction

This report covers a description of the second expert and stakeholder workshop, hold within work package 6. It briefly presents the purpose, setting and participants of the international stakeholder workshop held in Florence, Italy in October 2014. The main objective of this workshop was to present and discuss major outcomes and results from the SurPRISE project regarding decision support, policy options and recommendations developed within the participatory events (described in the next section) conducted in SurPRISE with experts from different fields.

1.1 Purpose and setting of the stakeholder workshop

The employment of the stakeholder workshop served the main purpose to get additional input, win new perspectives and expert perceptions about the recommendations derived from the large-scale citizen summits and the small scale events as described in the next section. For this reason, a number of international experts from different fields were invited to the workshop in order to discuss a set of recommendations addressing a number of issues raised by the citizens.

The setting of the workshop consisted of three main building blocks: (1) a brief background information a few days before were submitted to the participating experts. (2) the workshop started with presentations given by members of the SurPRISE consortium providing some insights into the main results from the project (for details see section 4). (3) The main part of the stakeholder workshop was dedicated to moderated table discussions with the experts. In order to establish a vivid climate for discussions with different perspectives, each table consisted of experts from different fields.

At each of these tables 4 draft recommendations were discussed by the stakeholders. These recommendations were gathered from the results of the different discussion rounds at the participatory events and represent major issues of concern for the participating citizens. The topics were mixed ranging from legal, technical, organisational, political and economic issues in the privacy-security context that were discussed and raised by the citizens during the participatory events. At the workshop each table was facilitated with members of the SurPRISE consortium one acting as moderator the other as a table secretary taking notes that were directly integrated into a Web-based tool prepared by the Danish Board of Technology. In the next step, the main discussion points raised by the experts were presented via this tool from the note takers at each table to the audience for a short plenary discussion to gather the most important issues. During the lively discussions the experts brought in several additional and new perspectives to the recommendations derived from the participatory events. In total, this stakeholder workshop provided important input for assessing and improving the applicability of the recommendations towards decision making processes as will be elaborated in the final policy paper Deliverable 6.13.

An alliance with relevant experts and stakeholders is essential. They can contribute to a broader view and debate on citizens, privacy, security and surveillance. The experts who were invited are heterogeneous, representing different levels of interest and influence, but all of them play to a lesser or greater extent a role when it comes to changing the discourse as different perspectives are also crucial for considering and developing alternatives to existing security approaches.

The invited users and stakeholders for the workshop cover a broad range of different experts including decision makers, representatives from the security industry, technology developers and suppliers, the European Commission, national security research programmes, law enforcement agencies, data protection authorities, ministries as well as civil society, particularly members from human rights and privacy organisations. A list of participants can be found in section 5.

2 Background information

2.1 Citizen participation in SurPRISE

The increasing role and use of surveillance-oriented security technologies (SOSTs) for a variety of purposes is a matter of societal concern, which is evident in a number of public discourses. Although citizens are directly affected by the security and surveillance measures employed in their countries, their views and opinions on these issues are widely unknown. To narrow the gap, the SurPRISE project gave European citizens the unique opportunity to express and discuss their perceptions regarding security technologies and their implications at twelve 'citizen summits', which were organized in nine different countries: Germany, the United Kingdom, Denmark, Hungary, Norway, Spain, Italy, Austria, and Switzerland in the first half of 2014.[2]

Two series of participatory events were organised in order to learn more about how the general public perceives the relation between privacy, security and surveillance, and to consult citizens as to which policies they would like to see in place. These events were public meetings where citizens gathered to have face-to-face discussions about surveillance-oriented security technologies. The first series of participatory events were large-scale citizen summits organised in nine European countries in the first quarter of 2014 with about 150 to 200 citizens in each country. In addition, five countries out of these nine organised "Small-Scale Citizen Meetings" in June of 2014.

2.2 Large-scale participation with the citizen summits

The summits aimed at exploring the perceptions of citizens on the relation between privacy, security and surveillance, and at consulting them as to which policies they would like to see in place. The summits featured the analysis of three different SOSTs (smart CCTV, Deep Packet Inspection - DPI and Smart Phone Location Tracking - SLT). The use of SOSTs served two purposes: providing concrete examples for the discussions, as well as investigating the interrelations between perceived effectiveness and intrusiveness of SOSTs, and related concerns. To gain deeper insight into participants' opinions, the SurPRISE summits were based on a mixed approach combining quantitative and qualitative elements. In detail, a set of pre-defined questions and statements clustered around different topics was complemented by discussion rounds relating to such thematic blocks.

Participants were divided into groups of 6-8 people and sat at tables facilitated by a moderator. At each summit, the methodology was integrated by two interactive components: (1) the survey was linked to an electronic polling system that allowed participants to immediately answer the questions via keypads, whereas the results were presented right after the polling; (2) to stimulate discussions, for each of the two SOSTs, a short film was presented where experts from different backgrounds gave their assessments to the corresponding SOST. Prior to attending the summit, participants received an information brochure. The provided mix between written (brochure) and visual (films) information helped equalizing participants' knowledge, which enabled discussions on relatively equal footing. For each table, a moderator facilitated the discussion rounds and supported participants if necessary in case of general requests. In preparation of the summit, table moderators received guidelines about the process design, and were trained to perform their tasks. In total, three discussion rounds were conducted. Two one for each SOST, focussed on the perceived benefits and risks in relation to the particular form of surveillance, in order to gain more insights into the participant's views. The third and final discussion round aimed at participants developing suggestions and recommendations to policy makers at national as well as European level.

[2] http://surprise-project.eu/events/citizen-summits/)

2.3 Small-scale citizens meetings

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

A new and innovative, web-based[3] 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:

- 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[4]. 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.

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

4 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 Agenda

surprise

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

SurPRISE Experts Meeting

Florence, 16 October 2014

Palazzo Strozzi, Sala Altana
Piazza Strozzi, Firenze

CONTACT INFORMATION:

maria.porcedda@eui.eu; mathias.vermeulen@eui.eu; Claudia.DeConcini@EUI.eu

Please note that Palazzo Strozzi's exhibitions are open until 11 PM on Thursday (http://www.palazzostrozzi.org/)

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

PROGRAMME

9:45 – 10:15	**Registration** *Welcome Coffee*
10:15 – 10:30	**Welcome and presentation of the programme of the day** Professor Martin Scheinin (EUI) and Johann Čas (ITA – Austrian Academy of Sciences, SurPRISE coordinator)
10:30 – 11:45	**Presentation of the results of the participatory events** Mr. Jacob Skjødt Nielsen (DBT): *the participatory methodology and the DSS* Ms. Sara Degli Esposti (OU): *results of the 12 citizens summits* Ms. Marta Szenay (Median): *results of the 5 citizens meetings* Chaired by Ms. Maria Grazia Porcedda (EUI)
11:45 – 13:00	**Roundtable discussing the results of the participatory events** *Stakeholder's discussion of main results and Q&A* Chaired by Dr. Walter Peissl (ITA, deputy director)
13:00 – 14:30	*Lunch at Obikà, Via Tornabuoni n. 16*
14:30 – 16: 00	**Table discussions of recommendations and policy docs with DSS** Facilitated from the stage by Ms. Marianne Barland (NBT)
16:00 – 16:30	*Coffee break*
16:30 – 17:00	**Reporting of table discussion's results and synthesis** *Reports of the main results of the work at the tables (SurPRISE facilitators)* Chaired by Johann Čas (ITA, SurPRISE consortium leader)
17: 00 – 17:30	**Surveillance, Privacy and Security - Perceptions, Politics and Law in the aftermath of the Snowden revelations** Professor Martin Scheinin (EUI)
17: 30 – 17:45	**Closing remarks and end of conference** Johann Čas (ITA, SurPRISE coordinator)
18:00 – 19:00	*Wine tasting sponsored by Consorzio Vino Chianti accompanied by an Italian-style aperitif*

Chianti
CONSORZIO VINO CHIANTI

Con il Patrocinio del

COMUNE DI FIRENZE

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

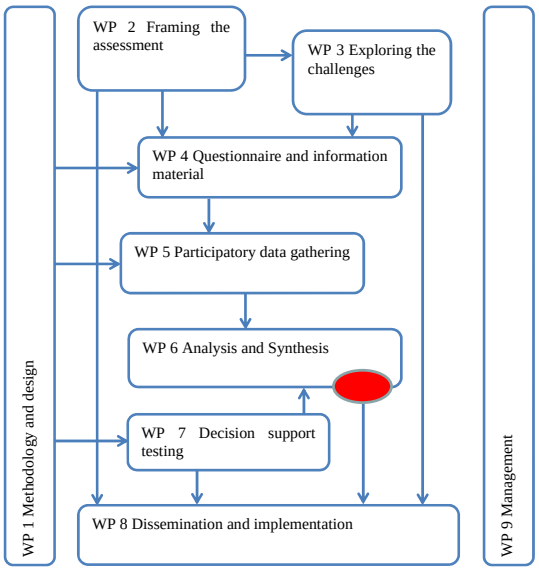
4 Presentations at the workshop

4.1 Introduction to the Expert & Stakeholder Workshop

Topic: The relationship between Human privacy and security

- **Problem:**
  - New security technologies are subjecting ordinary citizens to an increasing amount of permanent surveillance, potentially causing infringements of privacy and restrictions of fundamental rights
- **Research** questions and conditions
  - Do people **actually** think **in terms of a trade-off**?
  - What are **the main factors that affect public assessment**?
  - The **data should be gathered across Europe**
- **Objectives**
  - **Provide decision support for security investments,** taking into account **a wider societal context**.
  - **To design security policies and technologies in a way that respects human rights and European values**.

SurPRISE Work Packages



surprise

Your involvement today

- Feedback on the methodology and on main results of the participatory events
- Table discussions of recommendations
  - Based on citizens' main concerns and requests
  - Your (mixed) expertise is requested

ITA INSTITUTE OF TECHNOLOGY ASSESSMENT

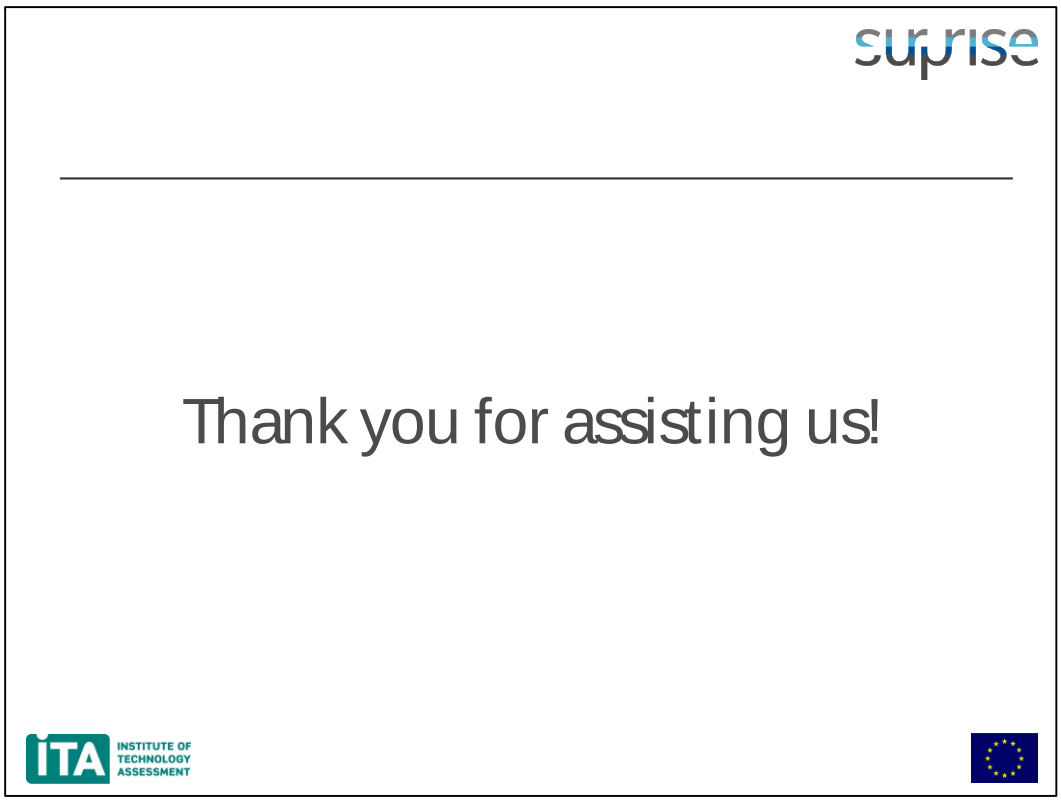
surprise

Invitation to Joint Conference

- Citizens' Perspectives on Surveillance, Security and Privacy: Controversies, Alternatives and Solutions
- Three EU FP7 research projects
  - SurPRISE
  - PACT
  - PRISMS
- 13th-14th November 2014, Vienna

http://surprise-project.eu/events/international-conference/

ITA INSTITUTE OF TECHNOLOGY ASSESSMENT


Thank you for assisting us!
INSTITUTE OF TECHNOLOGY ASSESSMENT

4.2 Presentations of the results of the participatory events

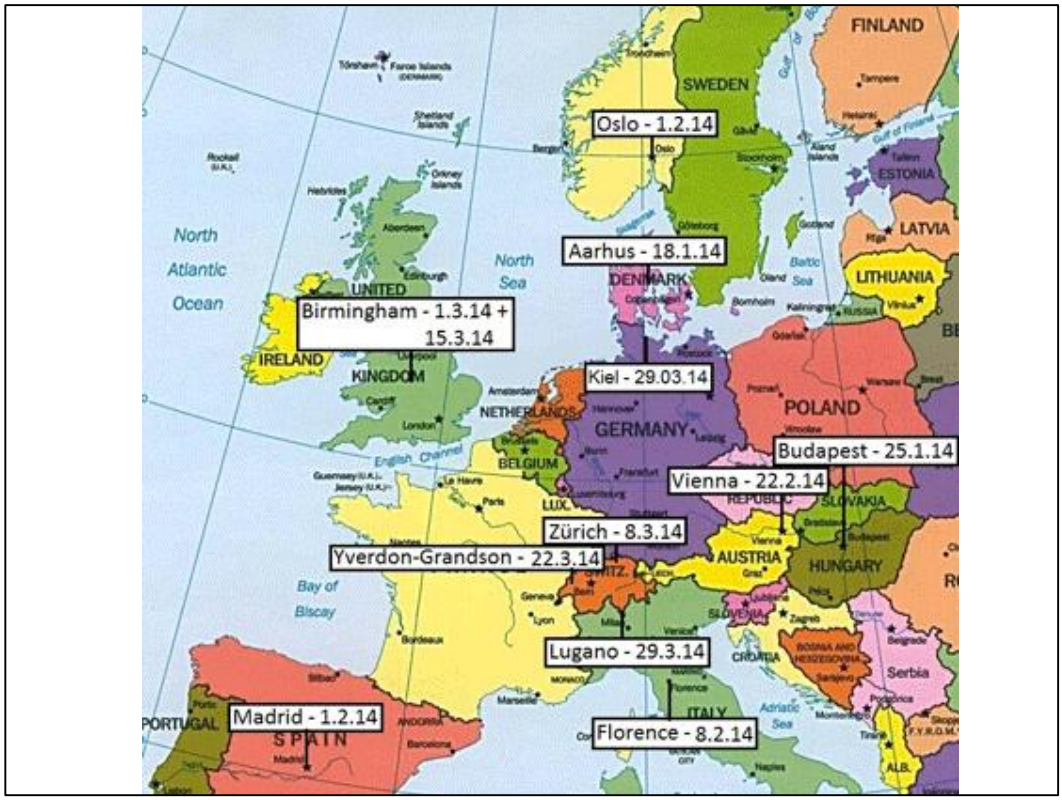
The participatory methodology and the Decision support system (DSS)

Surprise participatory events

- "Large-Scale Citizen Summits" in 9 countries with about 200 citizens in each summit.
- "Small-Scale Citizen Meetings" in 5 countries with about 30 citizen in each meeting.
- Decision support system (DSS)

The aim of citizen engagement

- Dialogue and assessment of *Surveillance Oriented Security Technologies* (SOSTs)
- Gain insights about what citizens think of certain controversial matters
- To inform policy makers.



Knowlegde and Information

- The citizens received the same information, both before and during the meetings (invitation letter, booklet, short films and explanations by meeting facilitators and table moderators.
- All meetings had the same facilitated process and participants answered the same set of predefined questions.

SurPRISE citizen summits

- SurPRISE citizen summits integrate academic research, technology assessment and policy making.
- The questions were developed using a theoretical model
- During a citizen summits, citizens learn the positions of **experts and stakeholder groups** and what **considerations other people** has.
- In combination with **their own values**, **worldviews and life experience**, the participants can better express informed opinions and make thoughtful recommendations.
- Giving the **citizens a voice** to be heard by decision makers
- The SurPRISE summits generated **quantitative and qualitative data** relevant to both academic researchers, policy makers and the media.

Large-Scale Citizen Summits setup

- Participants was assigned to groups of 6-8 people (approx. 200 people).
- Table facilitator moderate the discussions, ensure that everybody is heard.
- A head facilitator coordinates the event.
- Use of clickers (wireless audience response system)
- Anonymous and instant process made it possible to show participants their responses immediately.

Citizen summit questions

- General questions related to security
- Focus on two of three specific *surveillance-oriented security technologies* (SOSTs), which was introduced by a short film (5-7 minutes). (i.e. Smart CCTV; Deep Packet Inspection or Smart Phone Location Tracking).
- Questions about the SOST presented in the film. Repeated for two different SOSTs
- Each table formulated one recommendation

Small-Scale Citizen Meetings

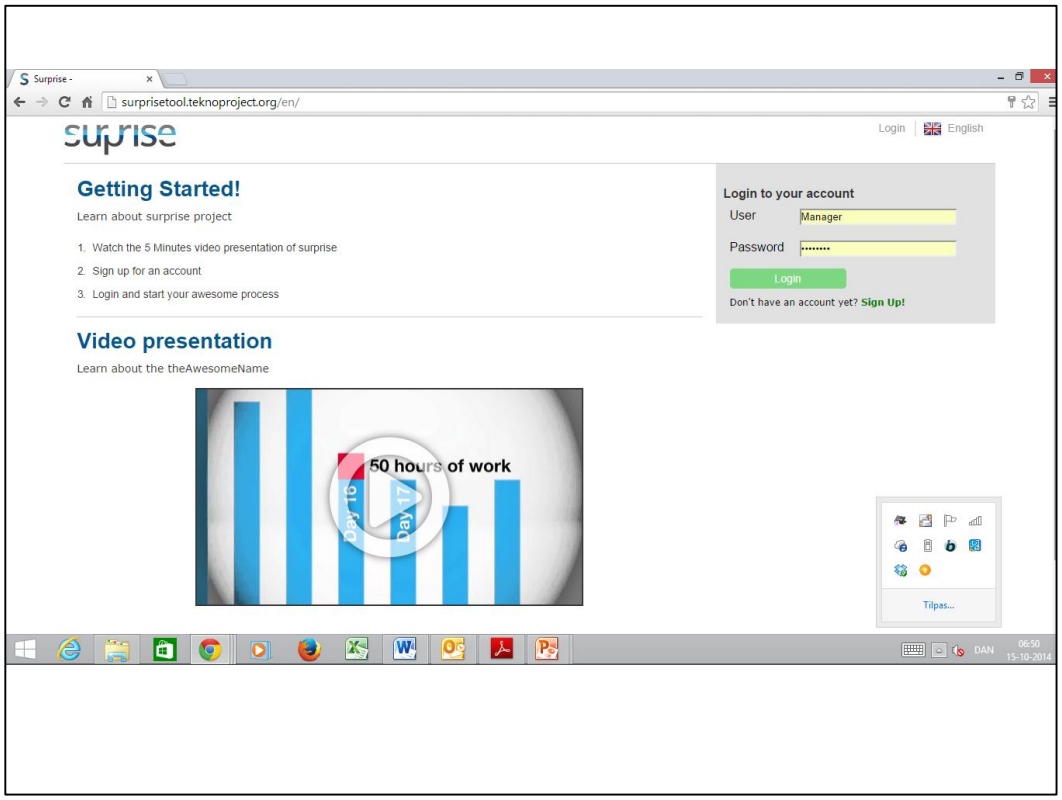
- The main objectives of the Small-Scale Citizen Meetings were to supplement the results of the large scale citizen summits:
- Including new SOSTs: drones and biometrics
- Investigating factors and criteria influencing trust and concerns of citizens about the security challenges
- In-depth discussions using qualitative methodologies
- To evaluate the use of a web-based tool to support and streamline the facilitation of the decision support system.

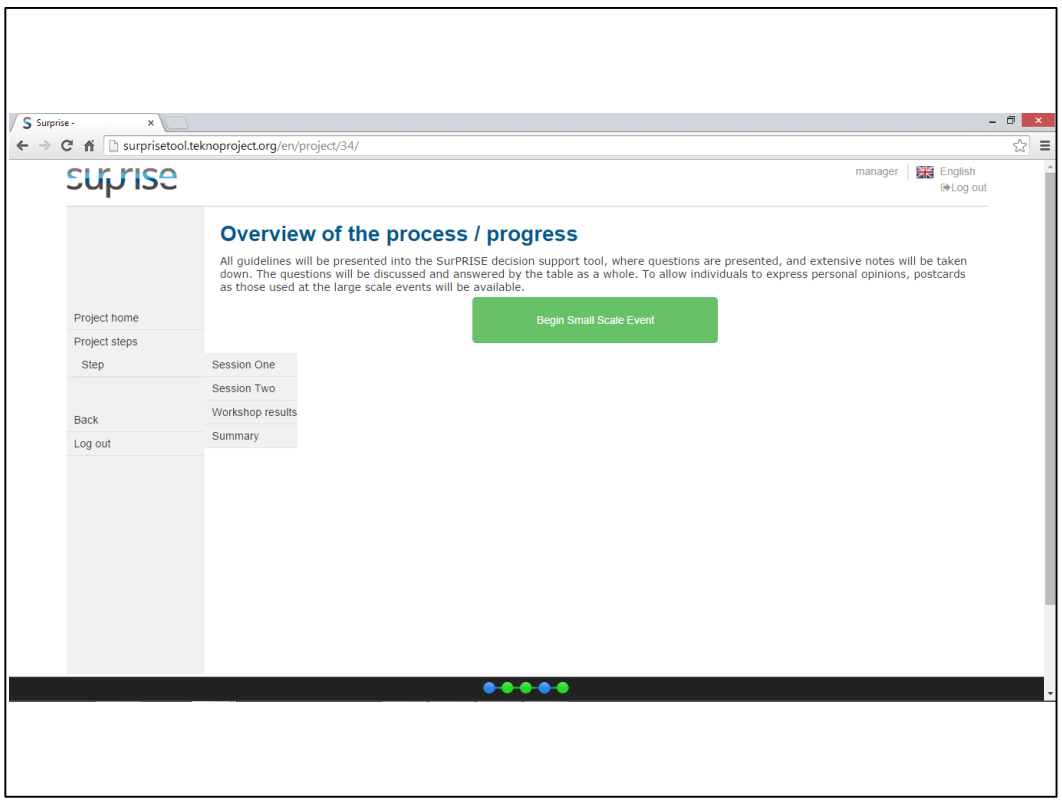
Small-Scale Citizen Meetings

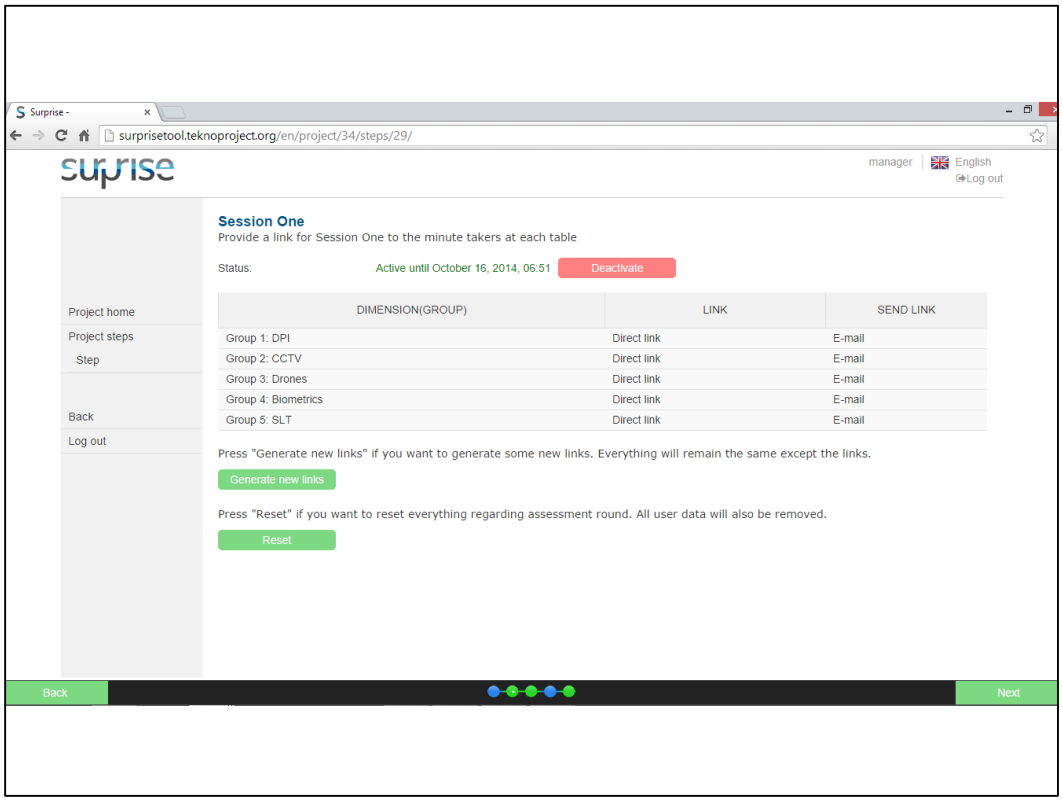
- Small-scale citizen meetings were held in Denmark, Hungary, Italy, Norway and Spain involving 25-40 participants in each country
- Learnings from the large scale summits – further investigation
- Information magazine including chapters on Drones, Biometrics and Alternative solutions.
- Discussions were recorded in the DSS

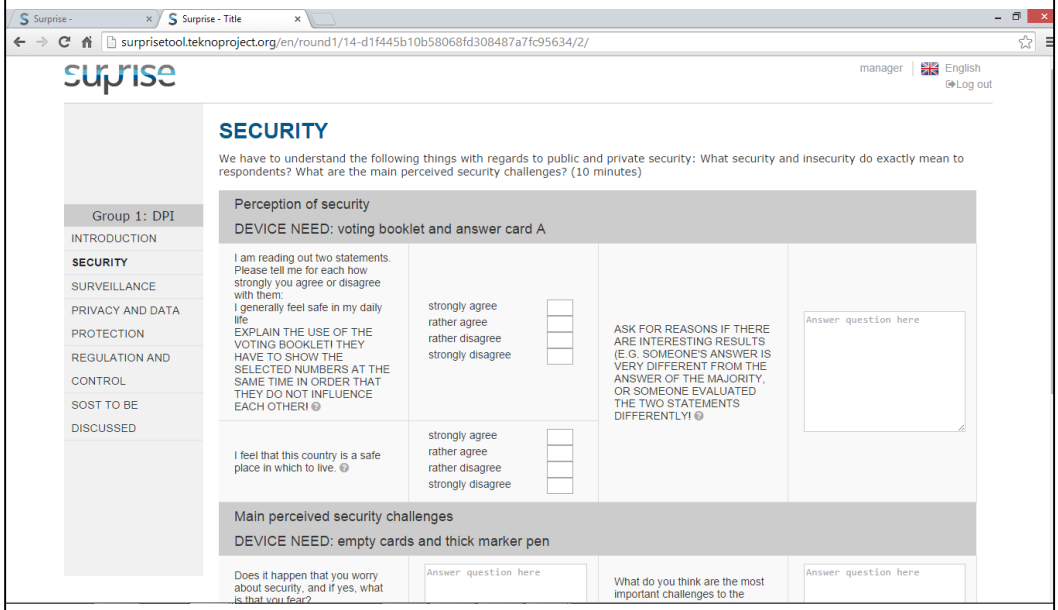
Small-Scale Citizen Meetings

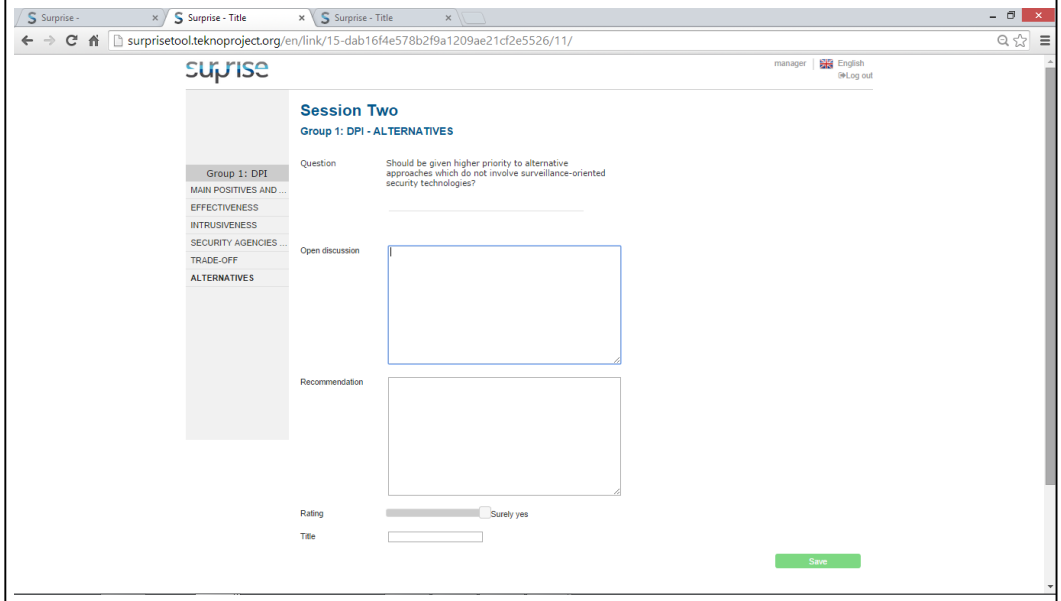
- The Small-Scale Citizen Meetings consisted of two sessions
- The first part investigated how citizens understand the central terms (security, surveillance, privacy, data protection, regulation and the institutions that make use of SOSTs.)
- The second part focused on one SOST and the participant made recommendations

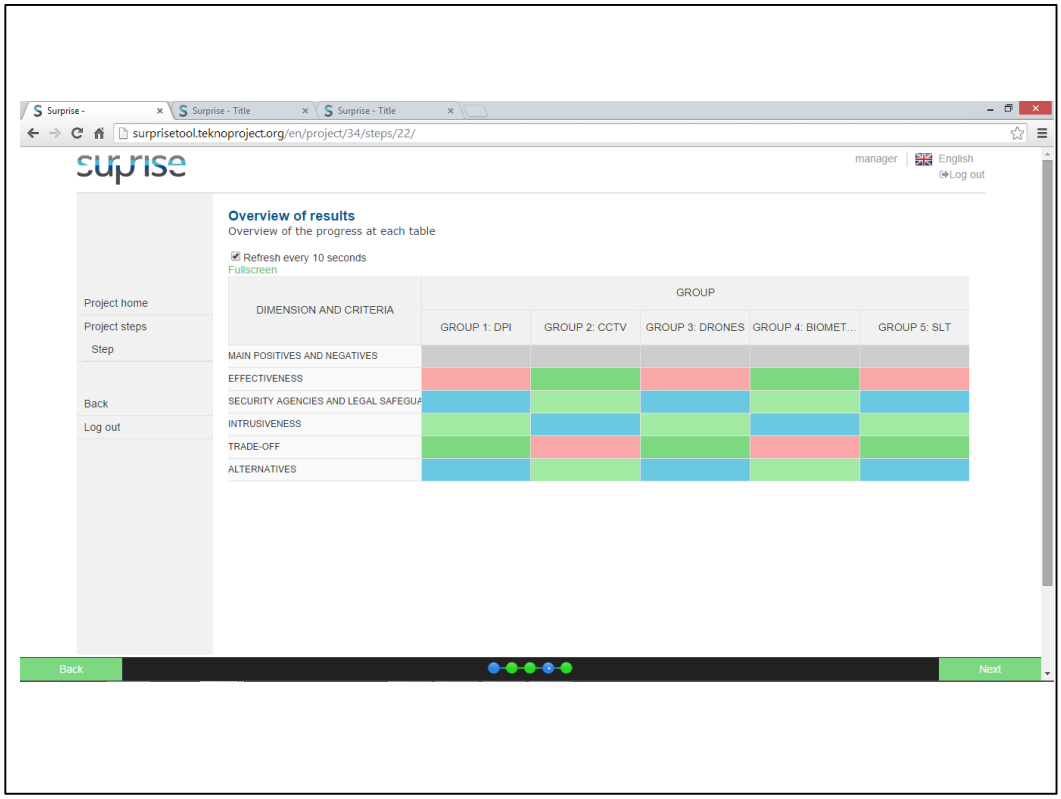

Surprise -
surprisetool.teknoproject.org/en/
surprise
Login | English
Getting Started!
Learn about surprise project
1. Watch the 5 Minutes video presentation of surprise
2. Sign up for an account
3. Login and start your awesome process
Login to your account
User
Manager
Password
Login
Don't have an account yet? Sign Up!
Video presentation
Learn about the theAwesomeName
50 hours of work
Day 1
Day 10
Tilpas...
DAN
06:50
15-10-2014

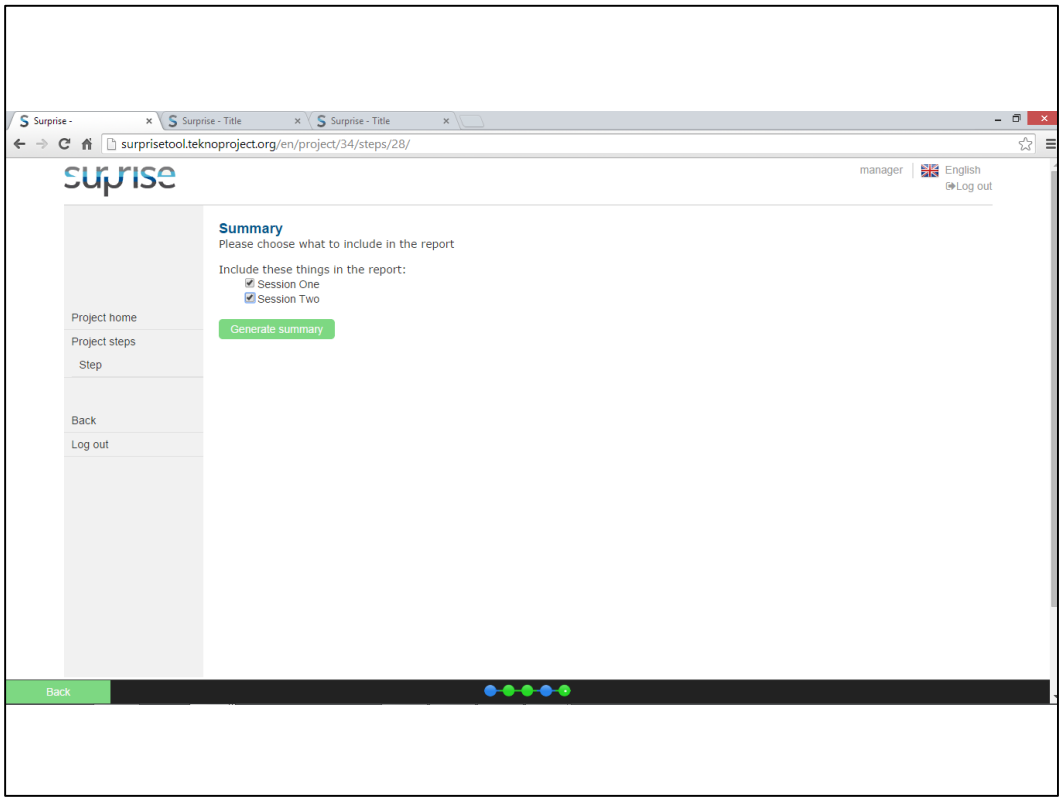

Surprise -
surprisetool.teknoproject.org/en/project/34/
surprise
manager | English
Log out
Overview of the process / progress
All guidelines will be presented into the SurPRISE decision support tool, where questions are presented, and extensive notes will be taken down. The questions will be discussed and answered by the table as a whole. To allow individuals to express personal opinions, postcards as those used at the large scale events will be available.
Begin Small Scale Event
Project home
Project steps
Step
Session One
Session Two
Workshop results
Summary
Back
Log out


Surprise -
surprisetool.teknoproject.org/en/project/34/steps/29/
manager
English
Log out
Session One
Provide a link for Session One to the minute takers at each table
Status:
Active until October 16, 2014, 06:51
Deactivate
DIMENSION(GROUP)
LINK
SEND LINK
Group 1: DPI
Direct link
E-mail
Group 2: CCTV
Direct link
E-mail
Group 3: Drones
Direct link
E-mail
Group 4: Biometrics
Direct link
E-mail
Group 5: SLT
Direct link
E-mail
Project home
Project steps
Step
Back
Log out
Press "Generate new links" if you want to generate some new links. Everything will remain the same except the links.
Generate new links
Press "Reset" if you want to reset everything regarding assessment round. All user data will also be removed.
Reset
Back
Next


Surprise -
Surprise - Title
surprisetool.teknoproject.org/en/round1/14-d1f445b10b58068fd308487a7fc95634/2/
manager
English
Log out
SECURITY
We have to understand the following things with regards to public and private security: What security and insecurity do exactly mean to respondents? What are the main perceived security challenges? (10 minutes)
Group 1: DPI
INTRODUCTION
SECURITY
SURVEILLANCE
PRIVACY AND DATA PROTECTION
REGULATION AND CONTROL
SOST TO BE DISCUSSED
Perception of security
DEVICE NEED: voting booklet and answer card A
I am reading out two statements. Please tell me for each how strongly you agree or disagree with them:
I generally feel safe in my daily life
EXPLAIN THE USE OF THE VOTING BOOKLET! THEY HAVE TO SHOW THE SELECTED NUMBERS AT THE SAME TIME IN ORDER THAT THEY DO NOT INFLUENCE EACH OTHER!
strongly agree
rather agree
rather disagree
strongly disagree
ASK FOR REASONS IF THERE ARE INTERESTING RESULTS (E.G. SOMEONE'S ANSWER IS VERY DIFFERENT FROM THE ANSWER OF THE MAJORITY, OR SOMEONE EVALUATED THE TWO STATEMENTS DIFFERENTLY!
Answer question here
I feel that this country is a safe place in which to live.
strongly agree
rather agree
rather disagree
strongly disagree
Main perceived security challenges
DEVICE NEED: empty cards and thick marker pen
Does it happen that you worry about security, and if yes, what is that you fear?
Answer question here
What do you think are the most important challenges to the
Answer question here


surprisetool.teknoproject.org/en/link/15-dab16f4e578b2f9a1209ae21cf2e5526/11/
manager
English
Log out
Session Two
Group 1: DPI - ALTERNATIVES
Group 1: DPI
MAIN POSITIVES AND ...
EFFECTIVENESS
INTRUSIVENESS
SECURITY AGENCIES ...
TRADE-OFF
ALTERNATIVES
Question
Should be given higher priority to alternative approaches which do not involve surveillance-oriented security technologies?
Open discussion
Recommendation
Rating
Surely yes
Title
Save


surprisetool.teknoproject.org/en/project/34/steps/22/
manager
English
Log out
Overview of results
Overview of the progress at each table
Refresh every 10 seconds
Fullscreen
Project home
Project steps
Step
Back
Log out
DIMENSION AND CRITERIA
GROUP
GROUP 1: DPI
GROUP 2: CCTV
GROUP 3: DRONES
GROUP 4: BIOMET...
GROUP 5: SLT
MAIN POSITIVES AND NEGATIVES
EFFECTIVENESS
SECURITY AGENCIES AND LEGAL SAFEGUA
INTRUSIVENESS
TRADE-OFF
ALTERNATIVES
Back
Next


Surprise -
Surprise - Title
Surprise - Title
surprisetool.teknoproject.org/en/project/34/steps/28/
surprise
manager
English
Log out
Summary
Please choose what to include in the report
Include these things in the report:
Session One
Session Two
Generate summary
Project home
Project steps
Step
Back
Log out
Back

Results of the 12 citizen summits

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

Surveillance, Privacy and Security:

Results of large scale participatory events

Sara Degli Esposti
Centre for Research into Information Surveillance and Privacy (CRISP)

Vincenzo Pavone and Elvira Santiago
Institute of Public Goods and Policies (IPP-CSIC)

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

Research questions

1) What are the **factors** which play a major role in shaping public attitudes toward SOSTs?
2) What are the effects of relying on the privacy-security **tradeoff model** in assessing SOSTs?
3) What are the **criteria** that should be adopted when introducing new SOSTs?

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

Citizen summits dates & locations

1.	**Denmark** (Aarhus 18/Jan)	**SLT & sCCTV**
2.	**Hungary** (Budapest 25/Jan)	**SLT & sCCTV**
3.	**Norway** (Oslo 01/Feb)	**DPI & SLT**
4.	**Spain** (Madrid 01/Feb)	**sCCTV & DPI**
5.	**Italy** (Florence 8/Feb)	**DPI & SLT**
6.	**Austria** (Vienna 22/Feb)	**sCCTV & DPI**
7.	**United Kingdom** (Birmingham, 1/Mar and 15/Mar)	**sCCTV & DPI**
8.	**Switzerland** (Zürich 8/Mar, Iverdu 22/Mar, Lugano 29/Mar)	**DPI & SLT**
9.	**Germany** (Kiel, 29/Mar)	**SLT & sCCTV**

	sCCTV	DPI	SLT
1	Denmark	Norway	Denmark
2	Hungary	Italy	Hungary
3	Spain	Spain	Norway
4	Austria	Austria	Italy
5	UK	UK	Switzerland
6	Germany	Switzerland	Germany
	1.198	**1.202**	**1.144**

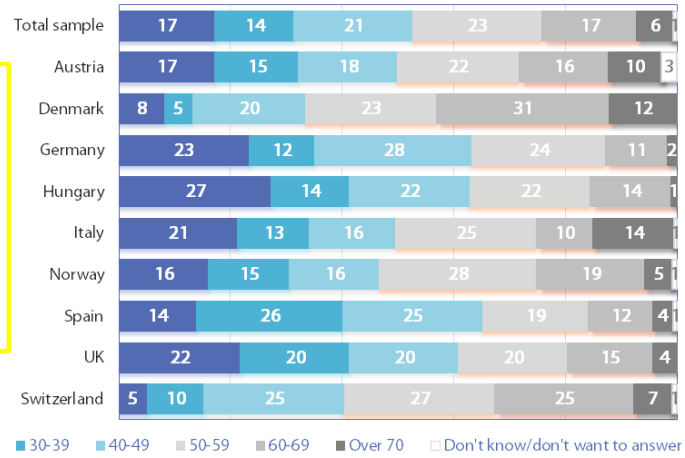
About 1.000 citizens were asked questions about each SOST

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

Demographics

A balanced sample

About 200 citizens per country



Gender	Austria	Denmark	Germany	Hungary	Italy	Norway	Spain	UK	Switzerland	Total
Female	108	94	117	89	98	61	75	99	142	883
	50,7%	59,9%	63,6%	43,4%	52,7%	54,5%	46,6%	47,4%	58,2%	52,8%
Male	105	63	67	116	88	51	86	110	102	788
	49,3%	40,1%	36,4%	56,6%	47,3%	45,5%	53,4%	52,6%	41,8%	47,2%
Total	**213**	**157**	**184**	**205**	**186**	**112**	**161**	**209**	**244**	1671
	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

Q1: Factors influencing acceptance

1) ***Institutional Trustworthiness***
   1) Security agents' Ability; Benevolence; Integrity
2) ***SOSTs' Perceived Effectiveness***
   1) Accuracy; Perceived Security; Validity
3) ***SOSTs' Perceived Intrusiveness***
   1) Risk of Embarrassment; Intrusiveness; Risk of human rights infringement
4) **SOSTs' Social, Spatial & Temporal Proximity**
5) ***Substantive Privacy Concerns***
   1) Intimacy; Anonymity; Solitude
   2) Information Privacy Concerns (Data Collection; Unauthorised Secondary Use; Improper Access; Errors)

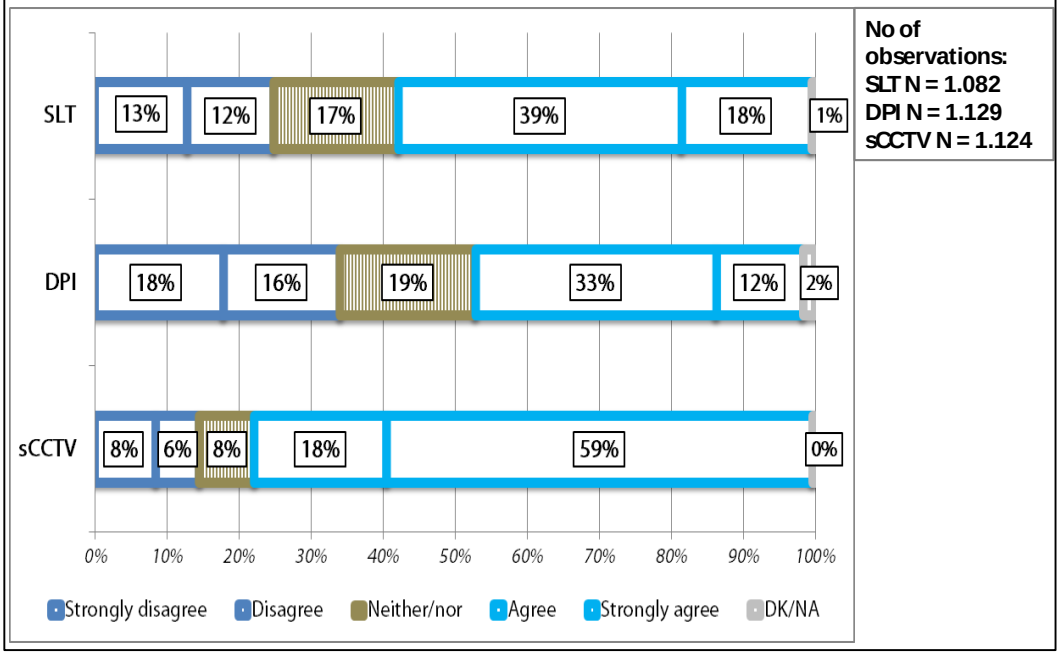
Acceptability of
(A) sCCTV
(B) DPI
(C) SLT

Age; Gender; Education; Earnings

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

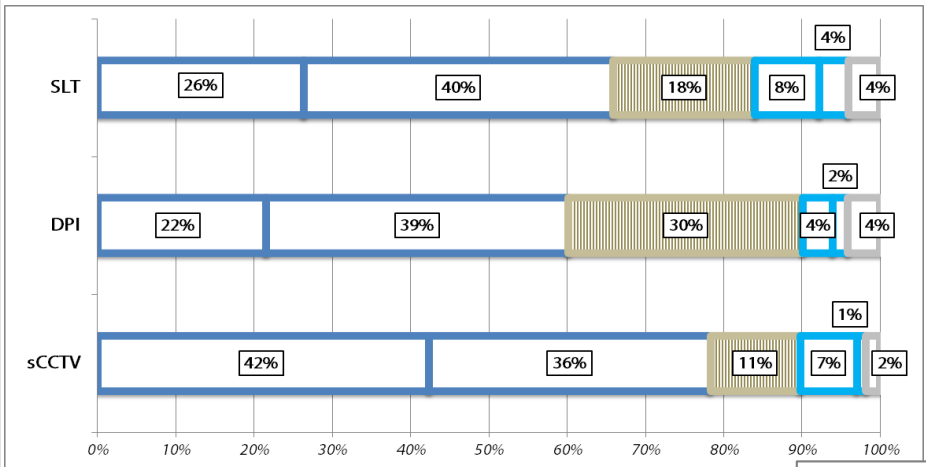
sara.degliesposti@open.ac.uk

DV1: Overall I support the adoption of sCCTV/ DPI/SLT as a national security measure



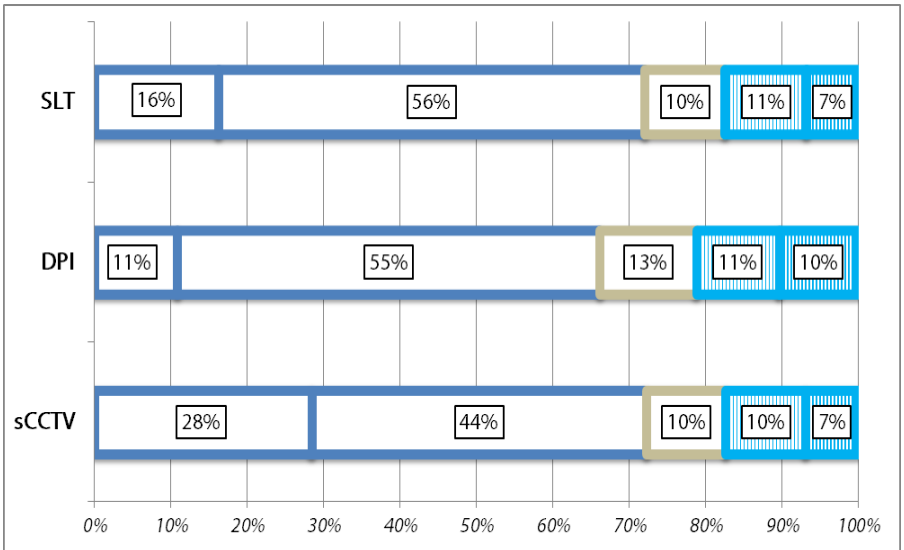
No of observations:
SLT N = 1.082
DPI N = 1.129
sCCTV N = 1.124

DV2: Active avoidance of sCCTV/DPI/SLT

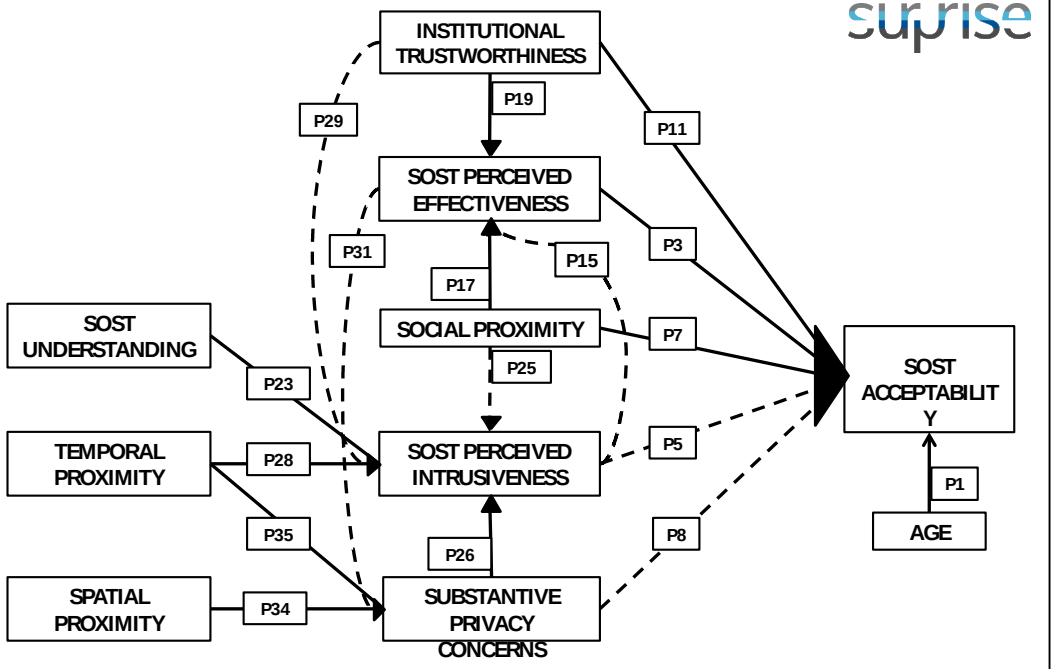


No of observations:
SLT N = 1.087
DPI N = 1.134
sCCTV N = 1.141

DV3: Opposing/Resisting sCCTV/DPI/SLT

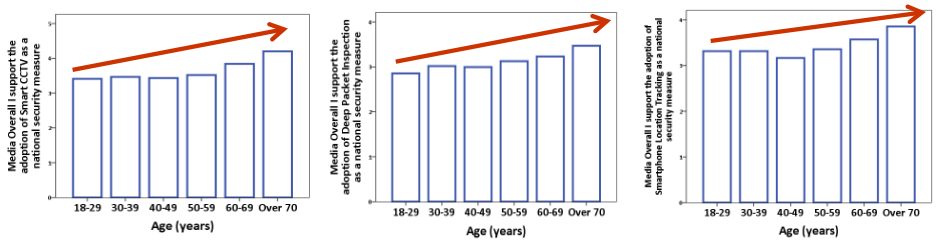


No. of observations:
ACC_CCT3 = 1.141
ACC_DPI3 = 1.134
ACC_SLT3 = 1.087

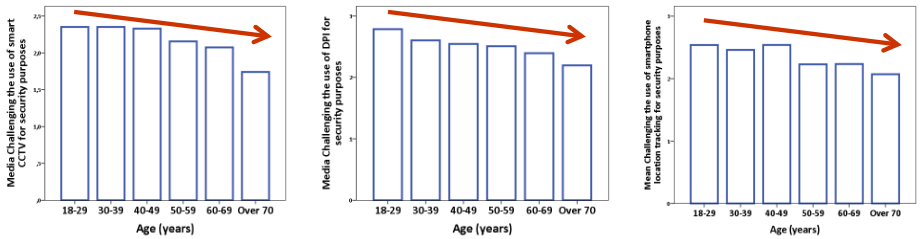


Q1: Factors influencing SOSTs' Acceptability, SOSTs' Perceived Effectiveness, SOSTs' Perceived Intrusiveness and people's Privacy Concerns

Acceptance increases with age..



.. While young people are those more willing to oppose a new SOST.



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

Q1: ACCEPTABLE SOSTs..

MUST BE..

- ..ACCURATE & EFFECTIVE
- ..MANAGED BY CAPABLE & HONEST SECURITY AGENTS
- ..CLEARLY TARGETED TOWARD CRIMINALS.

SHOULD AVOID TO..

- ..PROCESS SENSITIVE INFORMATION ABOUT PEOPLE's INTIMATE LIVES
- ..EXPOSE PEOPLE TO THE RISK OF FEELING EMBARASSED AND SELF CONSCIOUS.

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

sara.degliesposti@open.ac.uk

Q1: Emerging Qualitative Factors

SOSTs which..

Favorable assessment

✓ ..target crimes which are within the citizens' priorities;
✓ ..empower citizens and make them feel in control;
✓ ..are employed with a clear, delimited purpose in mind.

Unfavorable assessment

× ..promote intolerance and segregation;
× ..posit high function creep risks;
× ..undermine the role of humans;
× ..involve private sector or other pro fit-oriented entities.

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

Q1: Emerging Qualitative Factors

Trustworthiness

The more trustworthy the security agencies managing a specific SOST are, the more likely to be perceived as acceptable the SOST will be. **The opposite is also true**: the use of a more acceptable SOST (CCTVs or SLT) helps security agencies to be perceived as more trustworthy.

*The key question is not just how safe is the technology, but also **how safe is the context** in which the technology is implemented.*

Privacy Concerns

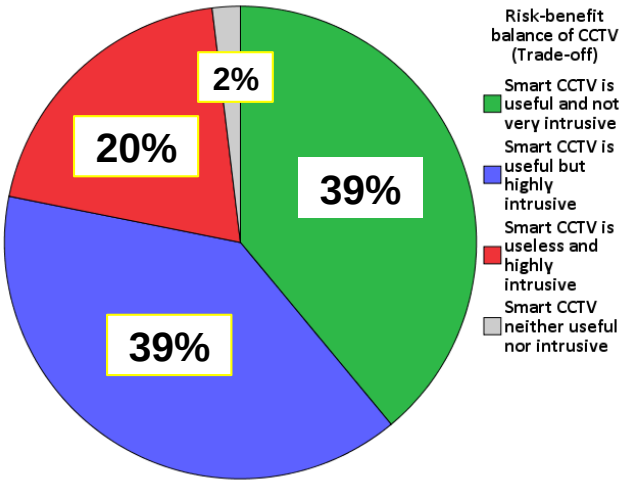
With regards to privacy, **SOSTs which violate one's information privacy (e.g. DPI) are perceived as less acceptable** than SOSTs intruding into one's bodily privacy (e.g. CCTV and SLT). [The internet is misleading perceived as a private space rather than a public space]

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

Q3: Reliance on the Privacy-Security Tradeoff

	Useful	Useless
Highly Intrusive	39,16%	19,95%
Not very intrusive	39,98%	1,92%

Smart CCTV

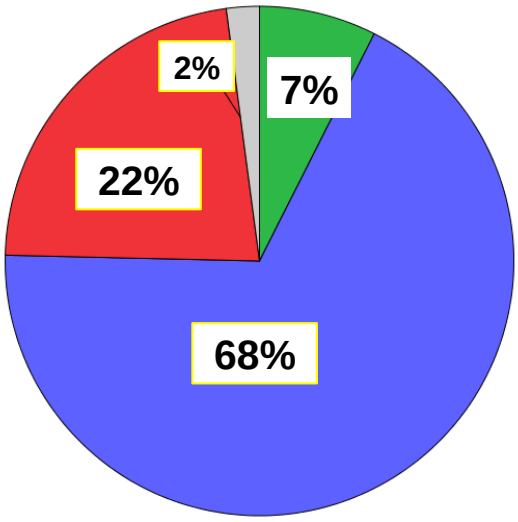


This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

Q3: Reliance on the Privacy-Security Tradeoff

	Useful	Useless
Highly Intrusive	67,91%	22,55%
Not very intrusive	7,45%	2,02%

Deep Packet Inspection (DPI)

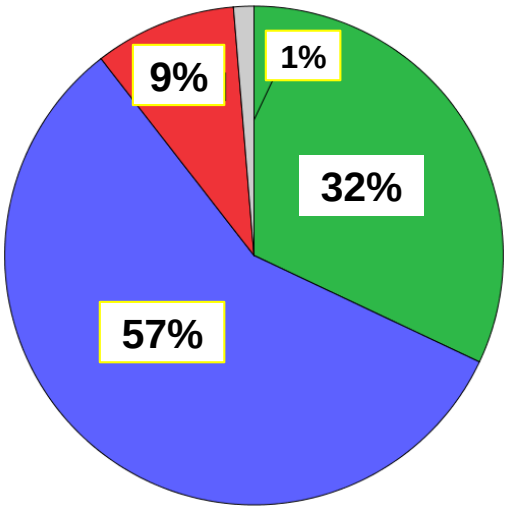


This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

Q3: Reliance on the Privacy-Security Tradeoff

	Useful	Useless
Highly Intrusive	57,46%	9,2%
Not very intrusive	32,02%	1,31%

Smartphone Location Tracking (SLT)



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

Q2: Effect of relying on the tradeoff on the likelihood of considering SOSTs acceptable

- ✓ **Tradeoff**: People who adopt the tradeoff, and see SOSTs as both intrusive and effective, are more likely to accept SOSTs.
- ✓ **Positive View**: People who consider SOSTs as effective and not intrusive are more likely to accept SOSTs.
- ✓ **Negative View**: People who consider SOSTs as intrusive and not effective are less likely to accept SOSTs.
- ✓ **Cultural Effects**: Citizens in German-speaking countries are less likely to accept SOSTs.

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

Distinction between factors and criteria

- **FACTOR**: something that helps produce or influence a result / one of the things that cause something to happen.
  - Factors can be assessed through both quantitative and qualitative methods
- **CRITERION**: something that is used as a reason for making a judgment or decision / a standard on which a judgment or decision may be based.
  - Criteria can only be assessed through qualitative methods.

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

Q3: Criteria under which SOSTs are more likely to be considered acceptable

1) Public regulatory supervisory body/legislation.

Acceptable SOSTs are technologies operating within a clear legal framework and under the control of a EU/International regulatory body.

2) Transparency, information and accountability

Citizens want to be informed and be aware when SOSTs are used, how SOSTs function, for what purpose they have been installed and who is in charge of managing the system.

3) Public/private separation

Acceptable SOSTs are technologies operated only by public authorities for the sake of the public interest. The participation of private actors in security operations should be limited and strictly regulated.

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

Q3: Criteria under which SOSTs are more likely to be considered acceptable

4) Cost-effective

Acceptable SOSTs are technologies who offer good value for money. They should be not only effective but also efficient.

5) Data control

Acceptable SOSTs give people control over their data: the right to access, rectify and delete data must be ensured.

6) Data minimisation

Acceptable SOSTs keep sensitive information to a minimum, and keep only the information strictly necessary for security purposes. They need to avoid collecting data in spaces considered "sensitive" such as private emails or social media.

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

Criteria: qualitative analysis

7) Scope and aims of surveillance

Acceptable SOSTs are technologies that do not operate blanket surveillance. After reasonable evidences are gathered, they address specific targets, in specific times and spaces and for specific purposes. Their priorities may change but they need to do so explicitly.

8) Alternatives

Acceptable SOSTs are technologies that work and operate in combination with non-technological measures and social strategies addressing the social and economic causes of insecurity. SOSTs should complement and not substitute investments in human resources and social policies.

9) Privacy-by-design

Acceptable SOSTs are technologies that always incorporate privacy-by-design protocols and mechanisms.

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

Conclusions

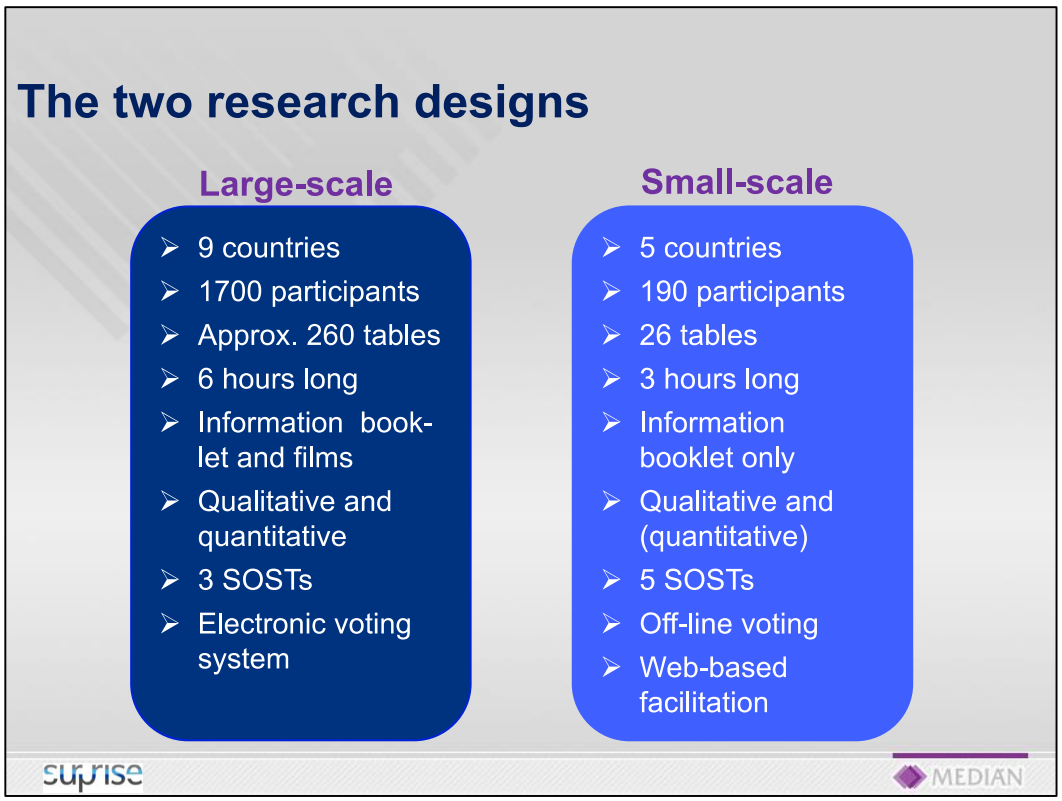
- ✓ Acceptable Security Measures—which embed surveillance functionalities—must demonstrate to be able to **foster public safety both in objective** terms, by reducing crime, **and in subjective terms**, by helping people feeling secure and protected.
- ✓ SOSTs should be targeted and should not be part of blanket surveillance strategies. They should be managed by **trustworthy agents** and should **not** make people feel exposed and embarassed.

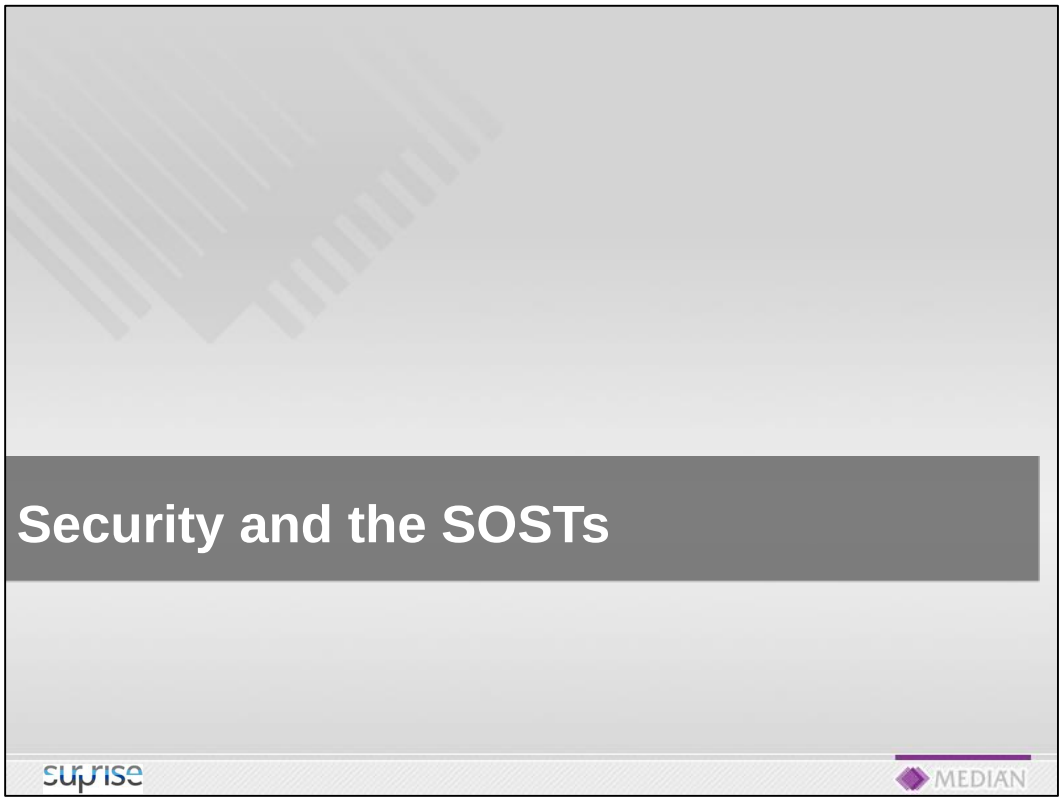
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.

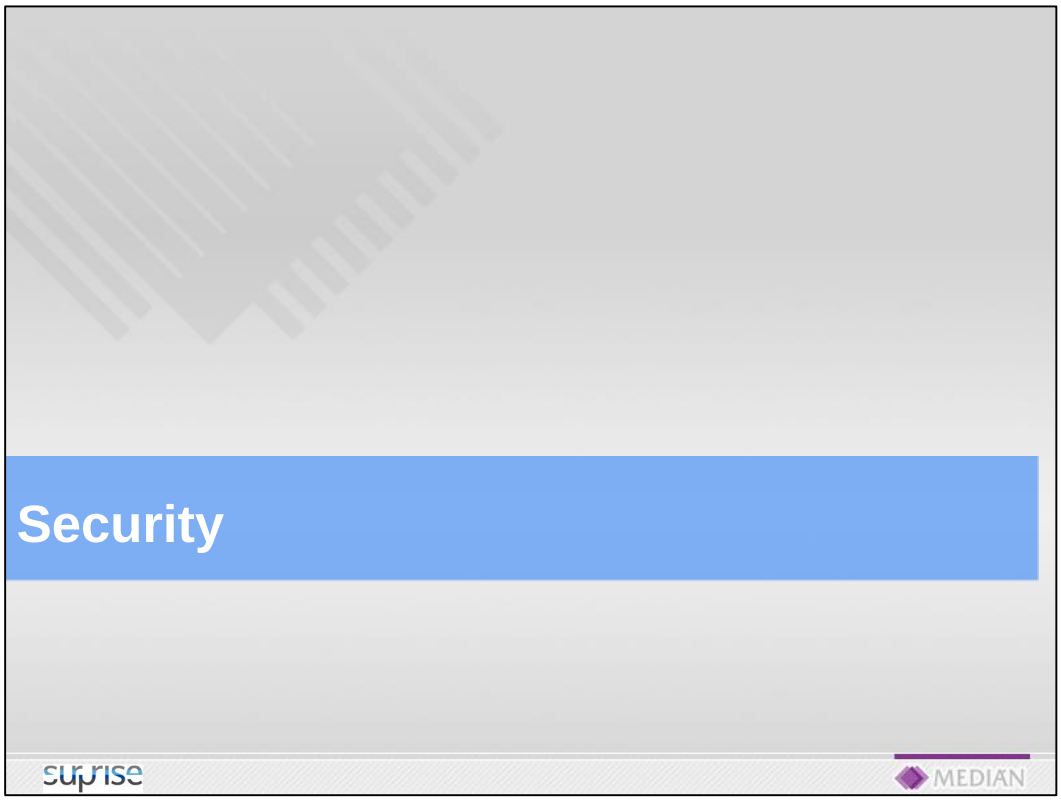
sara.degliesposti@open.ac.uk


THANKS!
surprise
SURPRISE-PROJECT.EU
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 285492.
CRISP
CENTRE FOR RESEARCH INTO INFORMATION, SURVEILLANCE & PRIVACY
The Open University

Results of the 5 citizen meetings




Security and the SOSTs
MEDIAN

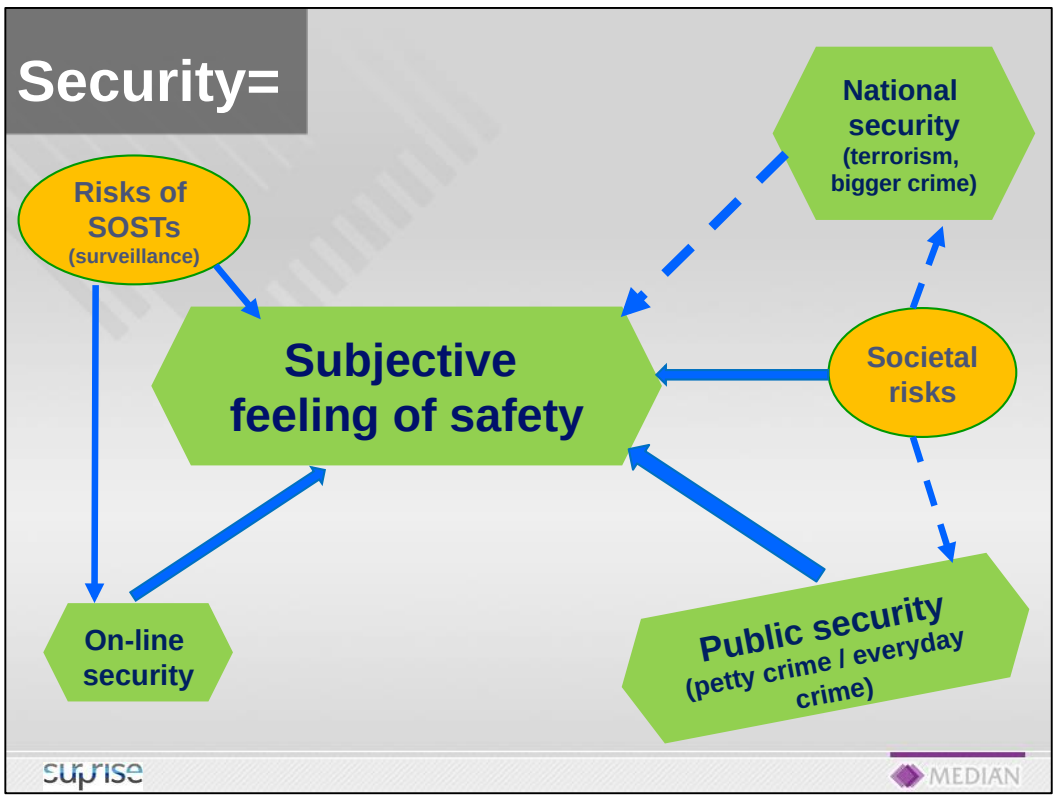

Security
MEDIAN

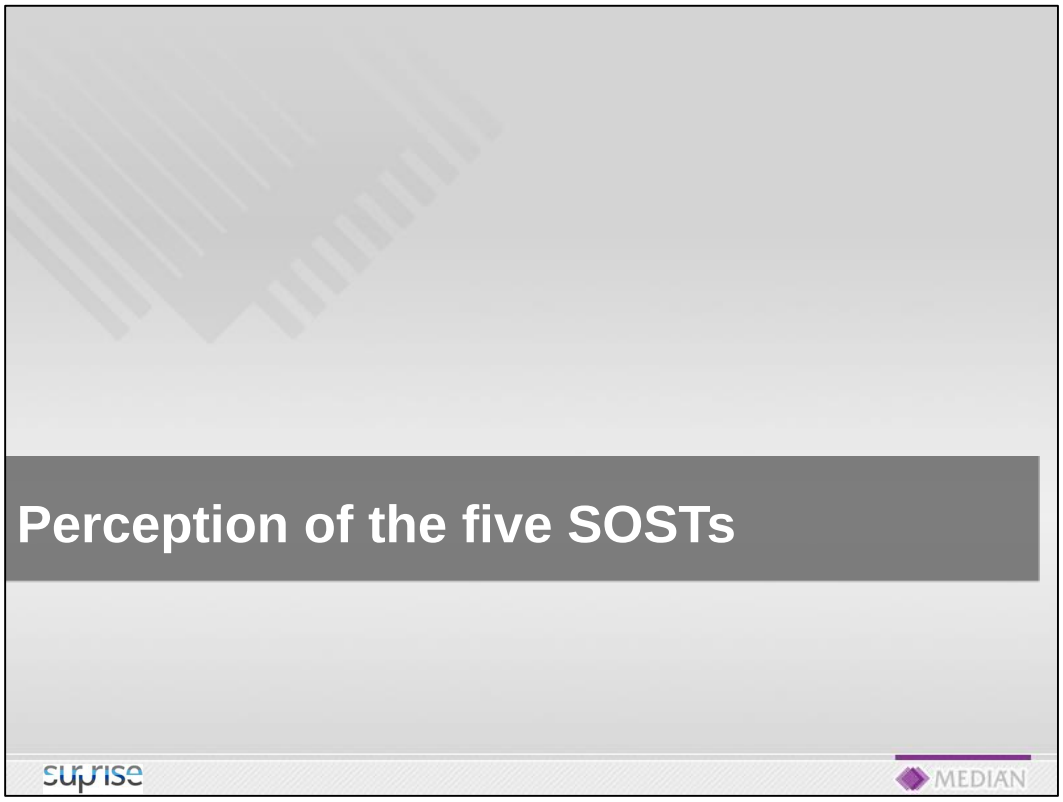
Connection between variables: threat level and acceptability

~~The more that citizens are concerned about threats to their security, the more likely they are to find SOSTs acceptable.~~

But why?

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





Deep packet inspection (DPI)

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


Smartphone location tracking (SLT)
Convenience technology
Useful in investigating or preventing crime only to a limited extent
Improves the sense of personal security
Rather intrusive (danger to democratic freedom, lack of control on the consequences drawn from location data)
Distrust towards the service providers
Trade-off between convenience and privacy
MEDIAN

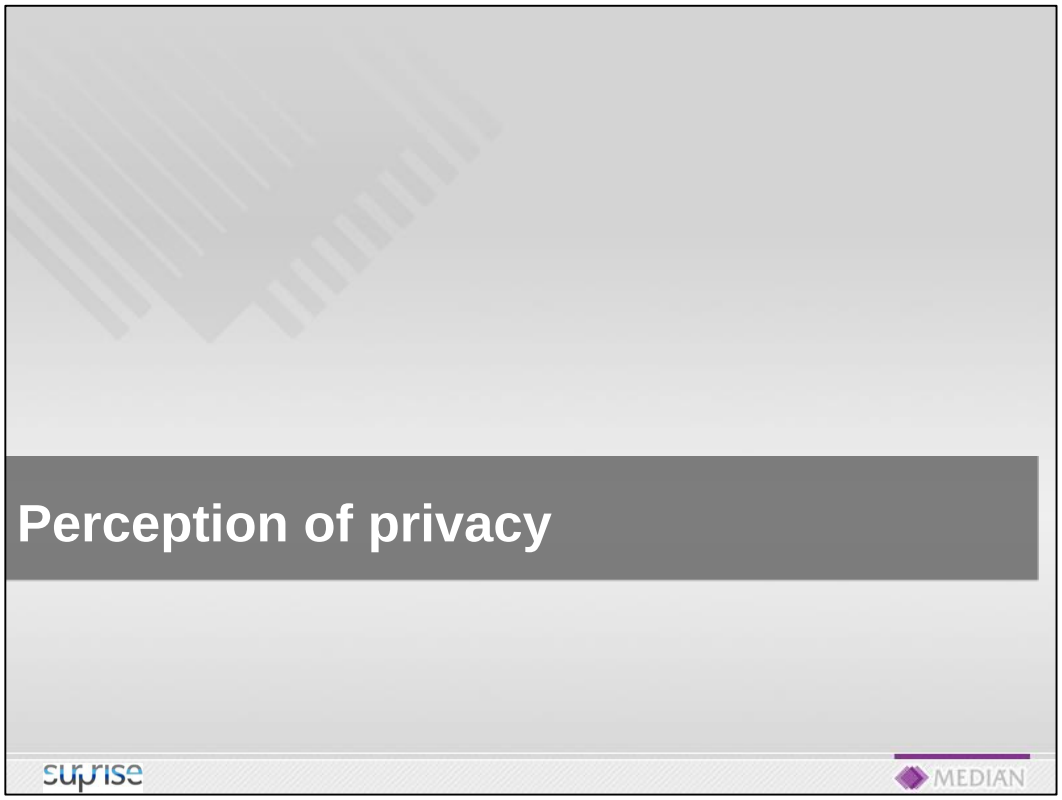

(Smart) CCTV
Smart functions are not known
Preventive with regards to petty crimes
Can help to detect crime retrospectively
Improves public security and the feeling of safety by its deterrent effect
Not very intrusive; it does not target individuals (but smart cameras do)
The most accepted technology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

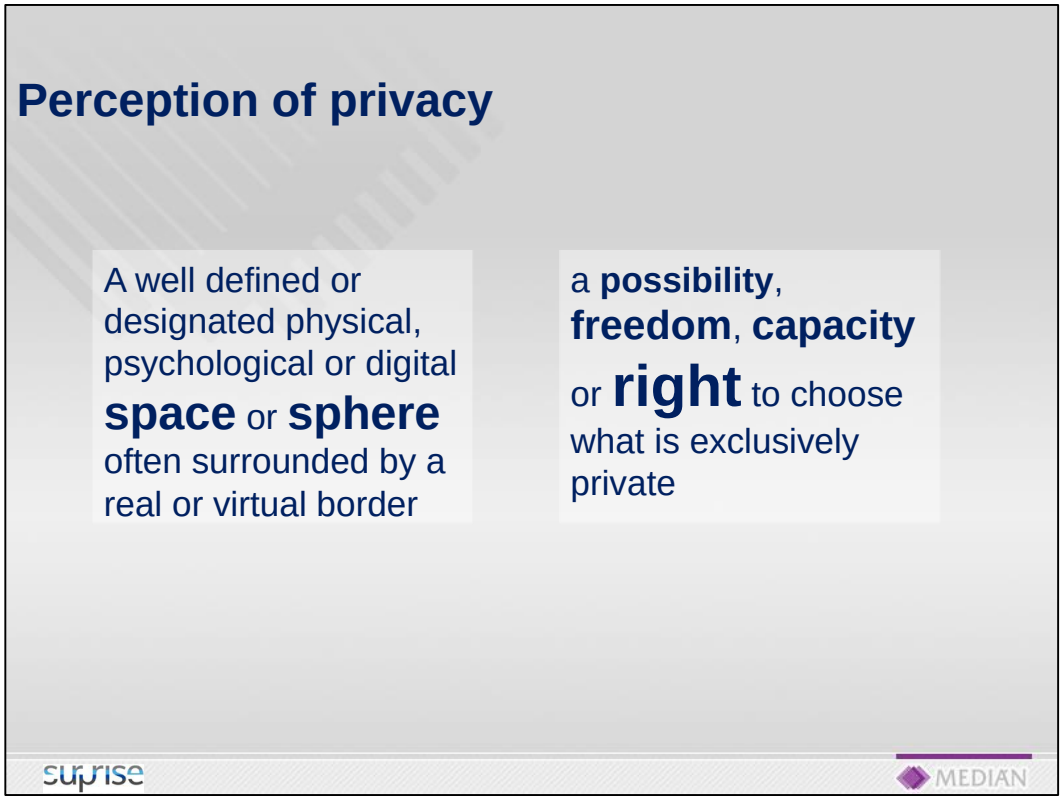
Drones

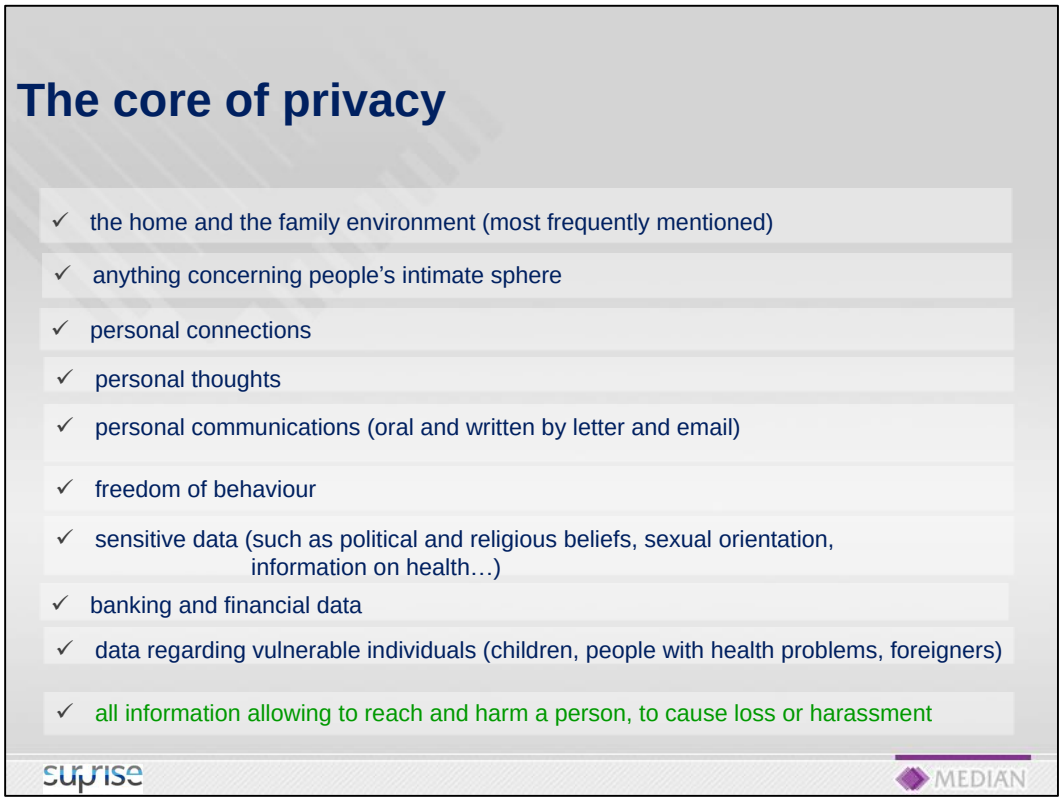
- Not known as SOST
- Modern technology (represents the development)
- The associated military use might generate distrust
- Improves national and personal safety only if it used in specific situations: accidents, disasters, terrorist attacks, fire to provide and overview
  for search and rescue to avoid putting people into hazardous situations
  after a serious crime has been committed (for following criminals)
  in dangerous situations to increase public safety (mass events)
- Very intrusive if used for prevention in generale
- Dangerous technology not only because of surveillance

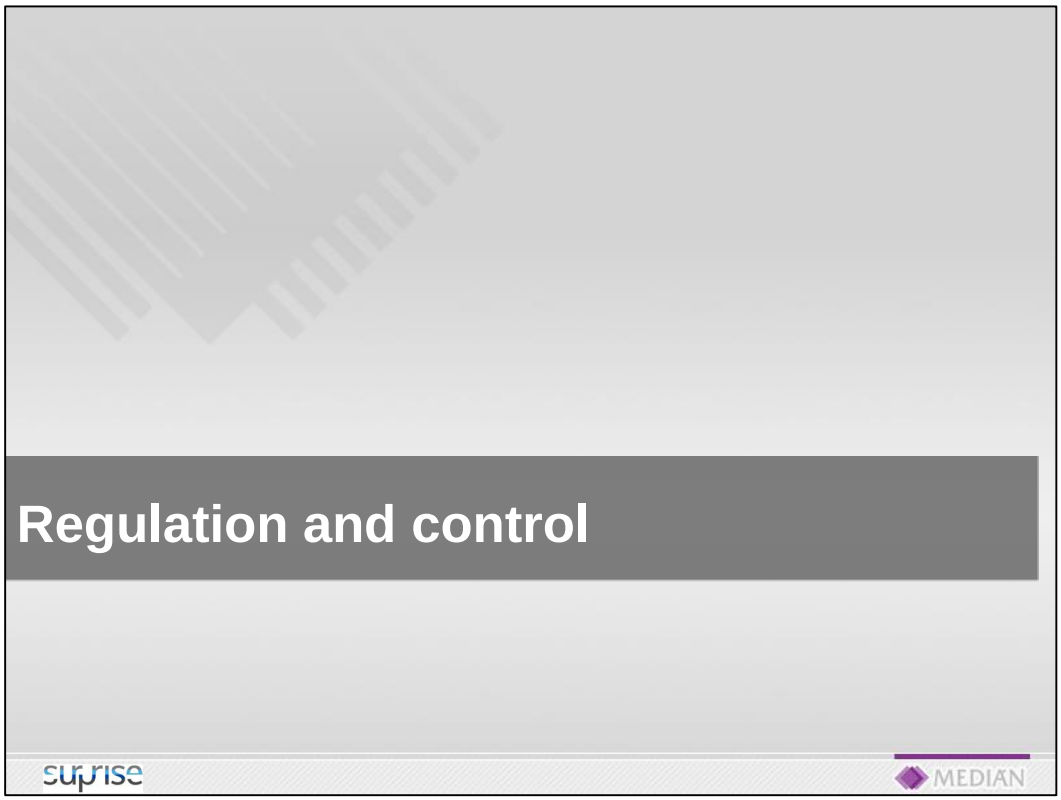
Biometric identification

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


Perception of privacy

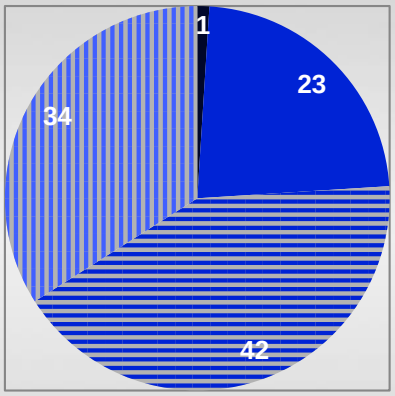

Perception of privacy
A well defined or designated physical, psychological or digital space or sphere often surrounded by a real or virtual border
a possibility, freedom, capacity or right to choose what is exclusively private


The core of privacy
✓ the home and the family environment (most frequently mentioned)
✓ anything concerning people's intimate sphere
✓ personal connections
✓ personal thoughts
✓ personal communications (oral and written by letter and email)
✓ freedom of behaviour
✓ sensitive data (such as political and religious beliefs, sexual orientation, information on health…)
✓ banking and financial data
✓ data regarding vulnerable individuals (children, people with health problems, foreigners)
✓ all information allowing to reach and harm a person, to cause loss or harassment
MEDIAN


Regulation and control
MEDIAN

Knowledge on regulation and control
(percentages; individual rating, N=190)

- very knowledgeable
- know a good amount but would learn more
- have some knowledge
- know little to nothing



Believes

+

A number of citizens maintained positive attitudes, and assumed that even if they were not aware of regulation, it exists

-

A number of citizens stated that the use of SOSTs was not sufficiently regulated, and even if it was, security agencies would not abide by the rules

Expectations towards legal safeguards

The majority of citizens did not demand a direct say in the regulation of SOSTs, leaving this work to professionals, under the condition that the results ought to be communicated to the public in a comprehensible language.

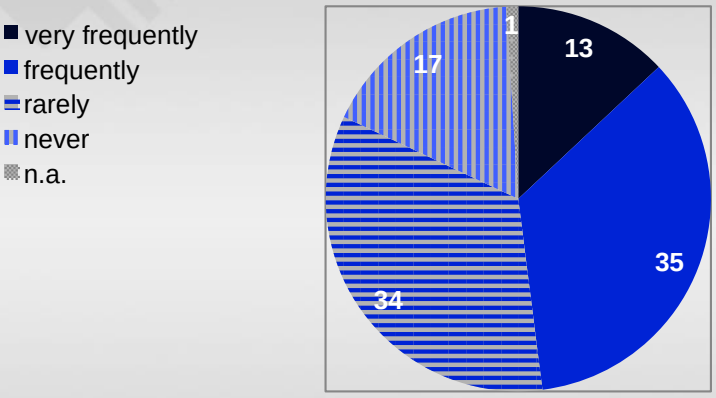
Expectations towards legal safeguards

- ✓ Active, permanent control over security agencies that use SOSTs by a body or organisation, which should be **independent** from politics, industrial and commercial interests as well as from the users of SOSTs, so as to ensure accountability and to avoid unfettered discretion
- ✓ Securing access to an individual's own personal data upon request
- ✓ Judicial authorisation of the access of public security agencies to the collected data
- ✓ The necessity, adequacy and proportionality of each measure should be assessed
- ✓ Citizens should be informed about lawful data collection and processing operations and existing legal safeguards
- ✓ Legal safeguards should also be at hand when private companies use SOSTs
- ✓ safeguards cannot be so bureaucratic as to make it difficult for public security authorities to do their job

Surveillance in everyday life

„How frequently, if at all, do you worry about the use of SOSTs in your daily life?"

(percentages; individual rating, N=190)



Reactions to surveillance in everyday life

Rational thinking: trying to protect privacy as much as it is possible

Accept the „trade-off": *"I have nothing to hide"*
„Only criminals or those who have skeletons in the closet have to worry about surveillance."

Personal data is not interesting to anybody *("We are such little things." "**They** want to observe others not us.")*

Helplessness/vulnerability: *"We are too little to do anything against it."*

Resignation: *"Everybody knows everything."*

Fear: Surveillance is seen as a tool in the hand of the authorities against citizens

Trust and distrust in security agencies

Trust and concerns

Trust in security agencies is often combined with concerns that such agencies will abuse their power

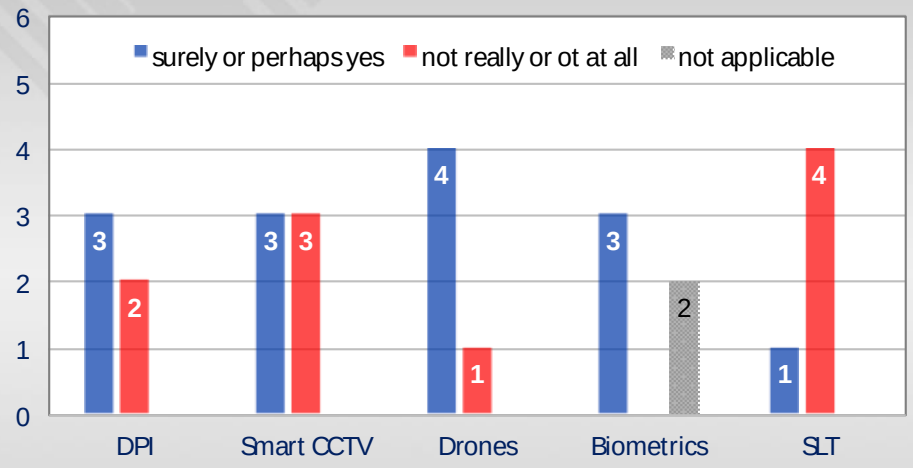
Explanation

Citizens often distinguish between those who direct the whole systems (perceived not in terms of individuals but of authorities) and the field operators

If private actor is involved in the data collection, this might influence the evaluation: Citizens often expressed that they trust in security agencies significantly more than in (profit-led) private companies.

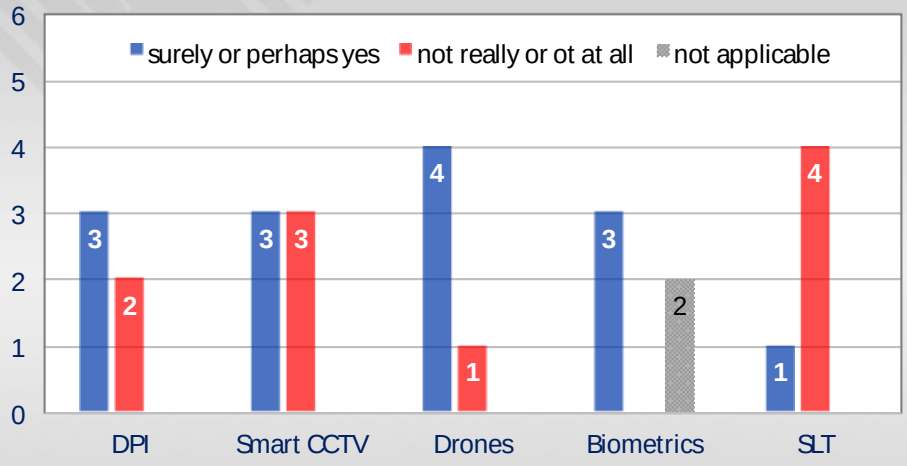
Trust in security agencies

"Do you trust in security agencies who use the given SOST in your country?"
(number of groups selected the answer possibility, 5 groups per SOST but 6 at smart CCTV)



Trust in security agencies

"Do you trust in security agencies who use the given SOST in your country?"
(number of groups selected the answer possibility, 5 groups per SOST but 6 at smart CCTV)



5 Participants

Surname	Name	Affiliation	Country	
Andrew	Jonathan	European University Institute	Italy	SURVEILLE project
Ariu	Davide	University of Cagliari, Pra Lab	Italy	Invited expert
Bådum Bang	Nicklas Bang	The Danish Board of Technology Foundation	Denmark	SurPRISE project
Baeriswyl	Bruno	Data Protection Commissioner of the Canton of Zürich	Switzerland	Invited expert
Barland	Marianne	The Norwegian Board of Technology	Norway	SurPRISE project
Berglez	Regina	Institute for the Sociology of Law and Criminology (Verein für Rechts- und Kriminalsoziologie)	Austria	SurPRISE project
Brouwer	Evelien	Vrije Universiteit Amsterdam	Netherlands	Invited expert
Brugger	Michael	Austrian Ministry for Transport, Innovation and Technology – Technology Transfer and Security Research	Austria	Invited expert
Bütschi	Danielle	TA-SWISS, Centre for Technology Assessment, Swiss Academies of Arts and Sciences	Switzerland	SurPRISE project
Calamari	Marco	HERMES and WinstonSmith.org	Italy	Invited expert
Čas	Johann	Institute of Technology Assessment, Austrian Academy of Sciences	Austria	SurPRISE project
Caselli	Antonio	Italian Data Protection Autority (Garante per la protezione dei dati personali)	Italy	Invited expert
De Concini	Claudia	European University Institute	Italy	SurPRISE project
Degli Esposti	Sara	The Open University	United Kingdom	SurPRISE project
Derkacz	Jan	AGH University of Science and Technology	Poland	Invited expert
Di Giovanni Bezzi	Raffaele	European Commission (DG Connect)	Belgium	Invited expert
Drobek	Piotr	The Bureau of the Inspector General for Personal Data Protection, and Cardinal Stefan Wyszynski University	Poland	Invited expert
Ellerman	Jan	Europol (data protection office)	Netherlands	Invited expert
Ferrari	Elena	Univeristà Insubria, DiSTA STRICT Social Lab	Italy	Invited expert
Filippini	Sara	Italian Forum for Urban Security	Italy	Invited expert
Ghernaouti	Solange	University of Lausanne	Switzerland	Invited expert
Gorissen	Koen	Belgian Data Protection Authority	Belgium	Invited expert

Hayes	Ben	Statewatch	United Kingdom	SurPRISE project advisory panel
Jeanneret	Dilini-Sylvie	TA-SWISS, Centre for Technology Assessment, Swiss Academies of Arts and Sciences	Switzerland	SurPRISE project
Klonk	Jeannette	The Austrian Research Promotion Agency (FFG), NCP Security Research	Austria	Invited expert
Krieger-Lamina	Jaro	Institute of Technology Assessment, Austrian Academy of Sciences	Austria	SurPRISE project
Krisch	Andreas	European Digital Rights (EDRi)	Austria	Invited expert
Majtényi	László	University of Miskolc	Hungary	SurPRISE project advisory panel
Martin	Scheinin	European University Institute	Italy	SurPRISE project
Miller	Elaine	European Commission (DG Justice)	Belgium	Invited expert
Orwell	James	Kingston University	United Kingdom	Invited expert
Pavone	Vincenzo	Spanish National Research Council (Agencia Estatal Consejo Superior de Investigaciones Científicas)	Spain	SurPRISE project
Peissl	Walter	Institute of Technology Assessment, Austrian Academy of Sciences	Austria	SurPRISE project
Porcedda	Maria Grazia	European University Institute	Italy	SurPRISE project
Robles Tardio	Luisa	Madrid Municipal Police	Spain	Invited expert
Rone	Julia	European University Institute	Italy	Invited expert
Russo	Stefano	ItalDron	Italy	Invited expert
Santiago	Elvira	Spanish National Research Council (Agencia Estatal Consejo Superior de Investigaciones Científicas)	Spain	SurPRISE project
Schlehahn	Eva	Unabhängiges Landeszentrum für Datenschutz	Germany	SurPRISE project
Semler	Christian	Federal Ministry of Interior	Austria	Invited expert
Skjødt Nielsen	Jacob	The Danish Board of Technology Foundation	Denmark	SurPRISE project
Snijder	Max	EU Biometrics Group	Netherlands	Invited expert
Sperber	Sebastian	European Forum for Urban Security	France	Invited expert
Strauss	Stefan	Institute of Technology Assessment, Austrian Academy of Sciences	Austria	SurPRISE project
Szénay	Márta	Median Opinion and Market Research Limited Company	Hungary	SurPRISE project
Tallacchini	Mariachiara	European Commission (DG Joint Research Centre Institute for the Protection and Security of the Citizen)	Italy	Invited expert
Tranø	Nina	One Voice AS	Norway	SurPRISE project advisory panel

Vermeulen	Mathias	Vrije Universiteit Brussel – LSTS centre	Belgium	SurPRISE project
Zinner	Hannah	Institute of Technology Assessment, Austrian Academy of Sciences	Austria	SurPRISE project