

surprise

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

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

Citizens’ Perspectives on Surveillance, Security and Privacy: Controversies, Alternatives and Solutions
13th November 2014, Vienna

SurPRISE - Surveillance, Privacy and Security

surprise

Institut für Technikfolgen-Abschätzung / Österreichische Akademie der Wissenschaften Coordinator, Austria	
Agencia de Protección de Datos de la Comunidad de Madrid, Spain	
Instituto de Políticas y Bienes Públicos / Agencia Estatal Consejo Superior de Investigaciones Científicas, Spain	
Teknologirådet - The Danish Board of Technology Foundation, Denmark	
European University Institute, Italy	
Veren für Rechts- und Kriminalsoziologie, Austria	
Median Opinion and Market Research Limited Company, Hungary	
Teknologirådet - The Norwegian Board of Technology, Norway	
The Open University, United Kingdom	
TA-SWISS / Akademie der Wissenschaften Schweiz, Switzerland	
Utdatnings- og Datatilsynet, Germany	

- **FP7 Security Research**
- **Coordinated by ITA,**
- **11 partners from nine countries**
- **Duration 36 months, start February 2012**

Objectives

- **To explore the trade-off concept**
- **To contribute to security technologies/policies that respects human rights and European values**
- **Provide decision support for security investments, taking into account a wider societal context.**



Two empirical research designs

Citizen Summits

- 9 countries
- 1700 participants
- Approx. 260 tables
- 6-7 hours long
- Information booklet and films
- Qualitative and quantitative data
- 3 SOSTs
- Electronic voting
- Recommendations

Citizen Meetings

- 5 countries
- 190 participants
- 26 tables
- 3 hours long
- Information booklet only
- Qualitative and (quantitative)
- 5 SOSTs
- Off-line voting
- Web-based facilitation
- Recommendations

Distinction between factors and criteria

- **Factors:** 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
- **Criteria:** 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.

/

Criteria adopted by participants to decide on acceptability

1) Public regulatory supervisory body/legislation

SOSTs are more acceptable when operating within a clear legal framework and under the control of a EU/International regulatory body complementing and transcending national frameworks and national authorities.

2) Transparency, information and accountability

SOSTs are more acceptable if implemented in a context where information is provided to citizens on: a) where SOSTs are used, b) how SOSTs function, c) for what purpose they have been installed and d) who is in charge of managing the system.

3) Public/private separation

SOSTs are more acceptable when operated only by public authorities and for the sake of the public interest. The participation of private actors in security operations makes SOSTs less acceptable.

Criteria adopted by participants to decide on acceptability

4) Cost-effectiveness

SOSTs are more acceptable when if they offer good value for money. They should be not only effective but also efficient.

5) Data control

SOSTs are more acceptable if they give people control over their data: the right to access, rectify and delete data must be ensured.

6) Data minimization

SOSTs are more acceptable if they keep sensitive data gathering to the minimum, and keep only the information strictly necessary for security purposes. They are more acceptable if they avoid collecting data in spaces considered "sensitive" such as home, private emails or social media.

Criteria adopted by participants to decide on acceptability

7) Scope and aims of surveillance

SOSTs are more acceptable if they do not operate blanket surveillance, address specific targets, in specific times and spaces and for specific purposes and, when their priorities change, they do so explicitly.

8) Alternatives

SOSTs are more acceptable if they work and operate in combination with non-technological measures and social strategies addressing the social and economic causes of insecurity. SOSTs are more acceptable if they complement and not substitute investments in human resources and social policies.

9) Privacy-by-design

SOSTs are more acceptable if they incorporate and maintain over time privacy-by-design protocols, procedures and mechanisms.

Résumé

- **Results**
 - **New and better understanding**
 - **Recommendations**
 - **Model of involving citizens into decision making**
- **Limits**
 - **Necessary conditions**
 - **Narrow setting**

Thank you!



Name of the lecturer – name of institution
Email of the lecturer

