"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 6.13 – Policy paper and manual

Lead Beneficiary: ITA/OEAW

Editor: Johann Čas (ITA/OEAW)

Author(s): SurPRISE Consortium

Due Date: January 2015

Submission Date: February 2015

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
2 The evolution of the recommendations 2
2.1 Citizen participation in SurPRISE 3
2.1.1 The Citizen Summits 3
2.1.2 The Small-Scale Citizen Meetings 4
2.2 The Expert Workshop 5
3 The SurPRISE Recommendations 6
3.1 The legal framework on data processing must meet the challenges of technological advances 7
3.2 Enforcing data protection in Europe 8
3.3 Protect personal data in transit, notably on the Internet 8
3.4 Strengthen agencies providing supervision, guidance and control 10
3.5 Implement proper safeguards 11
3.6 Limit the scope of data collection 12
3.7 Increase accountability and prevent abuse 13
3.8 Regulate and limit the role of private and non-governmental actors in the provision of public and national security 14
3.9 Establish a privacy-orientated competitive market 15
3.10 Implement and improve transparency 16
3.11 Improve training and education of security authorities 17
3.12 Raise awareness on security and privacy 18
3.13 Foster participation in decision making 18
3.14 Establish technology assessment and on-going evaluation 19
3.15 Request mandatory Privacy by Design and Privacy by Default 20
3.16 Focus on root causes of insecurity 21
4 Criteria and factors determining the acceptability of security technologies 22
5 Manual: How to engage citizens 26
5.1 The participatory methodology and the SurPRISE DSS 26
5.1.1 The voice of the citizens 26
5.1.2 The engine of the discussion 26
5.1.3 Possibilities for future use 27
5.2 SurPRISE DSS within the participatory methodology and the decision making 28
5.3 Checklist of items and steps required to involve citizens 29
5.4 Discussions during the citizen consultations 30
5.5 Analysis 31
5.6 How to start one´s own project 31
6 Conclusions 31
7 List of Figures 34

8 List of Tables 35
9 List of Abbreviations 36

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', and 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 was organised in eight[1] technical work packages. WP1 supported research activities by developing and establishing common project methodologies. WP2 developed a theoretical framing of criteria and factors influencing the acceptance and acceptability of security technologies, which was evaluated and tested in the empirical work done later in the project. Following this theoretical framing, WP3 identified and elaborated on options to shape security measures, to comply with ethical and privacy requirements from a technical, legal and social perspective. Combining the results of WP2 and WP3, WP4 developed an empirical model, which was applied and tested in large-scale participatory activities. WP4 also provided supporting material for the involvement of citizens, including comprehensive information brochures to allow for informed debates and video clips to present a range of conflicting opinions from experts. WP5 organised and conducted large-scale participatory technology assessment events in nine European countries. These "Citizen Summits" involved on average about 200 citizens per country. These citizen summits were full day events, with alternating phases wherein participants received information, discussed the topics and emerging issues in small groups of six to eight persons and voted electronically as individuals on general aspects of the relation between surveillance and security and on specific surveillance technologies. As concluding activity each of the small groups of citizens was asked to develop and formulate recommendations to policymakers. In WP6, the qualitative and quantitative data from the citizen summits were analysed in depth, and synthesised to form conclusions and develop recommendations, combining expert knowledge and citizens perspectives. The methodological approach and results from the citizen summits were also used in WP7 to develop a decision support system, allowing the involvement of citizens in decision-making on security measures and technologies in small-scale participatory events. This approach, called "Citizen Meetings", was also tested in five countries and the results were integrated into the analytical work and the development of policy recommendations.

[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

The objectives of this paper are to present recommendations for security measures and technologies that respect human rights and European values, to summarise the main factors and criteria influencing the acceptability of surveillance oriented security technologies (SOSTs) and to outline how to involve citizens in future decision making on security measures, based on methods developed and tested within the SurPRISE project.

The 16 recommendations described in this document are a key output of the SurPRISE project. They synthesize the results from scientific research, the recommendations elaborated by about 2000 participants of the Citizen Summits and the Citizen Meetings, the large scale and small-scale participatory events conducted in nine and five European countries respectively, and external experts' opinions. The multitude of factors and criteria taken into account by the citizen when evaluating SOSTs clearly demonstrates that the regular trade-off approach between privacy and security by far oversimplifies empirical reality and should therefore be abandoned in decision-making. The involvement of citizens in the decision making process is, as demonstrated, a feasible and effective way to develop more effective and sustainable solutions, in line with fundamental rights.

One of the core objectives of SurPRISE was to put into question the trade-off approach between privacy and security which largely dominates security policy-making and the development and implementation of surveillance orientated security technologies. SurPRISE challenged this approach from different perspectives: from a theoretical one, which was subsequently empirically tested in large-scale participatory events; from a practical one, investigating technical, regulatory and societal options to eliminate privacy and human rights infringements caused by surveillance technologies; and with a participatory approach, involving 2000 European citizens in the discourse of these issues in informed debates and asking them to develop their own suggestions and recommendations on how to maintain or increase security.

The broad base of stakeholders involved in the process of developing the recommendations as well as the holistic approach, integrating different views and tackling a number of issues regarding security, privacy and surveillance, make them specifically important and relevant for policy-making in general and for all groups involved in the development, production, implementation and use of security technologies. The recommendations are not confined to surveillance technologies as such. On the contrary, they also embrace data protection regulations at large, issues of accountability, transparency, information and education, which are of key importance for law enforcement in particular and governments in general. Additionally, they address the importance of open public debates and the involvement of citizens and civic society organisations in decision making about the implementation and use of surveillance orientated security technologies, and last but not least, the urgent need to tackle root causes of insecurities and finding long-term solutions to pressing economic and societal problems in Europe.

An open and broad search for solutions to security threats, grounded on the defence of democratic values and strict compliance with fundamental rights, will be especially important with regard to new terrorism threats which aim to create fear and eliminate freedoms, like the attacks in Paris in January 2015.[2]

Chapter 2 of this paper provides an overview of the background of the project and of the genesis of the recommendations by describing the sequence of steps involved in the formulation of the presented set of recommendations. The third chapter contains the individual recommendations and contextual information. The fourth chapter summarises our empirical research on factors and criteria relevant for the acceptance and acceptability of SOSTs. The fifth chapter provides a manual for the involvement of citizens in security related decision-making, describing the participatory approach developed and applied by the SurPRISE project.

[2] On the morning of 7 January 2015 two Islamist terrorists forced their way into the offices of the French satirical weekly newspaper Charlie Hebdo in Paris. They killed 12 people and injured 11 others. After the Charlie Hebdo shooting, a further 5 were killed and 11 wounded in several related shootings that followed in the Île-de-France region, where a third Islamist terrorist was also involved. (http://en.wikipedia.org/wiki/Charlie_Hebdo_shooting)

The following figure sketches the main steps undertaken to derive the results presented here, indicating the main parties responsible for the outcome of each task, the SurPRISE project team, external experts and stakeholders and citizens participating in the summits and meetings organised by the project.

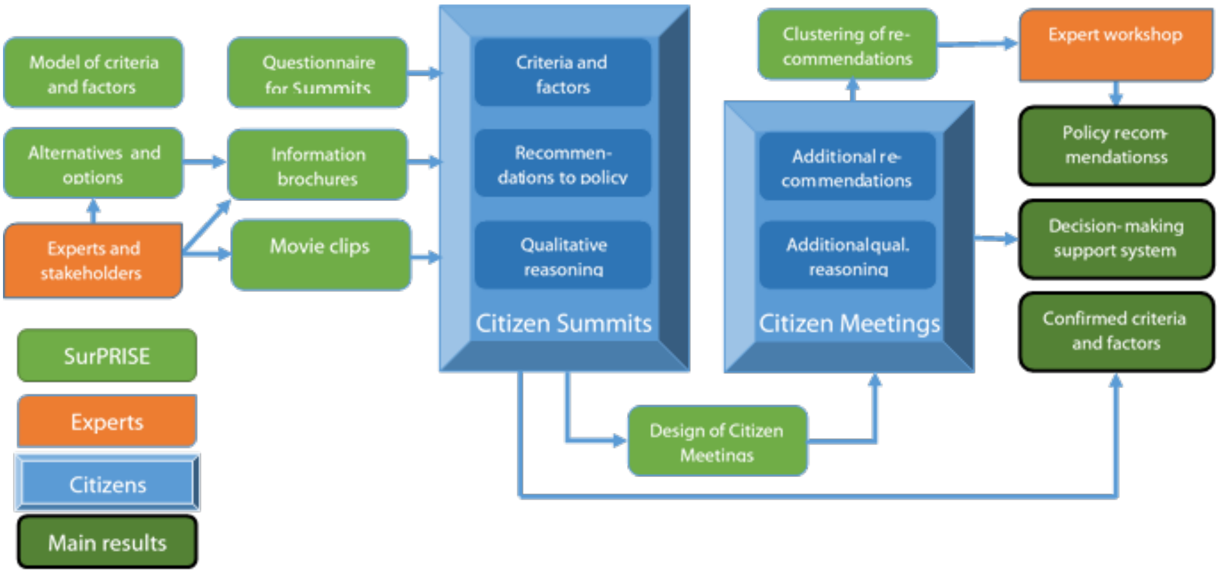
Model of criteria and factors
Questionnaire for Summits
Alternatives and options
Information brochures
Experts and stakeholders
Movie clips
Criteria and factors
Recommen-dations to policy
Qualitative reasoning
Citizen Summits
Clustering of re-commendations
Additional re-commendations
Additional qual. reasoning
Citizen Meetings
Expert workshop
Policy recom-mendationss
Decision-making support system
Confirmed criteria and factors
Design of Citizen Meetings
SurPRISE
Experts
Citizens
Main results

Figure 1: Overview of tasks and responsibilities

The main focus in this report is on the SurPRISE project results that have specific relevance for policymakers and further stakeholders involved in decision-making in security matters. Please refer to the respective reports[3] for detailed descriptions of the constitutive and analytical work.

[3] D2.2 and D2.3 describe the theoretical framework for the analyses of criteria and factors, D2.4 incorporates the analyses of the data gained in SurPRISE empirical research into the theoretical framing. D3.1 and D3.2 describe technical and regulatory options to achieve fundamental rights compliant security technologies, D3.3 investigates non-technical alternatives, D3.4 provides a synthesis of these results. D4.3 outlines the information brochures and movie clips developed for the citizen summits; the information material used during the citizen summits and citizen meetings is available in all used languages from the project homepage. D6.1 to D6.9 represent the results of the individual national Citizen Summits and D6.10 synthesises the country reports. D7.1 describes the individual Citizen Meetings and its results and D7.2 provides a comparative analyses of the small-scale events. All SurPRISE deliverables mentioned in this report are available on the SurPRISE homepage: http://www.surprise-project.eu.

2 The evolution of the recommendations

2.1 Citizen participation in SurPRISE

The increasing role and use of surveillance-orientated 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 and across Europe, their views and opinions on these issues are widely unknown. To narrow this gap, the SurPRISE project gave about 2000 residents of nine European countries the unique opportunity to express and discuss their perceptions regarding security technologies and their implications at twelve citizen summits. These summits were organised in nine different countries in the first half of 2014 (in alphabetical order): Austria, Denmark, Germany, Hungary, Italy, Norway, Spain, Switzerland and the United Kingdom.[4] The events were full-day public meetings where citizens gathered to have face-to-face discussions about surveillance-orientated security technologies. In addition to the citizen summits, in five countries[5] "Small-Scale Citizen Meetings" were arranged in the summer of 2014 with a total of about 200 participants.

2.1.1 The Citizen Summits

The SurPRISE Citizen Summit-method is an innovative technology assessment exercise that gathers both qualitative and quantitative data on the basis of a precise and thorough research design. This method ensures that participants[6] not only have a chance to express preferences among a set of predetermined options, they also have an opportunity to voice their own views, ideas, knowledge and proposals during table discussion rounds. The SurPRISE citizen summits provided two types of outcome: (1) a deep scientific understanding[7] of the rationale behind rejection or acceptance of SOSTs; and (2) recommendations for policy makers and stakeholders involved in decisions on, and the provision of, security related services and technologies, by providing guidance on how to increase the appropriateness and effectiveness of security measures embedded in complex social realities while respecting fundamental rights.

The summits featured the analysis of three different SOSTs (Smart CCTV, Deep Packet Inspection - DPI, and Smartphone Location Tracking - SLT). The use of specific 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 an approach which combined quantitative and qualitative elements. Sets of pre-defined questions and statements clustered around different topics were complemented by discussion rounds relating to each thematic block. Chapter 3 - The SurPRISE Recommendations represents the main results from the qualitative research, whereas chapter 4 - Criteria and factors determining the acceptability of security technologies is predominantly based on quantitative data analysis.

Participants were seated at tables in groups of six to eight individuals, and each table discussion was facilitated by a moderator. The summits comprised alternating quantitative and qualitative phases. The surveys were linked to an electronic polling system that allowed participants to immediately answer the questions via keypads, and the results were presented for each individual question right after the polling. Prior to attending the summit, participants received an information brochure. At the event, before the discussion of individual SOSTs, movie clips were presented to the audience. The clips

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

[5] Denmark, Hungary, Italy, Norway and Spain

[6] The recruitment for the SurPRISE Citizen Summits aimed at getting groups of citizens respectively residents who are, on the one hand, not professionals in the area of surveillance, privacy and security, and that, on the other hand, reflect the national demographics regarding age, gender, geographical zone (rural, urban and metropolitan), educational level, occupation and minorities.

[7] See D2.4 for a comprehensive presentation of theoretical background, applied methodology and achieved results.

provided additional information to that contained in the brochures, and were designed to stimulate recall and discussion. SurPRISE produced a short film of about seven minutes duration on each of the debated SOSTs. Experts from different backgrounds were interviewed and asked to briefly describe the technology, to provide their assessments of the pros and cons, and to address open questions in relation to the corresponding SOST. The mix of written information (the brochure) and more thought-provoking visual information (the film clips) helped equalize participants' knowledge, thus facilitating discussions on relatively equal footing.

At each table, a moderator facilitated the discussion rounds and supported participants if necessary, e.g., in case of general requests. At some tables, note takers were also present, who documented questions raised and lines of argumentation, to expand and amend the qualitative data collected at these events. In preparation for the summit, table moderators and note takers received guidelines about the process design, and were trained to perform their tasks. In total, three discussion rounds were conducted per summit. One round was devoted to each of the two SOSTs allocated to the different countries, focussing on the perceived benefits and risks in relation to the particular form of surveillance and with the objective of gaining more insights into the participant's views and reasoning. The purpose of the third and final discussion round served for participants to develop suggestions and recommendations targeted at policy makers at the national as well as the European level.

2.1.2 The Small-Scale Citizen Meetings

The main objectives of the deliberative research undertaken at the small-scale citizen meetings were to supplement the results of the large-scale citizen summits and to test the SurPRISE Decision Support System[8] (DSS). At the Citizen Meetings the societal context of two more SOSTs and further factors and criteria influencing trust and citizens' concerns about security challenges were investigated.

These small-scale citizen meetings were organised in Denmark, Hungary, Italy, Norway and Spain involving about 35-40 participants per country. Besides the three technologies of Deep Packet Inspection (DPI), Smart CCTV and Smartphone Location Tracking that were also discussed during the large-scale citizen summits, two additional technologies were included in the assessment process: drones and biometrics.

The informed discussion was supported by a new information brochure for the participants, which was a re-edited, adapted and updated version of the one used during the large-scale events, and supplemented with new chapters on Drones and Biometrics as well as on further alternative (non-technical) solutions.

The 3-hour Citizen Meetings were preceded by a short introductory plenary session and consisted of two discussion rounds conducted in small groups:

- The first session tried to gain a deeper insight on how citizens feel about security, surveillance itself, and the surveillance-based security technologies. Additionally, perspectives of participants on privacy and data protection as well as on regulation and control connected to the use of these surveillance-based technologies were addressed and discussed. This discussion round was completed using the SurPRISE decision support web-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. Citizens were asked 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.

During the group work at the tables, open discussions alternated with individual or group voting to answer a questionnaire. At the end of the meeting, participants as well as moderators assessed the event using a self-administered questionnaire.

[8] See D7.3 for a description of the Decision Support System tool developed by SurPRISE.

2.2 The Expert Workshop

Based on citizens' experiences and opinions expressed in the different participatory events, and on the approximately 300 recommendations collected at the Citizen Summits and Meetings, an initial set of 20 recommendations was developed by the project team. This process comprised the clustering of recommendations in order to eliminate repetitions and to reduce overlapping requests, re-formulations, allowing for the mutual enhancement of scholarship's theoretical findings with participants' views, and, if required, also transformations of contents to better reflect the demands of the participants.

In the expert workshop, this set of recommendations was presented to and discussed with a diverse group of experts and stakeholders. The invited experts comprised policy makers, representatives from the security industry, technology developers and suppliers, the European Commission, national security research programmes, law enforcement agencies, data protection authorities, governments/ministries as well as civil society organisations.

The stakeholder workshop served the main purpose of getting additional input and gaining new perspectives and expert perceptions on the recommendations derived from participatory events.

The workshop consisted of four phases: As preparation a brief background information sheet was sent to the participating experts a few days before the event. The workshop itself started with presentations given by members of the SurPRISE consortium providing some insights into the preliminary results from the project; it continued with feedback from the invited experts and a roundtable discussion on the results from the participatory events; the main part of the stakeholder workshop was dedicated to moderated table discussions with the experts. In order to establish a conducive climate for discussions with different perspectives, each table consisted of experts and stakeholders from different fields.

Four draft recommendations, representing major issues of concern for the participating citizens, were discussed at each of these tables. The topics were mixed, ranging from legal, technical and organisational to political and economic issues in the privacy-security context. The recommendations also differed in their level of concreteness. At the workshop, each table was facilitated by members of the SurPRISE consortium: one acting as moderator, the other as a note taker. The resulting notes were directly integrated into a Web-based tool developed by the project. In the next step, the main discussion points raised by the experts were presented via this tool by the note takers to the plenary audience, for a short discussion to gather the most important issues. During the lively discussions, the experts brought in several additional perspectives on applying and implementing the recommendations. Therefore the workshop provided important input for improving the final set of recommendations.

3 The SurPRISE Recommendations

As described in the previous sections, the generation of the recommendations is based on several steps, involving a very large number of individuals with varied backgrounds. An essential contribution came from citizens participating in the Citizen Summits and Meetings. About 300 recommendations were developed by approximately 2000 residents from nine different European countries. These recommendations were integrated in and enriched by academic research and expertise within and external to SurPRISE. They were transformed in various ways to become the output presented here in a more coherent form. In the following, it will be explained why and in which way this transformation was conducted.

The information brochures and the introductory movie clips, providing unbiased information and divergent expert opinions on the SOSTs discussed, influenced to some extent the discussions among citizens. These inputs provided factual and technical knowledge, and conflicting views on important issues involved and combined theoretical work done within SurPRISE with knowledge and opinions of external experts.

The participating citizens partially responded or referred to this material to formulate a great number of opinions and recommendations. While the ample feedback was appreciated and very valuable, the recommendations contained many similar or overlapping requests. Therefore, the numerous and detailed recommendations of the citizens required summarisation and reformulation to enable a comprehensive, yet easy to grasp report on their key aspects. In some cases an additional effort was made to reformulate the citizens' recommendations into "policy-oriented" language. The SurPRISE project team tried its best to keep the original spirit of the requests made by citizens. This implied, however, in a few cases apart from reformulation, also a refocusing or re-aligning specific requests. For example, participants frequently wanted to establish an institution responsible for the protection of data and privacy, but such an institution already existed in all participating countries in form of data protection supervisory authorities. Nevertheless, many participants felt helpless and unsupported regarding protection of the privacy, as they were not aware about existing legislation and responsible authorities. Therefore, these requests were transformed and combined with requests for more information about and better enforcement of existing regulations.

Participants of the expert workshop and members of the SurPRISE advisory panel advised rephrasing some general recommendations to be more specific, to take on a more operational and directly implementable form. Where appropriate, we included suggestions regarding the implementation and provided additional information on the policy initiatives concerned.

SurPRISE, with all its diverse expertise on board, has done its best to fulfil these partly conflicting demands and to integrate the citizens' views when formulating its recommendations. In this context, we would like to thank the members of our advisory panel and the external experts for their advice and feedback. Specifically, we acknowledge the essential contributions of about 2000 European citizens, but take full responsibility for this set of recommendations.

There were also several contributions from participants asking for a reconsideration of security by broadening the perspective and putting security problems in relation to more general issues of social justice, integration and equality. The last recommendation in this set "Focus on root causes of insecurity" addresses these concerns, going beyond traditional perceptions of security and security technologies.

The following comprehensive recommendations are presented by describing the recommended action, followed by its factual, legal, political and social background, providing a more detailed view on what's the problem and where this recommendation comes from. Background details include specific means to address a recommendation, who should be involved, possible first steps, how it fits into the status quo, what has to be changed, why is the topic important, what are possible solutions etc. Where applicable, links to current policy initiatives at the European level are added, describing debates, current legislative or policy initiatives in Europe for which our recommendations are relevant.

3.1 The legal framework on data processing must meet the challenges of technological advances

The current data protection legal framework needs to be adapted and modernised to meet the specific challenges of the most recent tools and techniques of (big) data processing performing data crawling, matching, linkage and analysis functions. In particular, the impending major reform of the EU-level data protection legal framework should set rules that explicitly target the functions (or effects) of such tools in the course of private and public activities including law enforcement, to preserve protection levels independently from technological progress.

These rules should be specified and operationalised in form of technical annexes. The annexes should be regularly updated and, if required, be extended to allow the law to keep in line also with future technological advancements.

Background

Technological advances of the new millennium have paved the way to efficient and cheap tools for scraping, matching, linking and analysing a huge trove of data – so-called Big Data. Positive developments include the possibility of processing of anonymous data for public policy and science.

Yet, the Big Data wave is driven by profit-led processing of personal data, and by governmental inquiries into the data stocks held by companies. Law enforcement reaps the benefits, too. Only a part of such data derives from the fusion of existing governmental databases. Large amounts of data are collected either from citizens who use seemingly free services (social networking services, online gaming, music platforms, cloud-based storage and messaging etc.) or whose data, derived from online transactions, are resold.

Increasing computing power, sophisticated algorithms and larger collections of personal data increase the potential impact on the personal lives of individuals as well. Comprehensive personal profiles are attractive for both commercial interests of the private sector, as well as for governmental security agencies. Intentions may go beyond the classic investigation purposes, extending them to so-called predictive policing. This shift towards a proactive and predictive focus challenges data protection principles of purpose limitation and necessity, fundamental rights of citizens like the protection of personal data and communications, and the presumption of innocence. The use of algorithms shifts decision making from humans to computers and thus reduces its transparency as the inputs and formulas are cloaked in confidentiality (see also recommendation 3.7 - Increase accountability and prevent abuse).

Technical progress thus clearly hampers an effective protection of communications, private life and personal data. The law is thus far silent. Participants of the SurPRISE events all over Europe understood the need for the police and other authorities to be abreast of the latest techniques, and were, in general, ready to support national authorities as long as sufficient safeguards (addressed by recommendation 3.5 - Implement proper safeguards) are in place. The first and foremost safeguard is appropriate regulation, entailing clear rules on what is permissible and what is not, for both private companies and law enforcement agencies. The adoption of legal bases (in line with the general principles of law) is the first tenet for compliance with the rule of law, the principle to which European countries adhere through their membership in the Council of Europe.

Links with current policy initiatives at the European level

This recommendation is along the lines of recently adopted documents that confirm the importance of protecting personal data, communications, and private and family life, vis-à-vis increased data processing capabilities. Examples include the Council of Europe Recommendation on the protection of individuals with regard to automatic processing of personal data in the context of profiling [CM/Rec(2010)13]; Council of Europe Recommendation on Improving user protection and security in cyberspace [2041 (2014)], and European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)).

The recommendation supports the current review of the Council of Europe Convention 108, and the adoption of the General Data Protection Regulation, the proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data COM (2012) 10 final.

3.2 Enforcing data protection in Europe

The impending revision of the data protection legal framework on the EU-level and amendments of national law should provide for mechanisms to effectively enforce data subjects' rights, also when tackling national and public security.

To this effect, an integrated strategy should be adopted at the national and European level (where applicable also on the local level) that takes into account the interaction between the private and the public sectors. At the local/national level, real control over data processing should be enabled, e.g., with mandatory ex post notification of data processing in law enforcement, the failure of which is subject to sanctions. Data protection authorities should be given harmonised powers of investigation and sanctioning, backed by sufficient human and financial resources. At the European level, collective lawsuits for mass-scale violations and the infliction of deterring sanctions should be enabled.

Background

Difficulties of effective data protection in Europe stem as much from outdated laws vis-à-vis the technological evolution (see recommendation 3.1 - The legal framework on data processing must meet the challenges of technological advances) as from the problematic enforcement of data protection rights. The latter has in turn many root causes: individuals' limited awareness of their rights, the difficulty of identifying violations and challenging them in court, and scarce resources of national data protection authorities which limit them in their enforcement activities, targeting low-hanging fruits only.

Consent plays a fundamental role for the right to protection of personal data, however, today it is increasingly seen as the Achilles' heel of data protection, as it becomes more and more difficult to obtain informed consent. Citizens referred to this notion as "control", and often reported feeling defencelessness when it comes to controlling their own personal data. Most of them are not aware of their existing rights, and if they do, they are confronted with under-staffed national DPAs. To re-establish consent, an investment in effective enforcement is required, which can only be achieved if the different dimensions of the implementation of data protection law are taken into account and seen in relation.

Links with current policy initiatives at the European level

The main message of this recommendation is line with the recommendations contained in the European Parliament resolution of 12 March 2014 on the US NSA surveillance programme (2013/2188(INI)).

This recommendation calls for the adoption of suitable mechanisms for the enforcement of data subjects' rights within the proposed Directive on the protection of individuals with regard to the processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences.

This recommendation supports the introduction, within the General Data Protection Regulation, of effective investigative powers for data protection authorities and deterring sanctions.

3.3 Protect personal data in transit, notably on the Internet

Technical and legal solutions need to be adopted to protect data in transit, notably on the internet, and in particular data travelling outside the European Union and the Schengen area.

Technical means to protect the privacy of transferred data should be explored and implemented. The conclusion of legally binding treaties with other countries, like the United States of America, is strongly recommended. Such treaties would protect data subjects in the context of both

commercial activities and operations conducted for the pursuit of public and national security. The transfer of data, especially for law enforcement purposes, to jurisdictions that do not offer an equivalent protection with regard to data processing, should be the exception and be duly accounted for.

A common policy should be developed and rules should be uniformly applied and enforced throughout the European Union and the Schengen area.

Background

The Internet challenges traditional jurisdictional boundaries. Data travel the Internet following logics that test the limits of the current data protection framework, and force lawmakers to find suitable alternatives that take into account the elusiveness of data transfers. Technical solutions could change the ways data packets travel the internet, e.g., by the support of European cloud services, in order to avoid such data leaving European territory. Another possibility could be to protect all data travelling over the Internet by encryption.

Participants also requested the law to provide safeguards and to offer redress. Insofar as such safeguards are contained in existing regulations, they are hardly known or not regarded as sufficient or sufficiently enforced (see recommendation 3.2 - Enforcing data protection in Europe). An example of such safeguards is avoiding transfers to countries known to have levels of protection of data lower than the EU and EFTA countries, including the need to duly justify transfers for law enforcement purposes. After the revelations by Edward Snowden, the negotiation of a treaty with the US in the context of law enforcement activities, as well as discussions concerning the revision of the Safe Harbour scheme, seem to be more pressing than ever. Citizens aim for legal clarity and more protection for themselves, instead of broadening the powers of intelligence agencies, and request the adoption of corresponding international legal instruments, such as an international treaty.

Links with current policy initiatives at the European level

This recommendation is along the lines of the EU Human Rights Guidelines on Freedom of Expression Online and Offline (2014), the Council of Europe Guide to human rights for Internet users (2014), and the UN General Assembly Resolution on The right to privacy in the digital age (A/RES/68/167) of 18 December 2013.

The recommendation’s main message corroborates the recommendations contained in the European Parliament resolution of 12 March 2014 on the US NSA surveillance programme (2013/2188(INI)), as well as in the European Commission’s Communication on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU COM(2013) 847 final.

This recommendation calls for the adoption of appropriate safeguards for transnational data transfers within the proposed General Data Protection Regulation and the proposed Directive on the protection of individuals with regard to the processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences. It grants importance to the negotiation of international agreements, such as the Framework agreement on data protection in the field of police and judicial cooperation (‘Umbrella Agreement’) with the United States of America, and the implementation of appropriate safeguards within the Safe Harbour, thus supporting the current position of the European Commission in their negotiations with the US. It calls for reflection on existing mutual legal assistance treaties and data exchange practices of EU agencies such as Europol and Eurojust.

This recommendation supports the Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, adopted on 10 April 2014 (819/14/EN WP 215) and the Working Document on surveillance of electronic communications for intelligence and national security purposes, adopted on December 5, 2014 (14 / EN WP 228) from the Article 29 Working Party (WP 29).

This recommendation should be taken into account when discussing additional protocols to the Cybercrime Convention and supports technical initiatives, such as those conducted by the recently started Internet Privacy Engineering Network.

3.4 Strengthen agencies providing supervision, guidance and control

For the processing of personal data, particularly in the field of police and justice, harmonised guidelines on a high level of protection are necessary. This especially applies to the respective control instances as well as to their control standards. Where data protection authorities exist in the EU member states which are already concerned with such tasks, they should be strengthened. Independent, competent and empowered data protection authorities should ensure meaningful supervision, guidance and control regarding the protection of personal data and the privacy of the individual. They should be enabled to include representatives of different knowledge areas and societal domains into their personnel structure.

With the background of already existing local, national and European supervisory authorities, it is recommended that these authorities are organised in such a way that governance is provided by them close to the European citizens and with effective means of enforcement even in cases of cross-border data transmissions.

An effective supervision and control of personal data processing by private (and internationally operating) companies is needed. These companies are oftentimes obliged to cooperate with security agencies. As for the security agencies themselves, a clear concept for the competences of data protection supervisory authorities and their jurisdiction over intelligence agencies is required.

All data protection supervisory authorities should be made better known to the citizens.

Background

For the processing of personal data within the member states for law enforcement purposes, the European Data Protection Directive 95/46/EC as well as the Council Framework Decision 2008/977/Jha for the police and justice sector are not applicable. Therefore, no fully harmonised guidelines maintaining a high level of protection for the processing of personal information by police and justice exist so far. The European Commission has submitted a proposal for a Directive in 2012, which has not yet been adopted by the Council and the Parliament.

European citizens oftentimes are not even aware of the currently established data protection supervisory authorities on national and European levels. As far as they are aware of them, they mostly perceive them as severely lacking essential personnel resources, regulatory powers and meaningful instruments of enforcement. This is also important due to the increasing and intensified joint work of security agencies across Europe, involving the exchange of information between each other. Also, the interdigitating way of cooperation between security agencies and private companies is noticeable, especially where the increasing number of governmental requests aiming at commercial data stock plays a role. In the case of data retention, this led to telecommunication providers being legally obliged to keep traffic data for security purposes. Companies, which are in the field of telecommunication and tele-media, oftentimes operate globally. All of these circumstances require a strengthening of European data protection supervisory authorities. By the processes as recommended above, they would then be able to contribute to an evolvement of the European data protection framework in a harmonising way, thereby also adequately addressing the challenges of cross-border data transfers and jurisdiction issues.

Participants were also specifically concerned about surveillance of their communication and transactions on the Internet via deep packet inspection. The requested top level European or international supervisory authority should therefore also have competences and powers regarding surveillance activities by foreign states like the NSA programs revealed by Snowden. And it was also suggested that such an agency should comprise expertise from a wide range of disciplines to allow for a holistic view on surveillance and its impact on society, including also sociology, technology or philosophy.

The obvious lack of awareness and knowledge about existing data protection agencies and regulations suggests to reinforce information activities, e.g., by establishing strong communication and interaction platforms reporting their competences, activities and offers of assistance.

Links with current policy initiatives at the European level

This recommendation has relevance for the proposed General Data Protection Regulation and the Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences.

3.5 Implement proper safeguards

Untargeted mass surveillance circumvents existing legal safeguards. Any restriction of fundamental rights resulting from the use of surveillance technologies and derived personal data must be based on a stringent case-by-case examination of their permissibility, such as that foreseen by articles 52.1 and 52.3 of the Charter of Fundamental Rights of the European Union. Such examination must ensure that:

a) **any restriction of fundamental rights has a proper legal basis;**

b) **these restrictions are compatible with a democratic society;**

c) **any exercise of discretion by (administrative) authorities is foreseeable and constrained;**

d) **these restrictions are reasonable, necessary and proportionate in achieving an identified and pressing aim;**

e) **they do not violate the core dimensions of privacy (as progressively identified).**

Such a test should be performed prior to the adoption of a tool or derived data, they should encompass the implementation and use and they should be subject to ex post reviews by independent judicial authorities.

Background

After major terrorist attacks a large increase of intelligence-led policing backed by hastily adopted statutes (e.g., criminalising inchoate crimes) can be observed. This tendency is accompanied by the routine use of surveillance technologies without a proper assessment of their potential drawbacks. The policies regulating the adoption of SOSTs framed the relationship between privacy and security predominantly in terms of the need to 'strike a balance' or to establish a 'trade-off' between the collective interest of security and the individual right to privacy (a concept here encompassing both the right to respect for private and family life, and the right to data protection). The ensuing restrictions imposed on the two fundamental rights for the purpose of security have arguably exceeded the permissible scope of limitations to both rights so that it can be questioned whether all resulting limitations are actually compatible with the values these rights seek to protect.

Law and oversight can provide answers to existing problems. In matters not touching the essence of privacy (core), a proper proportionality assessment is required, including through demonstrating that the benefits actually delivered are greater than the intrusion into privacy. Intrusions into the core of privacy are prohibited and must be avoided by redesigning the surveillance, including through privacy by design features. There is also need for a common definition of the core of privacy, taking national and European case law decisions into account.

At the SurPRISE events, the vast majority of participants saw privacy as a cherished right, both at the individual and collective level, and feared that the power of control intrinsic in privacy is fading away, due to fast paced technological evolution, unmatched by the law or by means of enforcement, which leaves too many grey areas. Only a minority of citizens embraced the trade-off, accepting to give in privacy for increased security. The majority of participants did not believe that privacy and security are irreconcilable, and challenged the assumption that security can be obtained at the sacrifice of privacy. They articulated different views: either the relation between privacy and security has to be negotiated on a case-by-case basis, or appropriate legal solutions need to be found to achieve a comprehensive and earnest balance.

The formulation of this recommendation combines SurPRISE research results and the citizens' proposals. Although citizens did not use legal jargon, their recommendations fulfil many points of the legal formulation of the permissible limitations test. In particular, citizens:

1. Asked for a legal basis for the use of SOSTs, in connection to precise purposes (a).
2. Saw privacy as an evolving concept, containing a core that should not be intruded upon (e.g., sensitive data, medical records, intimate habits, home and family) (b)
3. Agreed that SOSTs can be used for the investigation of crimes, to pursue national security, and help the ones in need, but any other use should be banned. Citizens reject the idea that their personal communications be checked for national security. Citizens strongly supported the idea that data should be collected based on judicial authorization (c).
4. Demanded to 'watch the watchers'. Accountability was the key to trust. They strongly supported the idea of direct control by a data protection supervisory authority or an Ombudsman, with the possibility to access one's data. (d)
5. Recommended that measures which are not effective should not be used. This preconditions an earnest evaluation of effectiveness to achieve the intended original purpose. Some citizens expressed that since from their point of view, our society is not under threat, and SOSTs should not be routinely used at all. (d)
6. Expressed that a measure is probably proportionate if targeted, e.g., limited in time, scope, concerned persons or space; mass surveillance must be prohibited. The check of the respect of the principles of necessity, adequacy and proportionality must be performed by a judicial authority. (e)

This recommendation summarises the elements of examination to ensure compliance with fundamental rights. Some of these elements are related to other recommendations, containing more detailed descriptions or suggestions on how to implement them: e.g., d) needs 3.14 - Establish technology assessment and on-going evaluation for its operationalization and clearly addresses 3.6 Limit the scope of data collection and 3.4 - Strengthen agencies providing supervision, guidance and control could be responsible for the implementation of the safeguards.

Links with current policy initiatives at the European level

This recommendation is along the lines of the EU Human Rights Guidelines on Freedom of Expression Online and Offline (2014), the Council of Europe Guide to human rights for Internet users (2014), and the UN General Assembly Resolution on The right to privacy in the digital age (A/RES/68/167) of 18 December 2013.

Its main message corroborates the recommendations contained in the European Parliament resolution of 12 March 2014 on the US NSA surveillance programme (2013/2188(INI)). It has a strong impact on the debates concerning the proposed Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences.

This recommendation is also reflected in the proposed Data Protection Regulation in relation to the accountability and responsibility provisions.

3.6 Limit the scope of data collection

Enable a more effective preservation of citizen's right to privacy by meaningful enforcement of the principles of purpose limitation and proportionality. This encompasses a genuine consideration of non- or less intrusive alternatives prior to the deployment of broad dragnet surveillance measures for security purposes. Develop, foster, and prioritise measures (including SOSTs) with a narrower scope of data collection, storage and use whenever they are suitable instead of focusing on forms of untargeted mass surveillance.

Background

Security agencies in Europe have shifted more and more towards pre-emptive measures, thereby endorsing an increased focus on a broader scope of data collection and analysis. However, the expansion of data collection, going along with emphasising police intelligence tasks, results in a gradual erosion of citizens' rights to privacy. This recommendation is based on research within the SurPRISE project as well as on the results of the citizen summits wherein citizens showed great concern about vast data collections both in the private as well in the public sector. Regarding data collections for security purposes, many citizens expressed that they oftentimes feel as if being under constant surveillance. This is mostly understood as a deep mistrust towards citizens in general from governmental side, putting the constitutionally manifested principle of the presumption of innocence at risk.

The principle of data minimisation and its comprehensive application in the context of security technologies forms the core of this recommendation. It is therefore in clear contradiction to past developments and ongoing tendencies to vastly extend the scope of the collection, exchange and use of data in bowls, commercial and law enforcement environments.

Links with current policy initiatives at the European level

This recommendation concerns, as most of the those related to legal issues do, again the adoption of the General Data Protection Regulation, the proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data COM (2012) 10 final.

This recommendation is also closely related to the principle of data minimization, or principle of privacy by default, which is recognized in the new proposed Data Protection Regulation.

This recommendation is connected to the position of the ECJ regarding the Directive on Data Retention and GT29 position thereon, adopted on August 1, 2014 "Statement on the ruling of the Court of Justice of the European Union (CJEU) which invalidates the Data Retention Directive (14 / EN / WP 220).

This recommendation is also linked to WP 29 activities on Big Data and on the Internet of the things (IoT); Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU, adopted on September 16, 2014 (14 / EN / WP221) and Opinion 8/2014, on the on Recent Developments on the Internet of Things, adopted on 16 September 2014 (14 / EN / WP 223).

3.7 Increase accountability and prevent abuse

European states need to promote and pursue a sincere political reflection as to how to design and deploy technology for security purposes in compliance with fundamental rights. Stronger accountability and liability for misuse and abuse must be established in both the public as well as the private sector. Measures include:

- **introducing and enforcing effective and deterrent sanctions;**
- **making misuses publicly known;**
- **supporting whistleblowing schemes;**
- **storing data securely, and never reselling or transferring them; and**
- **limiting automated decision-making based on the collected data (algorithms-based decisions) so that they assist humans, rather than replace them.**

Organisational and technical measures should be implemented to prevent abuse and to make abuses detectable to supervisory agencies.

Background

Although law enforcement authorities are generally trusted, higher levels of trust are hindered by the opaqueness in using SOSTs and uncertainty regarding existing legal safeguards, oversight mechanisms, and appeal of adverse decisions. Feelings of rampant abuse of power and misuse of collected data endanger trust in institutions and organisations responsible for security. Even if citizens support the use of surveillance technologies for public and national security purposes, they fear abuses. A lack of enforcement activities is observed when it comes to problems with fundamental rights and data protection. Also trust in the automated judgements issued by algorithms is low. Citizens are afraid that SOSTs are replacing, rather than supporting, human action, and feel they have no voice in the decision as to how these technologies are used to maintain society secure. They therefore propose higher degrees of accountability and a human–centric use of SOSTs to minimize the risk of abuse and of (adverse) automated decisions.

This recommendation demands improved protection of fundamental rights as part of a responsible use of surveillance-orientated security technologies. It explicitly requests more transparency, stricter controls, precautions and sanctions to increase accountability and to avoid the misuse of data. Best practices and mechanisms used in other sectors, e.g., in the fight against corruption could be applied, and NGOs active in the spheres of transparency and the protection of fundamental rights should be supported. In addition, this recommendation takes into account the widespread opinion that the technology should help the responsible personnel to do their jobs, but not to replace them.

Links with current policy initiatives at the European level

This recommendation is relevant for the proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data COM (2012) 10 final.

3.8 Regulate and limit the role of private and non-governmental actors in the provision of public and national security

Security should remain the responsibility of state actors. It should be clarified to which extent and in which way the private sector and non-governmental actors currently contribute to the pursuit of security and to which degree these contributions are necessary. Outsourcing security and cooperating with private actors (including data requests) should be made known and subjected to public scrutiny. Suitable and legitimate cooperation between such actors and the state must be strictly regulated. Breaches of the law should be strictly sanctioned.

Security functions may only be outsourced if the contributions of private actors are equally or better than public standards in both terms, compliance with fundamental rights and quality of services.

The ownership and control of data should always remain under European legislation, security related data must not be mixed with other private data. The limitation concerns also the transfer of data from public authorities to private entities, it must be not allowed to sell data to private actors, neither for security nor for commercial purposes.

Background

SurPRISE did not feature specific questions about the private sector over the course of the consultations with the public. Nevertheless, participants at the events raised the issue frequently during table discussions. They expressed concern regarding data collection, processing and storage by commercial actors due to their drive for profit. Participants voiced strong criticism against the cooperation of law enforcement with private companies in general and against one-sided governmental requests of access to data stocks of private entities. They expressed the need to be thoroughly informed about such relations and which data are shared with whom. Lack of transparency concerning such relations is a serious issue. The same is true for the absence of legal bases for forms of cooperation and the increasingly unofficial partnerships.

Links with current policy initiatives at the European level

This recommendation is along the lines of the UN OHCHR Guiding Principles on Business and Human Rights (2011), and other documents such as the Council of Europe Guidelines for the cooperation between law enforcement and internet service providers against cybercrime (2008).

This recommendation is relevant for the discussion of the General Data Protection Regulation and the proposed Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences.

It has a strong impact on the discussion of the opportunity to adopt a new Data Retention Directive.

Also this recommendation is related to the position of the ECJ regarding the Directive on Data Retention and GT29 position thereon, adopted on August 1, 2014 "Statement on the ruling of the Court of Justice of the European Union (CJEU) which invalidates the Data Retention Directive (14 / EN / WP 220).

It is related to the current consultation on the renewal of the EU Internal Security Strategy and the therein addressed cooperation with the private sector.

It is linked to the discussion of the opportunity to adopt a new Data Retention Directive.

It also relates to the proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing /* COM/2013/045 final - 2013/0025 (COD).

3.9 Establish a privacy-orientated competitive market

Policy makers should provide regulatory acts and incentives to establish a European market where privacy constitutes a competitive advantage. To this effect two sets of measures should be adopted. First, incentives in the form of regulation should be implemented, e.g., obligatory Privacy by Design for public procurement. Second, asymmetric or missing information of citizens concerning means of data collection, storage and use should be corrected, e.g., by mandatory information of users of "free services" about the basis of business models of such offers.

Background

As already mentioned, SurPRISE did not address specific questions about the private sector or markets. This recommendation refers to a large extent to general privacy concerns of the citizens in relation to the use of Internet or mobile services.

Two features characterise today's apps and service markets, legal grey areas, if not a legal vacuum, and asymmetric information, whereby users are largely unaware of the business models funding services and tools. Research shows that people want to use services for their convenience and prefer not to pay for services. However, it also shows that people are unaware that they pay services with their personal information, implicitly causing a loss of their rights.

Privacy becomes a negative externality borne by users. When this aspect surfaces, as it happened spontaneously during the SurPRISE summits, the picture changes. While users are not critical of services and tools per se, they challenge the use made of them by private companies. Users expect crucial information about the use of their personal data being provided to them, rather than being obliged to look for it. They also demand to control services and tools (and the personal data gathered by service providers). This includes particularly being able to choose between different services instead of being restricted to products and services provided by quasi-monopolistic international companies (referring to the excessive dependence from US-based firms and lock-in effects).

The citizens' recommendations go in the direction of stimulating a multi-faceted, competitive market, whereby the protection of privacy is seen both as a benefit for consumers and a competitive advantage for companies. Whereas approaches to address the externalities and asymmetries characterising this market are urgently requested, finding the most appropriate mixes of incentives and regulations constitutes certainly also an object for more research. Experiences gained for example in relation to environmental policies should be scanned and effective measures be transferred to problems of "data pollution". What happened in other sectors, e.g., the automotive industry and in the promotion of energy-saving products, could provide valuable inspirations, e.g., *"Green" Taxing schemes*. Certificates or privacy seals can assist citizens in the selection of data saving and privacy protecting products and services and serve as guidelines for public procurement. Clear statements like "this service is making profit out of your data" instead of information hidden in the terms and conditions should citizens make aware of privacy risks of using such services.

Implementations of this recommendation need to be carefully designed in order to favour really privacy enhancing products and services and exclude unintentional competitive advantages for less compliant Non-EU providers.

Links with current policy initiatives at the European level

This recommendation supports the introduction of mechanisms to take privacy into account from the early stage, and provide adequate information to data subjects. It calls for the adoption of appropriate incentives within the proposed General Data Protection Regulation.

It calls for considering additional mechanisms to invest in the area of privacy-minded technical solutions, for instance within the context of Horizon 2020.

It is related to several initiatives and projects aimed at establishing privacy certification schemes and seals. The EU Privacy seals project launched by the Institute for the Protection and Security of the Citizen of the Joint Research Centre (JRC) in collaboration with the Directorate-General for Justice (DG JUST) provides a comprehensive overview of such activities. [9]

3.10 Implement and improve transparency

Member states need to increase their efforts to implement and improve the transparency of policy decisions, of the work of security authorities as well as of corporations and companies, in particular if the privacy of the citizens is affected. Transparency must be supported actively as current arrangements are insufficient and must comprise more than existing rights to know. Different communication channels should be used to reach as many parts of the population as possible.

Information about data access rights is not enough, transparency must include information about who is doing what and why to get more active insight.

Transparency does relate to policy making, the Constitution and laws on the one hand, and also to the practices of data collection, storage, processing, linkage, and (re)transmission on the other hand.

At least three levels of transparency are to be envisaged:

- **transparency about policy (legislation transparency),**
- **transparency about security authorities (operational transparency),**
- **corporate transparency (corporate and social responsibility).**

- **Citizens should be given the right to access on a low-threshold level sufficient information on how surveillance systems operate,**
- **information on which and where surveillance systems have been implemented,**
- **information on how they can exercise their civic rights (e.g., in order to gain information about what kind of data about them is stored and processed where and by whom).**

Mandatory standards based on (independently evaluated) best practices according to operational transparency as well as corporate and social responsibility should be implemented.

Background

Especially SOSTs are operated in a context where transparency is perceived as lacking by the citizens. The need for transparency is not constrained to political decisions which may have an impact on society. More transparency is one of the key demands placed at the citizen summits. Greater transparency with reference to the purpose(s) of data collection and usage, appropriateness, costs, impact of SOSTs and surveillance practices is needed to ensure that citizens' privacy is respected. Transparency is also key factor for trust in security agencies and state actors in general.

[9] http://www.vub.ac.be/LSTS/pub/Dehert/481.pdf.

Links with current policy initiatives at the European level

These conclusions are linked to the adoption of the General Data Protection Regulation and the proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data COM (2012) 10 final.

It is linked to the Transparency Register run by the 'Joint Transparency Register Secretariat' (JTRS), staffed by officials from Parliament's and the Commission's Transparency Units.

It is related to the Council of Europe Committee of Ministers Recommendation on the Protection of Whistleblowers, asking that member states "have in place a normative, institutional and judicial framework to protect individuals who, in the context of their work-based relationship, report or disclose information on threats or harm to the public interest.

This recommendation, extrapolating the findings beyond the financial regime, is related to the proposal to amend the Directive 2013/34 / EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups[10].

3.11 Improve training and education of security authorities

There is a need for more training and education for the personnel of security authorities and stakeholders in various surveillance practices to improve their work in order to act in compliance with privacy and other fundamental rights. Stakeholders in surveillance practices refer to all parties who are involved in conducting surveillance practices such as governmental organisations, service providers (public and private), staff of (surveillance) technology producers and vendors, or consultancies advising security authorities.

Only authorised, trained and ethically aware personnel should be allowed to handle SOSTs and the derived data.

Background

There is an increasing fear among citizens that security authorities, law enforcement and other actors in the field of security exceed their powers and lack in respecting privacy and other fundamental rights. This fear does not imply that security measures are rejected on the whole as the work of police and other security authorities in general is considered as very important in the public. However, a major problem lies in the increasing gap between security competences and technical surveillance capabilities and the appropriate implementation of such activities in accordance with privacy.

The implementation of this recommendation requires mandatory professional education and training within certain iterate timeframes. Guidelines and codes of conduct based on best practice should be developed, taking into account the specific needs of particular stakeholder groups and involving independent third-party legal and scientific counselling. Ongoing evaluations of the training materials and the training process should be foreseen.

This recommendation demands also a major effort in education and training about potential privacy issues of engineers developing IT technologies and applications, used for commercial or for surveillance purposes.

To support transparency (see 3.10 - Implement and improve transparency) training material and information about the educational processes should be made public insofar not conflicting with security objectives.

Links with current policy initiatives at the European level

This recommendation is linked to Articles 32 and 49 of the proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of

[10] http://register.consilium.europa.eu/doc/srv?l=EN&f=PE%2047%202014%20INIT

prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.

This recommendation would require, in the proposal of European legislation on the subject, that the formation of these subjects were compulsory and extent legally required. In the same way that action on gender equality and public sector quotas are imposed, it should also be required training on privacy protection.

3.12 Raise awareness on security and privacy

Governments should support all actors in the field of education to reach citizens and educate the population on how new information technologies, and in particular SOSTs work, and how citizens can protect their privacy and manage their digital data. Appropriate strategies should be developed and implemented for different knowledge levels, ages and social backgrounds.

Background

During the citizen summits, strong emphasis was put not only on the need for a better information of the citizens in general but also on the obligation of governments to support all actors in the field of education in raising awareness for the pros and cons of social networks or emerging information technologies. This recommendation aims at increasing knowledge about new information technologies and digital literacy of the population in general. Participants frequently stated a lack of knowledge of how to protect their privacy; better information of citizens could enable a more responsible handling of new information technologies and reduce feelings of helplessness in view of increasing pervasiveness of information technologies and the resulting surveillance capabilities.

Links with current policy initiatives at the European level

This recommendation is linked to activities of the European Union Agency for Fundamental Rights (FRA), in particular the Handbook on European data protection law and the project on National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies.

The Data Protection Day, launched by the Committee of Ministers of the Council of Europe and celebrated each year on 28 January is another example of a Europe-wide awareness raising activity. The Data Protection Day could be used by national authorities to carry out or initiate information work on all levels of education.

3.13 Foster participation in decision making

Citizens need to be fully involved in the process of policy-making, at least at the local and national level. National and regional governments should open the debate on surveillance orientated security technologies to the public and find appropriate solutions for involving citizens directly in decision making. This may entail several approaches, such as enhanced information through media, citizen consultations, participative TA (see 3.14 - Establish technology assessment and on-going evaluation), or referenda. This involvement should come along with prior provision of objective information about facts which are related to the topics of the public discourse.

Background

Citizens expressed their concerns regarding the impact of surveillance technologies on society. They clearly link the respect for privacy to a healthy democracy and challenged the concept of achieving public security by deploying surveillance orientated security technologies; they rather feel exposed to governmental surveillance without protection. This impression oftentimes goes along with a missing understanding of the reasons why and under which circumstances such surveillance technologies are used. Citizens want to have a say in the decision of which surveillance orientated security technologies are used and for which purposes.

However, citizens do not have possibilities or do not know how to participate. Existing mechanisms of consultation, insofar as implemented, are not well known to the public. Excluding citizens from the decision-making process as to what technologies are permissible negatively affects the acceptance of such technologies and the right to good administration.

The recommendation is to achieve more transparency and societal support by involving European citizens before the deployment of new security technologies. By seriously involving citizens in determining security policies and related measures to be deployed, feelings of powerlessness are being addressed and democratic processes are initiated. Giving stronger emphasis to bottom-up approaches, such as civic engagement, and citizens' proposals concerning security, is also a contribution to increase societal resilience. The experiences at the citizen summits showed that the engagement of citizens also opens up the perspective and forms a counterweight to the technology bias that often dominates the range of solutions under consideration.

The decision support system developed in the SurPRISE project offers a practised, tested and improved approach of involving citizens in decision-making related to security policies and measures. The details of this method are described in more detail in chapter 5 of this report.

Links with current policy initiatives at the European level

This recommendation is linked to the Council Regulation (EU) No 390/2014 of 14 April 2014 establishing the 'Europe for Citizens' programme, the programme is implemented by the Executive Agency for Education, Audiovisual and Culture (EACEA).

A European citizens' initiative is an invitation to the European Commission to propose legislation on matters where the EU has competence to legislate. A citizens' initiative has to be backed by at least one million EU citizens, coming from at least 7 out of the 28 member states.

3.14 Establish technology assessment and on-going evaluation

A Technology Assessment (TA) should be conducted from the earliest stage of developing security technologies. A vital part of technology assessment is looking for and evaluating different alternative solutions, be it technical, organizational or legal. Applied TA methods should provide a transparent and participative assessment of alternatives. TA is therefore more comprehensive than a Privacy Impact Assessment (PIA) only. The discussions of which technologies are permissible (and acceptable) should be mandatory and fully included in the procurement and decision-making processes.

An evaluation of surveillance-orientated security technologies should also embrace implementation and deployment. Therefore, it needs to be regularly repeated during use by an impartial and competent entity. This evaluation should support and extend the case-by-case examination of their permissibility addressed in the recommendation 3.5 - Implement proper safeguards. It should operationalise the permissibility test by covering the following aspects: suitability, effectiveness, cost, robustness, ethical and societal impact, privacy impact assessment, means of intended deployment, and the existence of potential alternatives.

Background

The increasing use of surveillance orientated security technologies throughout Europe is oftentimes criticised and challenged with reference to lack of effectiveness, latent infringements of fundamental rights and severe risk of function or mission creep. It is argued that such mission creeps can cause considerable negative impact on the privacy of citizens on a case-by-case basis as well as an erosion of privacy as fundamental right in itself.

Surveillance orientated security technologies are complex technological systems and citizens are aware of this complexity. They sometimes feel that they are not able to cope with the complexity. Therefore, they are demanding assessments by trusted third parties, objective evaluators, who are able to understand the SOST and don't have a stake themselves in the issue. Acceptance and acceptability of SOSTs are dependent on their efficacy to a high degree. Providing answers to the question of appropriateness, taking into account (non-technical) alternatives, could be seen as a key element to foster trust in institutions producing and applying surveillance technologies. TA can provide procedures that enable this process.

The deployment of many surveillance orientated security technologies is also challenged on the basis of concerns regarding their potential intrusiveness on the privacy of individuals and the corresponding long-term societal impacts in general. One of the main aspects of the criticism is that the deployment of surveillance orientated security technologies has oftentimes a negative impact on citizens' fundamental rights without providing the proposed security enhancement. Citizens complain that in most cases it is completely non-transparent whether the surveillance technologies in question has any benefits. Therefore, an evaluation of surveillance orientated security technologies should be conducted by independent, objective parties/entities in a comprehensive way.

The evaluation must not be just a checklist of compliance. Ideally, it is conducted already during the design phase of surveillance orientated security technologies, but also necessarily during and after implementation, to take changes of relevant factors and circumstances into account, as well as for a better assessment based upon deployment experiences. The latter encompasses reflections about how good the technology fulfils the intended purpose and if anticipated risks have materialised. Also, a timely limitation of surveillance orientated security technologies deployment could be considered if suitable. As far as possible and suitable the process and the results of the evaluation should be made transparent to gain public trust.

Links with current policy initiatives at the European level

This recommendation supports the introduction of data protection impact assessments in the General data protection regulation.

The Parliaments and civil society in Technology Assessment project (PACITA) aims at increasing the capacity and enhancing the institutional foundation for knowledge-based policy-making on issues involving science, technology and innovation, mainly based upon the diversity of practices in Parliamentary Technology Assessment (PTA). Key practices in focus are interactive in the sense that they engage science, civil society organizations, stakeholders, citizens, parliaments and/or governments directly.

It is linked to results from the SurPRISE project, specifically to the Decision Support System (DSS) presented in chapter 5 - Manual: How to engage citizens.

3.15 Request mandatory Privacy by Design and Privacy by Default

The integration, maintenance, and further development of Privacy by Design and Privacy by Default principles should become a mandatory requirement for the development and implementation of surveillance orientated security technologies. Implementing PbD may occur in various ways, such as reducing the amount of data initially collected, obfuscation of sensitive information, preventing unauthorized access or misuse for other purposes. Furthermore, it must be ensured that the realisation of PbD is effective, comprehensible, evaluable, and that it goes along with an effective Privacy Impact Assessment in advance.

Background

Privacy by Design means that appropriate technical and organizational measures to meet privacy protection requirements are implemented, Privacy by Default means that only those personal data are processed which are necessary for each specific purpose in the default settings.

A fully-fledged implementation of Privacy by Design and Privacy by Default is not always possible due to the fundamentally intrusive nature of some SOSTs. Nevertheless, such technologies can be designed and programmed in a way that they support PbD principles. The aim should be the reduction, or even complete prevention of technology and use related data misuse, or failure risks. Thereby, it must be taken care that these principles are followed comprehensively and genuinely. It should be avoided that if a PbD process is implemented, an automatic assumption is fixed that the surveillance orientated security technology fulfils all requirements and PbD principles. So a continuous evaluation is needed as a flexibly on-going process to avoid such a fixed status quo, especially if the deployment context or other relevant circumstances have changed.

Implications for current policy initiatives

This recommendation supports the introduction of mechanisms to take privacy into account from the early stage of development of IT services and products in the proposed General Data Protection Regulation, explicitly including surveillance-oriented security technologies.

It is linked to the "Privacy and Data Protection by Design – from policy to engineering" report published by the European Union Agency for Network and Information Security (ENISA) in January 2015.

3.16 Focus on root causes of insecurity

Economic and social policies should become an integral element of security strategies at the level of the European Union and its member states. Reducing economic inequalities and addressing the general problems of lacking social justice are of essential importance for other key dimensions of security. It is an indispensable contribution to the prevention of violent radicalisation, and also a precautionary measure against poverty related crime, terrorism and the loss of political and societal cohesion in Europe. National and European policy-makers in the area of security policy should be aware of these intertwined factors and urgently foster measures to improve the economic and social situation.

Background

The economic crisis is among the most important concerns of European citizens, as confirmed by Eurobarometer polls. Many of them are worried about the security of incomes and jobs. Improving and maintaining economic and social security is an important objective as such. However, increasing poverty due to loss of jobs and incomes is also a root cause not only of petty crimes but also of increasing violent radicalisation on an individual as well as on a political system level. Economic security is thus also a prerequisite for the very existence and survival of the EU, not only as an economic power on the global scale but also as the most successful European peace project in the last half-century. The broader the perspective adopted when analysing policy options, the better the chances to develop sustainable solutions for security problems on national as well as EU level.

Implications for current policy initiatives

This recommendation clearly influences economic policies to resolve the enduring economic crisis in the European Union. It supports a change from austerity to growth oriented programmes and strategies. It demands for expanding social security throughout Europe and for reducing imbalances in working opportunities and in the distribution of incomes. EU's Cohesion Policy and Investment Strategy are also addressed.

It is linked to the Europe 2020 targets, particularly to target 1. Employment and 5. Poverty / social exclusion.

It addresses the Commission priority Investment Plan 2015-2017.

It demands for a revision of the Stability and Growth Pact.

4 Criteria and factors determining the acceptability of security technologies

In response to the oversimplifying trade-off approach, dominating not only political debates and decision making on security technologies but also informing and thus influencing empirical research on the acceptability of SOSTs, SurPRISE developed a comprehensive and complex model of factors and criteria influencing the assessment of security technologies by citizens. This model was empirically tested at the participatory events organised by SurPRISE. In this chapter the main findings on factors and criteria influencing the acceptability of SOSTs are briefly summarised.[11] It contains information of highest importance and relevance for policy makers, security agencies, security industry and citizens alike. In the context of SurPRISE, factors represent those elements that influence people's opinions, but that people usually do not explicitly state or that they recognize only partially. Criteria are argumentations consciously used by citizens to explain their position vis-à-vis the acceptability of SOSTs. Factors may be addressed by means of quantitative methods, while criteria can be better assessed qualitatively through table discussions and focus groups.

Institutional trustworthiness is a key factor determining the acceptability of SOSTs, and it shows that, besides what citizens may think or know about security technologies, the degree of trust that security agencies and political institutions enjoy is a crucial element that citizens do take into account when assessing the acceptability of security technologies. Interestingly, the perceived level of threat has a limited effect on the acceptability of SOSTs, whilst Social Proximity has a strong impact on acceptability, confirming that security technologies that operate blanket surveillance are considered significantly less acceptable than security technologies carefully focusing on specific targets. Both effectiveness and intrusiveness emerge as highly relevant factors in explaining the level of acceptability of SOSTs. Moreover, whilst much of the security technology discourses insists that security technologies need to be intrusive to be effective, citizens argue that the more a technology is considered intrusive, the less it might be considered to be effective. This results question the general idea that SOSTs need to be intrusive to be effective, and, consequently, radically questions the trade-off approach. Moreover, our analysis shows that the trade-off approach does not generally influence acceptability, except in the case of very controversial SOSTs, like DPI. Age is positively correlated with acceptability; a result that radically questions the general belief that the younger generation, due to their familiarity with ICTs and SOSTs, would be less concerned with privacy issues. Table 1 and Table 2 list the factors tested in the empirical model, Table 1 contains the factors that proved statistically significant, Table 2 those without statistical significance.

[11] See D2.4 - key factors affecting public acceptance and acceptability of SOSTs for a full description of the theoretical foundations of this model, of the complex hypotheses and relationships mapped in the model, of the methods applied in the empirical testing, and of the detailed results of the empirical analyses.

1. **General attitudes towards technology**. A generally positive attitude towards the ability of technology to enhance security makes SOSTs more acceptable. Conversely, a generally critical or sceptical view makes SOSTs less acceptable.
2. **Institutional trustworthiness**. Trust in security agencies makes the use of a given SOST more acceptable. The opposite is also true: the use of a more acceptable SOST (CCTVs or SLT, in this case) helps security agencies to be perceived as more trustworthy.
3. **Social Proximity.** SOSTs targeting specific groups or profiles, usually presented as "suspects" or "criminals" are eventually more acceptable than SOSTs (smart CCTVs and SLT) that operate on blanket surveillance (DPI).
4. **Perceived intrusiveness** has a negative influence on acceptability. The more a SOST is perceived as intrusive, the less it is considered acceptable.
5. **Perceived effectiveness** has a positive influence on acceptability. The more a SOST is perceived as effective, the more it is considered acceptable.
6. **Substantive privacy concern.** A higher concern for both information and physical privacy makes SOSTs less acceptable.
7. **Age**. Age is positively correlated with acceptability of SOSTs. Older participants are more likely to accept SOSTs than younger ones.

Table 1: Factors influencing acceptability of SOSTs (statistically significant)

1. **Perceived level of threat**. Contrary to expectations, a more intense perception of security threat would NOT make SOSTs more acceptable. Concerns for online security, though, do have a positive effect on acceptability: the more participants are worried about their safety online, the more willing they were to accept SOSTs.
2. **Spatial proximity**. The proximity of SOSTs located and/or operating close to the physical and virtual spaces usually frequented by the participants did not influence the acceptability of SOSTs. However, we found that it has an effect on Substantive Privacy Concerns, which decreases the likelihood of considering SOST acceptable.
3. **Temporal proximity.** The prospective of SOSTs being very influential in the future did not influence the acceptability of them. However, we found that it has an effect on SOST Perceived Intrusiveness and Substantive Privacy Concerns, which, in turn, decrease the likelihood of considering a SOST acceptable.
4. **Familiarity with SOSTs.** Contrary to expectations, a deeper familiarity with SOSTs does not influence the acceptability of them.
5. **Security/privacy balance**. Considering technologies as both intrusive and effective do not make these technologies, in general, more acceptable. This relation has been confirmed only in the case of DPI.
6. **Education.** The educational level does not influence acceptability of SOSTs.
7. **Income.** The income level does not influence acceptability of SOSTs.

Table 2: Factors influencing acceptability of SOSTs (statistically not significant)

Some of the most interesting results of this study stem from the qualitative analysis and suggest that additional factors like the type of crime targeted, the risk of function-creep, the clarity of the operational functions of SOSTs, or the role of human personnel as very relevant when citizens assess the acceptability of SOSTs. Participants suggested that acceptable technologies should primarily address the types of crime they consider a priority, such as street crime, political corruption and financial crimes. Table 3 list the most relevant these additional factors.

Are more likely to be considered acceptable, SOSTs which…

- target crimes which are within the citizens' priorities (Priority);
- empower citizens and make them feel in control (Empowerment);
- are employed with a clear, delimited purpose in mind (Focus);
- provide direct, personal services and benefits to their users (Benefit).

Are less likely to be considered acceptable, SOSTs which…

- promote intolerance and segregation (Discrimination);
- entail high function creep risks (Function creep);
- undermine the role of humans (Algorithms);
- involve private sector or foreign national security agencies (Delegation).

Table 3: New and emerging factors likely to influence SOSTs' acceptability (to be tested in future research).

Last but not least, the analysis of the qualitative data has identified a number of criteria influencing the acceptability of surveillance technologies.

SOSTs are regarded as more acceptable if:

- operating within a European regulatory framework and under the control of a European regulatory body.
- operating in a context where transparency about the procedures, information about both data protection rights and principles and about the purposes and the scopes of security actions as well as accountability of security operators is ensured at all times.
- operated only by public authorities and only for public benefits. The participation of private actors in security operations, such as when security agencies acquire banking data or Facebook data or when security functions are outsourced to private operators, therefore, must be strictly regulated.
- their benefits largely outweigh their costs, especially in comparison to other non-technological, less intrusive, alternatives.
- their operation can be regulated through an opt-in approach. Whenever this is not possible, their operation need to be communicated to targeted individuals.
- they allow monitored individuals to access, modify and delete data about themselves.
- they target less sensitive data and spaces, whenever possible, according to criteria and purposes know to the public.
- they do not operate blanket surveillance. After reasonable evidences are gathered, they address specific targets, in specific times and spaces and for specific purposes. Whilst their purposes may change, these changes need to be explicitly discussed and publicly approved.
- they incorporate Privacy-by-Design protocols and mechanisms.

- they work and operate in combination with non-technological measures and social strategies addressing the social and economic causes of insecurity. SOSTs are not alternatives but complementary to human resources and social policies.

All these criteria are also addressed by the recommendations included in the previous chapter. They should be integrated in decision making on SOSTS as an additional checklist and initial opening of the evaluation process.

5 Manual: How to engage citizens

This manual provides an overview of the unique methodology of the SurPRISE project, which is based on participatory events and employs the Surprise Decision Support System (DSS), an on-line tool that can help to facilitate similar projects in the future by engaging citizens, and have their voice heard in decision making.[12]

5.1 The participatory methodology and the SurPRISE DSS

5.1.1 The voice of the citizens

The core aim of the participatory methodology is to engage citizens in discussing complex topics during citizen summits. These summits are public meetings where citizens gather together to have face-to-face conversations about particular topics.

Citizen summits generate extremely valuable knowledge for public officials who have to make choices in the public interest. The richness and accuracy of the information gathered in a citizen summit overcome many limits of 'traditional' public opinion surveys. One of these limits is the lack of time and information a respondent receives before answering any survey question. This limitation is especially visible when the topic addressed in a survey is novel or complex, as is usually the case with new technologies. Traditional survey methods generally do not allow people to explain why they think in a certain way and to suggest improvements to the current state of affairs. The aim of a citizen summit is to gain insight into what informed citizens think about certain controversial matters, to unveil their political priorities, and to inform policy makers about alternatives for action. Participants are confronted with specific dilemmas, but there is also time for discussion and to allow new ideas freely emerge.

During such citizen summits, citizens learn what experts and stakeholder groups think, why and how those opinions differ, and which aspects other citizens may consider. By comparing all these viewpoints, citizen summit participants can gain a deep understanding of the issues discussed, yet still have the time to express considered judgments. By integrating the information provided with their own values, worldviews and life experience, **people can express informed opinions and make thoughtful suggestions**. Deliberative results provide a crucial reality test against which decision-makers can, for example, compare the views of competing stakeholder groups, each of whom claims to represent the public interest. The citizen summit is a way of letting the voice of citizens be heard by decision makers and policy makers at the local, national or regional level, as appropriate for the topic[13].

5.1.2 The engine of the discussion

The SurPRISE project organised two series of participatory events: large-scale Citizen Summits and small-scale Citizen Meetings. The name differentiates between the two series of events, in terms of the number of citizens involved as resource intensity in terms of costs and time.

Based on the participatory methodology applied during the large-scale citizen summits and the preliminary results of this first series of events, a web-based system was developed[14] called SurPRISE Decision Support System (DSS). The main purpose of this system is to provide an inspiring innovative infrastructure to help to facilitate discussions with citizens on surveillance-orientated security technologies (SOSTs) in a standardised way. The main technical and non-technical characteristics of the SurPRISE DSS tool is summarised in Figure 2.

[12] Detailed description of the methodology used in the SurPRISE project and detailed description of SurPRISE Decision Support System (DSS) can be found in the following deliverables of the project:
D1.4 Method description decision support test cases
D7.3 SurPRISE decision support web-tool

[13] For topics like global warming or biodiversity citizen consultations were organised on a global level too, see http://www.wwviews.org/ for more information.

[14] The IT development was partly based on the Dessi tool: http://securitydecisions.org/

This tool can be perceived as the ‘engine’ of the discussion phase of a participatory research about SOSTs. It is important to emphasise that the SurPRISE DSS can be used only if it is embedded in the wider process of a research, using the participatory methodology (see Figure 3).

The SurPRISE DSS facilitated the second series of participatory events within the Surprise Project, the abovementioned small-scale Citizen Meetings. The similarity of the main findings of the two series of participatory events validates the relevance of the participatory design and the SurPRISE DSS.

Non-technical characteristics	Technical characteristics/requirements
➢ It helps to involve many people (the number of parallel table discussions are not limited) ➢ It is flexible, it can be customised depending on the particular objectives of the research ➢ It inspires opinion sharing and constructive debates ➢ It stimulates the formulation of recommendations ➢ It provides in-depth understanding of the arguments and opinions of citizens ➢ It generates quantitative data as well (the statistical relevance of the quantitative results depend on the sample size and the representativeness of the sample) ➢ It is standardised (discussions ran at different tables, in different countries, about different options or technologies can be easily compared) ➢ It is transparent (participants can follow on a second monitor what the note-taker enter into the system) ➢ It provides immediate output and facilitates prompt feedback	➢ Internet-based solution, hence Wi-Fi and broad band internet access is needed ➢ Open source, which has the benefit of easy adaption to different needs ➢ Laptop on each table is needed ➢ A second screen is needed, on which table companions can follow how they formulate their messages and recommendations (this is a rather flexible requirement since other solutions/workarounds may be possible) ➢ User-friendly translation module, hence the DSS is easy to use in cross-national projects (it is currently available in seven European languages: English, German, Italian, Spanish, Danish, Norwegian and Hungarian)

Figure 2: The main technical and non-technical characteristics of SurPRISE DSS

5.1.3 Possibilities for future use

The participatory methodology facilitated by the SurPRISE DSS can be used for different purposes in the field of surveillance and security technology assessment[15] in order to understand the attitudes, requirements, needs and priorities of citizens, whose security is – finally – supposed to be improved by the discussed technologies.

Examples and ideas for a future use of the SurPRISE DSS include:

- Reflecting on decision processes, focused on the use of some kind of particular surveillance-based security technology (selection between alternative technologies and/or non-surveillance based solutions);
- When the implementation of a surveillance-orientated security technology is being considered in order to improve public security (e.g. a smart CCTV system is planned to be used in a particular district of a city in order to increase public security; biometric identification is planned to be introduced at the entrance of particular public institutions; drones are planned to be used by the police to control large mass moves events such as demonstrations);

[15] The SurPRISE DSS can easily be adapted for more widely use in participatory social scientific research and support of decision-making involving citizens. Footnote 8 contains links to reports describing the methodology and the web-tool and its adaptability in more detail.

- Before ordering or supporting particular security technology developments of the security industry;
- By the security industry, to research developing technologies that take into consideration the requirements of a wider public already from the very beginning of technology development (the involvement of citizens in early development can support Privacy by Design (PbD) and privacy enhancing solutions);
- Developing security strategies at different levels (e.g., on community, county or country level);
- Developing security-related plans regarding some kind of special field such as border security, public transport, fight against terrorism, enforcing traffic rules, etc.;
- When considering developments or changes of the legal framework, legal safeguards or control processes related to the use of SOSTs in general or in particular, considering a given technology or a specific use;
- Supporting communication and transparency regarding security technology and policy in general
- Providing a general decision support process in the field of surveillance-orientated security technologies, when limited resources make it impossible to have large-scale participatory citizen summits.
- When specific issues, opinions, paradoxes or concerns have emerged from previous studies but have remained unclear or difficult to understand;
- When policy makers are facing an especially controversial debate on the implementation of new security measures.

5.2 SurPRISE DSS within the participatory methodology and the decision making

Figure 3 provides an overview on the place of the participatory methodology and the SurPRISE DSS in the complex process of decision-making regarding surveillance-based security technologies. It should be emphasised that the "voice of the citizens", despite being depicted only as one element influencing the decision-making process, has an outstanding importance, because the final objective of all the decisions is to enhance the security and the well-being of the citizens.

The participatory research can be effectively used in strategy development or decision-making, where it can be assured that the results of such research will not be misused and interpreted in a way so that it would support other stakeholders' interests. To prevent such misuse, it is important that the participatory research is completed by independent research professionals. Further, some kind of control over dissemination of the results should be secured. An unbiased research could be realised or at least supported e.g., by involving data protection NGOs and independent experts prior and during the decision-making process and by pre-testing the quality and balance of the information material. In addition, it must be ensured that the participants well represent the different segments of the citizens whose security is aimed to be improved by the measures envisaged.

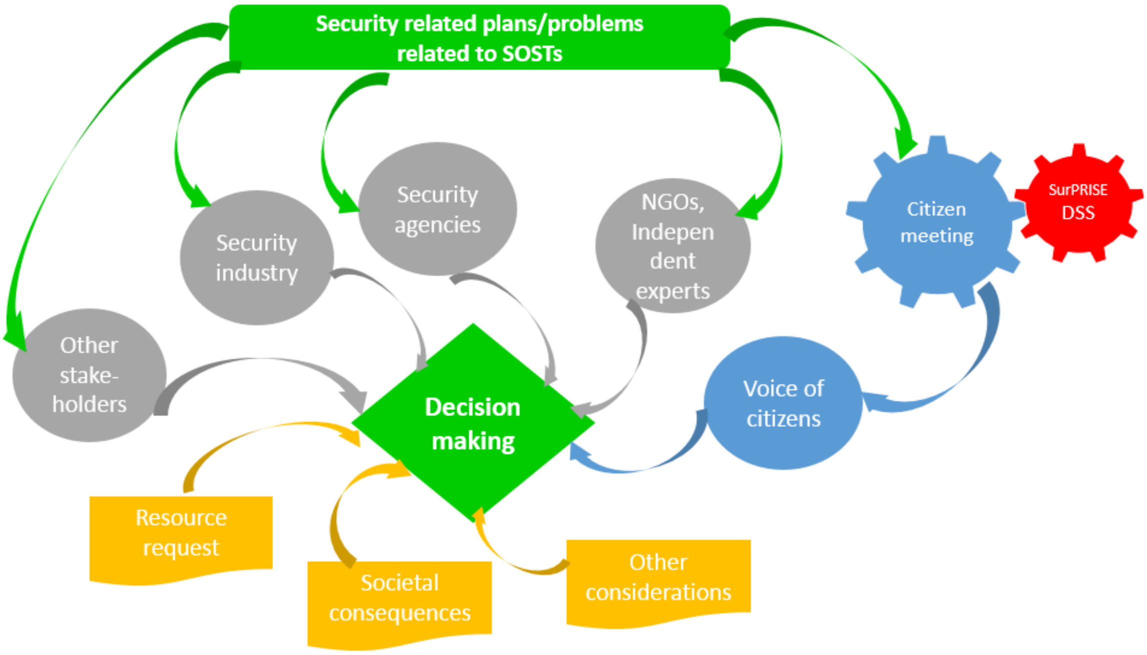

Figure 3: Contribution of citizens to decision making

5.3 Checklist of items and steps required to involve citizens

Elements needed to organise a citizen summit/meeting are listed below. The main steps of the whole process are shown in Figure 4.

- SurPRISE DSS adjusted to the specific requirements of the topic
- Definition of the target group (depending on the purpose of the research)
- Demographic quotas and methodology how to reach them (it is important that each main layer of the target group would be represented proportionately in the citizen consultation)
- Information booklet about the topic that will be discussed during the summit, including the different pros and cons of the particular solutions, the opinions of different stakeholder groups (it is crucial that the information material is unbiased; to this effect, its neutrality should be tested during pilots in advance to finalise it)
- Information material (this provides citizens with information about the project and a description of how to apply to participate)
- Invitation letters (sent out with the information booklet)
- Premises where the summit is held, with suitable acoustics and enough space to prevent groups from disturbing one another
- Round tables with 7-9 chairs
- Availability of human resources needed during the events: head facilitator, table moderators and note takers, staff to take care of registration, catering, contact to external contractors, participants needs…
- Preparation and adjustment the Webtool, provision of technical background (see Figure 2) and personnel responsible for it
- Drinks and food (as the event lasts 3-3,5 hours)
- Large screen and projector if there are materials to project or electronic voting system is used
- Voting system: electronic or paper based
- “Postcards” and “post-box” for individual recommendations that can be formulated any time during the event

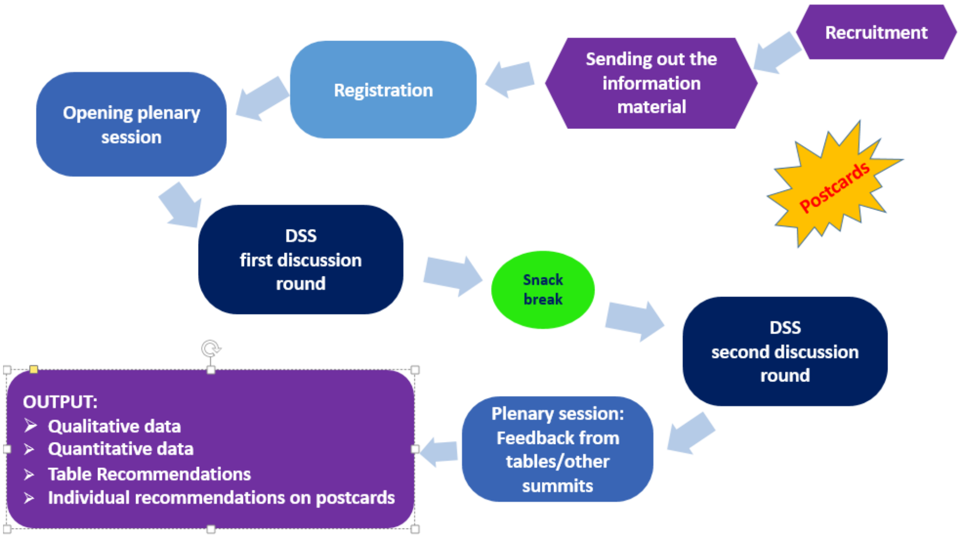
Recruitment
Sending out the information material
Registration
Opening plenary session
Postcards
DSS first discussion round
Snack break
DSS second discussion round
Plenary session: Feedback from tables/other summits
OUTPUT:
Qualitative data
Quantitative data
Table Recommendations
Individual recommendations on postcards

Figure 4: Overview of the participatory process

5.4 Discussions during the citizen consultations

Participants of the citizen summit or meeting share and confront their views with fellow citizens in groups of 6-8 people sitting around tables. The citizens' consultations, and consequently, the SurPRISE DSS, consist of two discussion rounds (see Figure 4).

The main characteristic of the first discussion round:

- It is similar for each group of table/summit/country of the particular research
- Besides open discussion topics, it includes questions for individual evaluation; these data - in addition to the qualitative analysis of the discussions and recommendations - can be statistically processed if the sample size makes it reasonable, (even if not, these data provide precious supplementary information in the analysis)
- Follow-up questions can be included to better understand the differences in individual voting results/opinions
- Instructions for table moderators and the note takers can be included
- Qualitative techniques can be used for better understanding participants attitudes
- The structure is flexible and can be reshaped according to the specific topic (in case of the SurPRISE-project, we utilised this possibility to better understand and to supplement the large scale results)

The main purpose of the second discussion round is to foster deliberation and recommendations. Features of this round include:

- Different groups at the same event do not necessarily discuss the same technology (e.g., more than one technology can be discussed)
- The main discussion is structured into different focus areas such as the assessment of positives and negatives of the technology, effectiveness, intrusiveness, acceptability, the trustworthiness of the security agencies using the discussed technology, legal safeguards, alternative possibilities, and so on. The number of dimensions can be increased or decreased according to the purpose of the research.
- The structure of each focus area is the same: first, a general question opens the debate, after which the participants try to find some common ground for a recommendation or a message to politicians. Transparency is ensured by the second monitor at the table – the participants can always see what the note taker writes down in the DSS. Then the group gives a meaningful title to the message, and finally, the section is closed with a group-voting about the initial question.

5.5 Analysis

The head facilitator can use the DSS to control the progress of each tables already during the event, and its output can be retrieved from the DSS immediately after the event. The output consists of:

- the notes taken by note-takers during the discussions,
- the recommendations formulated in the discussions within the different focus areas of the second table discussion round,
- the individual recommendations and messages formulated on postcards, and
- the data from the answers to the questions provided for individual rating in the first discussion round and for group-rating in the second.

Taking into consideration all the different outputs of the analysis, the main attitudes and requirements of the citizens can be understood, and thoughtful recommendations can be formulated for decision makers. The strength and relevance of the citizens' recommendations can be increased if, before finalising them, they are discussed with different stakeholders and experts who have a broader view on the problem. This additional phase of the research project can help researchers arrive at a final, refined formulation of the research results that include feasible recommendations which clearly support the interest of citizens and ensure that these requirements would not be misunderstood or misused to suit the interests of certain stakeholder groups. In the SurPRISE project, besides this additional phase, the final recommendations also took into account the theoretical work conducted by expert research[16] prior to the empirical phase.

5.6 How to start one´s own project

The SurPRISE DSS can be used as a tool facilitating your own participatory research project. It can be reached via the following link: http://surprisetool.teknoproject.org/en/.

A user guide is provided to the DSS in D7.3 SurPRISE decision support web-tool.

D1.4 Method description decision support test cases is another relevant deliverable, offering additional and useful information on how to set up the participatory research process.

Personal help can be received via the following links:

- Lars Klüver (Danish Board of Technology): lk@tekno.dk
- Márta Szénay (Medián Opinion and Market Research): szenay@median.hu

[16] These works are published in deliverables of WP2 and WP3:
D2.4 Vincenzo Pavone, Sara Degli Esposti, Elvira Santiago: Report on key factors
D3.1 Eva Schlehahn, Marit Hansen, Jaro Sterbik-Lamina, Javier Sempere Samaniego: Report on surveillance technology and privacy enhancing design
D3.2 Maria Grazia Porcedda, Martin Scheinin, Mathias Vermeulen: Report on regulatory frameworks concerning privacy and the evolution of the norm of the right to privacy
D3.3 Regina Berglez, Reinhard Kreissl: Report on security enhancing options that are not based on surveillance technologies

6 Conclusions

The years since the turn of the millennium have been characterised by dramatic changes in both the objectives and the means of security policies. The proclaimed war on terror after 9/11 2001 is a clear landmark of this development, although it denotes rather an accelerator of longer-term tendencies than a real turning point. These tendencies comprise political and societal developments of securitisation as well as technical progress in information technologies, creating unprecedented possibilities of data collection and surveillance. The attacks of 9/11 and subsequent acts of terrorism were exploited to make actual use of the surveillance capabilities offered by technology, obviously to a literally unlimited extent as the revelations made by Snowden on global surveillance programs conducted by the NSA uncovered.

The growing focus on pre-emption and proactive measures, resulting in increasing investments in surveillance capabilities, was predominantly based on an assumed trade-off between security on the one hand, and liberty and privacy on the other hand. Accordingly, more security requires infringements of privacy and related fundamental rights, and less privacy is almost automatically linked to more security. Although such an approach endangers key values and fundamental rights, characterising and constituting democratic societies, it informed security policies during the last decades and is still dominating security-related investments and measures to a large extent. The use of SOSTs for mass surveillance purposes is obviously eroding liberties and values it pretends to defend, nevertheless related programs remain largely untouched and unchanged, despite clear conflicts with fundamental rights and lack of evidence for their effectiveness.

The results from the involvement of about 2000 citizens from nine European countries in participatory assessment activities of SOSTs conducted by the SurPRISE project, confirm the scepticism against the trade-off approach in general and, in particular, as a suitable guideline for decision-making related to security policy. The participants of the Citizen Summits and Citizen Meetings predominantly requested strict limitations and regulations with regard to the use of surveillance technologies. These requests are largely in line with related conclusions and recommendations developed by high level expert groups, e.g., Opinion n°28 - 20/05/2014 – Ethics of Security and Surveillance Technologies[17] of the European Group on Ethics in Science and New Technologies (EGE) or the "The Right to Privacy in the Digital Age" report of the Office of the United Nations High Commissioner for Human Rights[18]. The recommendations are also in accordance with core objectives of the upcoming regulation and directive on personal data protection, thus supporting their adoption by the Council and the Parliament.

Participating citizens requested that the protection of privacy and personal data by updated regulations should be strictly enforced, both in the context of commercial and law enforcement activities. For this purpose they demanded that authorities responsible for the protection of privacy should be equipped with sufficient resources and include which comprise the international transfer of data and activities of law enforcement or intelligence agencies. The implementation and use of SOSTs should be targeted and accompanied by proper and strict safeguards. The use of surveillance technologies should be justified and justifiable on a case-by-case basis; blanket mass surveillance is not accepted.

Trust into institutions conducting surveillance was regarded as a key factor for acceptability. In this context the request for limitation of surveillance activities to public authorities was raised; involvement of private actors should be strictly limited and regulated. Participants requested enforced and increased accountability, liability and transparency as measures to create trust and to prevent abuse. They also wish to be actively informed about how they can protect their privacy in view of new information technologies, and in particular of SOSTs.

Another key demand concerned safeguards that SOSTs developed, implemented and used in an effective and fundamental rights respecting way. SOSTs should therefore be subjected to comprehensive technology assessments, comprising also privacy impact assessments, and mandatorily integrate technical and organisational measures for the privacy compliant operation. A comprehensive

[17] http://ec.europa.eu/archives/bepa/european-group-ethics/docs/publications/ege_opinion_28_ethics_security_surveillance_technologies.pdf

[18] http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc

technology assessment calls for a participative approach, i.e. the involvement of citizens in assessment and decision-making processes.

Last but not least the participants requested a more comprehensive, holistic and long-term approach to security, demanding a stronger focus on root causes of insecurity, i.e. tackling the enormous economic and social injustices resulting from the persistent economic crisis in Europe. SOSTs should not replace but only be used in combination with non-technological measures and social strategies addressing the social and economic causes of insecurity. A stable socio-economic environment is an essential precautionary measure not only against minor crimes but also against increasing violent radicalisation on an individual as well as on a political system level. Listening to the voice of citizens would therefore reduce the need for surveillance to and thus also lessen resulting risks for privacy and related fundamental rights, fostering democratic and societal development in line with European values.

7 List of Figures

Figure 1: Overview of tasks and responsibilities 2
Figure 2: The main technical and non-technical characteristics of SurPRISE DSS.................... 27
Figure 3: Contribution of citizens to decision making 29
Figure 4: Overview of the participatory process.................... 30

8 List of Tables

Table 1: Factors influencing acceptability of SOSTs (statistically significant) 23
Table 2: Factors influencing acceptability of SOSTs (statistically not significant) 23
Table 3: New and emerging factors likely to influence SOSTs' acceptability
(to be tested in future research). 24

9 List of Abbreviations

Abbreviation	Definition
AEPD	Agencia Española de Protección de Datos
CCTV	Closed circuit television
CJEU	Court of Justice of the European Union
DG JUST	Directorate-General for Justice
DPA	Data Protection Act
DPI	Deep Packet Inspection
DSS	Decision Support System
EACEA	Executive Agency for Education, Audiovisual and Culture
EC	European Commission
ECJ	European Court of Justice
EFTA	European Free Trade Association
EGE	Ethics in Science and New Technologies
ENISA	European Union Agency for Network and Information Security
EU	European Union
FRA	Agency for Fundamental Rights
ICT	Information and communications technology
INI	International Nitrogen Initiative
IoT	Internet of the Things
IT	Information Technology
JTRS	Joint Transparency Register Secretariat
NGO	Non Governmental Organisation
NSA	National Security Agency
PACITA	The Parliaments and civil society in Technology Assessment project
PbD	Privacy by Design and Privacy by Default
PIA	Privacy Impact Assessment
PTA	Parliamentary Technology Assessment
SLT	Smartphone Location Tracking
SOST	Surveillance-oriented security technology
TA	Technology assessment
UN	United Nations
US	United States
WP29	Article 29 Working party