SurPRISE was a large-scale participatory project to assess the reasons for citizens to accept or not security technologies in Europe. The project examined how citizens consider surveillance orientated security technologies *(SOSTs)* and whether they consider and accept that more security implies less privacy.

SurPRISE was a three-year collaborative research project under the European Union Framework 7 Security Research Programme, running from 2012-15.

This policy brief is directed towards European policymakers on the EU and national level. It also contains important information and recommendations for decision makers in security policies and in the implementation of security technologies and measures. The results of the SurPRISE project are particularly relevant for the Council of the EU and the European Parliament responsible for the European data protection reform.

Is Privacy the Price for more Security?

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 acceleration 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 from 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.

In this context a core objective of SurPRISE was to re-examine the relationship between security and privacy. This relation is commonly positioned as a 'trade-off', and accordingly infringements of privacy are regarded as an acceptable or necessary 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, and led to the growing focus on pre-emption and proactive measures, resulting in ever more increasing focus on improving surveillance capabilities.

surprise

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

Contacts:
Coordinator: Johann Čas
Institute of Technology Assessment
at the Austrian Academy of Sciences
Strohgasse 45/5, A-1030 Wien
E-Mail: info@surprise-project.eu
Web: www. surprise-project.eu

ITA INSTITUTE OF TECHNOLOGY ASSESSMENT ÖAW Austrian Academy of Sciences

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

However, an emergent body of scientific work and public scepticism question the validity of the security-privacy trade-off. In response to these developments, SurPRISE investigated the relation between surveillance, privacy and security from a scientific as well as citizen's perspective. Major aims of SurPRISE were to identify criteria and factors, which contribute to the shaping of security technologies and measures as acceptable, effective, non-privacy-infringing and socially legitimate security devices in line with human rights and European values, and to develop policy recommendations based on recommendations provided by about 2000 citizens from nine European countries. The involvement of citizens constituted an essential element of the identification of criteria and factors and of the formulation of policy recommendations. Two types of participatory events were organised and conducted by SurPRISE, large-scale "Citizen Summits" and small-scale "Citizen Meetings". Citizen Summits involved on average about 200 citizens per country, and were full day events, with alternating phases of receiving information, discussing the topics and emerging issues in small groups, electronic voting and formulating recommendations to policymakers. Citizen Meetings allow the involvement of citizens in decision-making in small-scale participatory events. Citizen Meetings are a

Policy Brief

decision support system[1] developed by SurPRISE. This method of participatory involvement was tested in five countries with about 200 participants; the results were integrated into the analytical work and the development of policy recommendations.

Recommendations

The results of 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[2] 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[3]. The recommendations are also in accordance with core objectives of the upcoming data protection regulation and directive.[4]

The development of the recommendations encompassed several steps. An essential contribution came from citizens participating in the Citizen Summits and Meetings. Their recommendations were integrated in and enriched by academic research and expertise within and external to SurPRISE.

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.

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.

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.

---

1 See the SurPRISE factsheet for a brief introduction into the decision support system (DSS) developed and tested by SurPRISE. It is available on the SurPRISE website http://surprise-project.eu/.

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

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

4 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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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 evalu-

ating 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

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.

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.

Details, backgrounds and suggestions for implementing all these recommendations can be found in the final policy paper D6.13 on the project's website:
http://surprise-project.eu/dissemination/research-results/

Criteria and factors determining the acceptability of security technologies

In the following lists the main findings on factors and criteria influencing the acceptability of SOSTs are briefly summarised.[5] 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.

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.

Some of the most interesting results 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. List 3 contains the most relevant of these additional factors.

5 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.

List 1 – Factors influencing acceptability of SOSTs

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.

List 2 – Factors not influencing acceptability of SOSTs

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.

List 3 – New and emerging factors likely to influence SOSTs' acceptability (to be tested in future research)

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).

List 4 – 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.

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.

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. Surveillance orientated security technologies should not replace but only be used in combination with non-technological measures and social strategies addressing the social and economic causes of insecurity.

For more information please contact the coordinator:
Johann Čas
Institute of Technology Assessment at the Austrian Academy of Sciences
Strohgasse 45/5
A-1030 Wien
Austria
info@surprise-project.eu
www. surprise-project.eu

The Consortium

Institut für Technikfolgen-Abschätzung,
Österreichische Akademie der Wissenschaften, Austria

Agencia de Protección de Datos de la Comunidad de Madrid,
Spain

Instituto de Politicas y Bienes Publicos,
Agencia Estatal Consejo Superior de Investigaciones Científicas, Spain

Teknologiradet – The Danish Board of Technology Foundation,
Denmark

European University Institute,
Italy

Verein für Rechts- und Kriminalsoziologie,
Austria

Medián Opinion and Market Research Limited Company,
Hungary

Teknologiradet – The Norwegian Board of Technology,
Norway

The Open University,
United Kingdom

TA-SWISS, Centre for Technology Assessment,
Swiss Academies of Arts and Sciences, Switzerland

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein,
Germany