INSTITUTE OF TECHNOLOGY ASSESSMENT

ITA-DOSSIER

Less privacy for more security?

In brief

- New surveillance technologies allow ever deeper observation of the lives of each individual.
- Security measures are increasingly reliant upon surveillance technologies, based on the claim that more security requires infringements of fundamental rights.
- Citizens have more nuanced views: although the use of surveillance technologies is not rejected as such, it remains a contested issue. Therefore their utilisation should be limited categorically and strictly regulated and controlled.
- The protection of personal data needs to be improved and ensured, also the case of security technologies. In addition, security should remain a public sector responsibility and social root causes of insecurity need to be addressed and solved.

What is it about?

From a technical view, the limits to surveillance have all but disappeared. The use of advanced information and communication technologies generates enormous amounts of data on individual preferences and behaviour. For example, data on participation in professional and private networks, subjects of personal interest, political attitudes or sexual orientation can all be collected and stored from Internet searches, websites visited, and activities in social networks or from motion profiles, generated by the use of mobile technologies. These data are of high interest both for commercial reasons and for issues of security. The capabilities of surveillance technologies are rapidly increasing: intelligent video surveillance systems are able to identify persons or to interpret their behaviour. Drones add mobility to video surveillance and allow for the scanning of large areas or for the inspection of individuals in an unnoticeable manner.

Terrorism is certainly an important factor that has contributed to the development and proliferation of surveillance technologies. However, there are also societal and political developments as well as economic interests responsible for making unrestricted use of the possibilities offered by technology. Obvious infringements of fundamental rights are in part consciously accepted. The generosity of revealing personal data in social networks is misinterpreted as a complete consent to the infringement of privacy. In times of policies minted by economic liberalism, maintaining social security is often regarded as a hindrance to economic competitiveness, rather than as a central objective of a civilised society. The desire for security focuses on other areas, even if this implies the full transparency of our day to day lives and deep infractions on human liberty. The security research programme of the EU links security objectives to industrial policy, hence reinforcing tendencies to prefer technical solutions.

Only a small minority of participants accept infringements of privacy as a trade-off for more security.

The relationship between security and privacy plays a substantial role in decision-making on the use of surveillance technologies. The dominant assumption is that more security necessarily implies less privacy. But is this assumption always valid? Is it possible to increase security with loss of privacy? Is this necessarily the case or are there alternatives to increasing security which are not based on constant and all-pervasive surveillance? How can security really be maintained and improved in the long run?
In the SurPRISE project citizens played a central role in helping answer these questions. About 2000 individuals from nine European countries were invited to participate in citizen summits to discuss advantages and disadvantages of specific surveillance technology areas. Based on comprehensive information provided in advance, they also debated the relationship between security and privacy in general. The participants held votes on specific issues and developed in small groups policy recommendations.

Basic data

Project title:	SurPRISE – Surveillance, Privacy and Security
Project team:	Čas, J., Peissl, W., Krieger-Lamina, J., Strauß, S. in international consortium coordinated by ITA.
Duration:	02/2012 – 01/2015
Funded by:	EU FP7, Grant Agreement 285492
Website:	surprise-project.eu

Key results

The results differ considerably, both between the participating countries and the three technology areas discussed: intelligent video surveillance, smart phone location tracking and deep packet inspection (DPI), a technology capable to survey the Internet traffic entirely, also being deployed for the revealed spying activities of the NSA.

About four out of five Austrian participants consider themselves to be living in a safe country. Regarding concerns that surveillance technologies are entrenching privacy, Spain is leading with about 90%, followed by Austria and Germany. In contrast, with hardly 40% Hungary showed by far the lowest share of participants reporting to be burdened by this issue.

Citizens debating about surveillance technologies

Almost two thirds of participants agreed to the statement that surveillance technologies improve public security. On the other hand, 70% believed that these technologies are likely to be misused once they are implemented.

One third of the participants agreed to the statement “If you have nothing to hide, you have nothing to fear”. However, even among the proponents of this frequently used justification for surveillance more than half are concerned that too much information is being collected and that it is being used to their disadvantage without their consent.

Essential for the acceptance of surveillance technologies is trust in the institutions that are implementing them. The level of perceived security has, contrary to expectations, no significant impact on acceptance.

One further important factor is aim and scope of surveillance measures: mass surveillance without real suspicion is considered unacceptable. Technologies for which it is well-known that they are highly vulnerable to abuse or systems in which computer-based decision-making replaces humans are also rejected. The outsourcing of security tasks to private organisations as well as the exchange of data between the public sector and private companies are also strongly criticised.

What to do?

The citizen summits produced about 300 policy recommendations. The SurPRISE project team and external experts summarised them to 16 requests, grouped in the following four core strategic areas:

- **Improvements in data protection in general:** This area concerns the adaptation and further development of data protection legislation to manage challenges raised by technical progress, and the provision of sufficient resources for data protection authorities to enforce existing regulations effectively. This protection should also include the transfer of data to non-EU countries.
- **Development of protective mechanisms for the deployment of surveillance technologies:** Regulatory mechanisms shall guarantee that restrictions to fundamental rights are legitimate; and that their deployment is justifiable and compatible with democratic principles, and necessary and in proportion to the solution of urgent security problems. The collection and processing of data needs to be restricted and based upon concrete suspicion and to serve explicit and well-defined purposes. Mass surveillance is to be excluded.
- **Security should remain the responsibility of the public sector:** If the involvement of private organisations cannot be avoided in surveillance practices, regulations to protect the privacy of citizens should be strictly adhered to. To increase transparency citizens should participate in decision-making on the utilisation of surveillance technologies and the implementation of surveillance measures.
- **Focus on root causes of security loss:** Economic and social policies should be implemented to address fundamental causes of criminality, radicalisation and terrorism. In this context, a more just distribution of labour and incomes is regarded as an essential precondition for political stability and social coherence in Europe.

Further reading

SurPRISE Policy Brief (February 2015):
surprise-project.eu/wp-content/uploads/2015/03/policy_brief3.pdf

Contact

Johann Čas

E-mail: tamail@oeaw.ac.at

Phone: +43(1)51581-6582

IMPRINT: Owner: Austrian Academy of Sciences; Legal person under public law (BGBl. 569/1921 i.d.F. BGBl. I 130/2003); Dr. Ignaz Seipel-Platz 2, A-1010 Vienna; Editor: Institute of Technology Assessment (ITA); Strohgasse 45/5, A-1030 Vienna; oeaw.ac.at/ita/en. | Frequency: The ITA-Dossiers are published irregularly and publish the research results of the ITA. The ITA-Dossiers are published in print in small numbers only and are made available open access to the public via the Internet portal “epub.oeaw”: epub.oeaw.ac.at/ita/ita-dossiers | ISSN: 2306-1960 | This work is licensed under a Creative Commons Attribution 4.0 International License: creativecommons.org/licenses/by/4.0/ | ITA-Dossier no. 17, November 2015 | epub.oeaw.ac.at/ita/ita-dossiers/ita-dossier017en.pdf |
Co-authors: W. Peissl, J.Krieger-Lamina, S. Strauß