"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 6.10 – Citizen Summits on Privacy, Security and Surveillance: Synthesis Report

Lead Beneficiary: ITA/OEAW

Author(s): Stefan Strauß (ITA/OEAW)

Due Date: August 2014

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

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

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

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

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

Executive Summary

This document presents the major findings and implications from the large-scale citizen participation processes conducted in the SurPRISE project. A main objective of these participatory events was to investigate how European citizens perceive the interplay between privacy, security and surveillance in relation to the employment of surveillance oriented security technology (SOST) and the related practices. Although citizens are directly affected by security and surveillance measures employed in their countries, their views and opinions on these issues are widely unknown. To narrow this gap, citizen summits[2] were conducted in each of the countries involved in SurPRISE (Austria, Denmark, Germany, Hungary, Italy, Norway, Spain, United Kingdom, and Switzerland). To gain deeper insights into the opinions of the participants the methodology combined quantitative and qualitative elements, i.e. a set of pre-defined questions and statements clustered in different topics as well as discussion rounds in these thematic blocks. Three different SOSTs (smart CCTV, deep packet inspection – DPI and smart phone location tracking – SLT) were addressed at the citizen summits as concrete examples representing issues affecting different types of privacy such as visual, communicational and locational privacy, all of which can be expected to become issues of wider societal concern. The analysis is based on a mix between general and specific aspects to explore general attitudes and opinions on security and privacy as well as how these are linked to specific perceptions regarding the three SOSTs such as their effectiveness and intrusiveness, related views and concerns of the citizens. The content presented in this document is the outcome of the analysis of the quantitative and qualitative data gathered from the total sample and provides the overall synthesis at European level.

The report is structured as follows:

After a brief introduction section 2 presents an overview on policy relevant issues on security and privacy in the European context including major challenges of the EU security strategy, shifts in security policy as well as regulatory issues concerning privacy and data protection oversight. Section 3 describes the methodology and process design of the citizen summits and the basic structure of the total sample. In section 4, the main results on the citizens' perceptions on privacy, security and surveillance are presented; and section 5 sketches and highlights the major outcome of the table discussions and recommendations. Finally, summary and concluding remarks are presented in section 6.

The interplay between privacy, security and surveillance has undergone several changes in the last two decades. Security policy on a global level has shifted towards a wide-ranging conceptualisation of security that includes many different contexts and domains. During the 1990s the concept of human security emerged that put more emphasis on the individual than the traditional security concept before the end of the cold war. This changing role of security had impact on security strategies and policy-making on a global level and to some extent developed a momentum of its own. An extended framing of security together with an increasing demand for a holistic security approach aiming at tackling more complex security challenges strained the original idea of human security and partially led to a mixture of different security domains. This paradigm shift in security policy is the effect of so-called securitization, where security is framed as a holistic concept spanning across a wide array of different domains. Security becomes more and more framed as an ever-changing concept closely linked to political discourse. Security measures in such a framing become arbitrarily subject to politics and are at risk of becoming self-referential means that lack in effectiveness to tackle security threats, pressing societal challenges and endangering privacy protection.

Potential and given tensions between privacy and security intensify with an accelerating dynamic security landscape that increasingly employs surveillance technologies. The assumed trade-off between privacy and security contributes to reinforce a strained relation: it is based on the assumption that the employment of security measures per se requires privacy intrusion in order to come to a certain level of

[2] Individual country reports, the material produced and used for the different events and video documentations of the summits are available at: www.surprise-project.eu.

security. This logic inherently does as if privacy intrusions would be the only and inevitable option to effectively improve security. Consequently, the view of security measures is also narrowed down as it is neglected that there might be other non-intrusive or less intrusive options that do not intrude into privacy. In short, this model suggests that if one accepts security and surveillance measures, one has also to accept privacy intrusions.

The results of the citizen summits show that most of the participants do not follow this argument: citizens neither want to fear security measures nor lose their privacy. They deem the view on a trade-off between privacy and security inappropriate because both the effectiveness of security measures and the protection of privacy suffer from such a view as the perceived high intrusiveness of SOSTs decreases its perceived effectiveness. Citizens are aware that SOSTS are to some extent important and necessary to ensure public security. The effectiveness of SOSTs was not per se doubted but is overshadowed by high concerns and uncertainties due to a perceived lack of control, information and accountability as well as fears about abuses of power, function and mission creep. Citizens see a number of serious threats to privacy by extensive surveillance practices aided by technology that go beyond SOST-specific concerns. Here, the interrelations between effectiveness and intrusiveness of a technology play an important role. A trade-off is not necessarily given but only in cases where the effectiveness of a security measure cannot be gained without privacy intrusion. However, in this case, it needs to be assessed whether there are no other options to receive the effectiveness and to what extent privacy intrusion is necessary and if it is in accordance with the law. The results regarding intrusiveness and effectiveness of the SOSTs indicate that this is a crucial issue for citizens. Even if it is assumed that SOSTs benefit security, concerns about privacy intrusions are mostly rated higher than their effectiveness (sections 4.3, 4.4). The high concerns about information collection and abuse of personal information indicate that people are more concerned about trading their information than accepting such a trade (sections 4.4, 4.6). Contrary to a trade-off the citizens clearly expressed demand for both: effective security measures that are in accordance with an effective protection of their privacy.

This is closely related to trust which is a core issue in society and the relationship between citizens and institutions. However, the results (section 4.8) show that trust in institutions employing security and surveillance measures is heavily strained and lacks a foundation. Due to increasing surveillance tendencies together with lack of information and transparency of security authorities and SOSTs, there is little trust in laws and regulations (section 4.8 and 5). The abuse of power is among the highest expressed fears and the rule of law is perceived as crucial instrument against the abuse of power. However, it is barely trusted in terms of effectiveness. Closely related to that is a perceived lack of accountability and oversight of security authorities and surveillance practices. People would like to trust but perceive a lack of common grounds on which to build their trust. This is aggravated by perceptions that security and surveillance measures implemented by the relevant authorities are based on mistrust in the citizens. As a consequence, citizens feel more insecure and uncertain about SOSTs and security authorities themselves. There is a strong demand for a reconsideration of different perspectives that respects privacy and security more as complementary issues that are not in a natural conflict.

In order to alleviate this situation, an urgent need was identified to improve mechanisms that control the work of security authorities and ensure that their actions are in compliance with fundamental rights. A great degree of uncertainty regarding trust in institutions employing SOSTs derives also from the discussions and recommendations as the vast majority expressed unease and concerns about information abuse, extensive and uncontrolled power. A large number of citizens said to feel exposed to mass surveillance. Many concerns relate the tenet whereby innocent people should not be subjected to intrusive measures, referring to the presumption of innocence, which is a core principle of justice systems. Participants express fear that mass surveillance may erode this principle, and that as a consequence everybody could become suspicious. Hence, a gap between surveillance under known or plausible suspicion and untargeted surveillance of the masses was seen as critical problem. To deal with this problem, many argued there ought to be more control over surveillance activities, and there is demand for justified grounds to target real suspects and criminals instead of the general public. Mass surveillance is also perceived as inefficient, in that it raises costs, errors and brings little security benefits. Citizens request greater prior evaluation (and accordingly information) of purposes, appropriateness, costs and impacts of SOSTs and surveillance practices, pursuant to the principle of proportionality. Hence participants request investing more in transparency and accountability in order to control and verify what data and information is being collected, who is responsible and allowed to gather and use it

and for what purposes they are intended and why. A need for more strict laws to control the implementation of SOSTs and practices was identified. This also refers to an implementation of evaluation frameworks for security and surveillance measures to check these against the rule of law and accordance with fundamental rights. More precisely, privacy by design and default as pivotal technology feature and privacy impact assessments prior to technology usage are needed. The demand for more effective legal privacy frameworks in Europe supports the adoption of the proposed data protection reform in the European Union. The expressed need for more checks and balances and effective control mechanisms to ensure that SOSTs and related practices are in line with fundamental rights indicates some need to reinforce already existing safeguards and the institutions in charge of implementing existing regulations. Particular need was expressed for independent oversight bodies able to scrutinize the proper use of security technologies and related practices within the limits of the law. Such bodies should safeguard privacy and data protection, and less intrusive security measures in accordance with fundamental rights. In this regard national and European DPAs play an important role. The outcome of the citizen summits provides support to facilitate the partially difficult situation of DPAs regarding competences and resources and upgrade the capacities of DPAs and other oversight bodies. In general, a turn away from mass surveillance and a reinforcement of checks and balances with more effective oversight are core issues to restoring security measures to a more acceptable level in order to regain the trust of the citizens and to move towards approaches that consider the complementary character of privacy and security.

Besides the identified need for change in security policy and the implementation of the appropriate measures it also became apparent that there is a certain need to focus more on root causes of security matters. European citizens are mostly concerned about the economic crisis, the related instabilities in national and international economies, as well as social insecurity. While pre-emptive security and surveillance measures gain high priority, measures to tackle issues on root causes and social and economic inequalities seem to be underestimated and not sufficiently addressed by policymakers in the views of the citizens. This was particularly underlined in those countries affected more by the economic crisis (such as Italy or Spain, section 2.4). To some extent this refers to a spill over effect in a sense that the despair and anger about the difficult economic situation in the countries was also expressed in the summits. However, this by no means implies that the expressed concerns and fears about privacy infringement can be relativized. Especially not because these privacy concerns are widely similar across all countries; including those that encounter less serious economic issues. What this implies is that for the citizens, issues such as economic stability, employment, and social coherence are of vast importance for security and safety. Citizens here identified a need for more political actions on these issues that might contribute to reducing social insecurity.

The recommendations that were proposed cluster around major themes, synthesized in the following:

- Reducing and constraining surveillance technologies and practices
- Improving checks and balances and prohibiting mass surveillance
  - Security measures must be limited and targeted, and the use of SOST must be backed by judicial authorizations
  - Enhancing compliance of law enforcement authorities with fundamental rights principles
  - Reinforcing independent data protection authorities to scrutinize security and surveillance measures
- Enhancing transparency, information and participation
  - Increasing accountability of bodies pursuing security and implementing surveillance measures
  - Involving civil society and human rights bodies in the elaboration of security policies
- (Re-)considering the human factor
  - Strengthening social cohesion, economic justice and social responsibility of institutions and individuals

  - Raising awareness and education among the public on privacy and security issues
  - Investing in training and greater expertise of security authorities and personnel
- Fostering privacy research and innovation
  - Fostering innovation for privacy by design as integral components of technologies
  - Strengthening security and privacy standards (e.g. encryption) in technology development and usage
  - Fostering the role of science and research particularly as regards alternative approaches

Above all, the major recommendation and demand of the citizens includes a reduction of surveillance, improvement of transparency, accountability and democratic scrutiny of SOSTs and practices, of the involved authorities as well as more checks and balances to re-establish a solid foundation of mutual trust.

1 Introduction

The complex interplay between surveillance, privacy and security is at the core of the SurPRISE project. The increasing role of this interplay is visible in a number of public discourses and controversies about the use of surveillance-oriented security technology (SOST) and related practices. Governments in Europe and worldwide are confronted with an increasingly complex global security landscape that led to incremental paradigm shifts in security policies, strategies and the employment of the according measures. Linked to this wider transformation of security policy is an increase in the use of SOSTS in many different domains as security measures often rely on technology. The foundation of contemporary security policy is mostly based on a model that frames privacy and security as a trade-off. Such a framing suggests that there is an inherent conflict between these two concepts and that for security improvements one has to accept privacy intrusions. If the relation between privacy and security is presented and understood in that way, it is rather difficult to consider to what extent both concepts might be complementary and on the same side of the coin. Thus, instead of asking how privacy can and should be protected, it is often merely asked whether privacy should be protected at all. This misses the point and as a consequence it is neglected that both values – privacy and security – are essential elements in the societies we live in. One challenge is therefore to find approaches that conciliate both values without losing either. The way in which security and surveillance measures are employed has societal impact and directly affects citizens. However, little is known so far about the views and opinions of citizens on these issues. The main focus of SurPRISE is thus to reduce this gap and to further explore the interrelations between surveillance, privacy and security with a particular focus on the perceptions of European citizens in this regard. For this purpose, large-scale participatory processes with about 200 participants each were conducted across the nine countries involved in the project, each with a similar setting. The main aim of these citizen summits was to learn more about citizens' perceptions on the interrelations between privacy, security and surveillance.

Objectives of this report

This report presents the major findings derived from these large-scale citizen summits and is structured as follows: Section 2 provides a brief overview on security and privacy in the European context including shifts in security policy and issues concerning privacy and data protection regulation. The methodology and process design of the citizen summits as well as the basic structure of the overall citizen panel are described in Section 3. Section 4 presents the main results on the citizens' perceptions on privacy, security and surveillance, whereas the major outcome of the table discussions and recommendation rounds is highlighted in Section 5. The final section 6 provides a summary and concluding remarks. The analysis is based on the quantitative and qualitative data gathered from the total sample and provides the overall synthesis at the European level. This report can be understood as a hub between Deliverable 2.4 that provides a sociological analysis of the overall sample of the citizen summits so as to understand the factors and criteria for acceptance of surveillance-oriented security technologies and the Deliverable 6.13 that focuses on policy implications derived from the overall results.

2 Security and privacy in the European context[3]

The role and meaning of security has significantly changed since the 1990s after the end of the Cold War. Increasingly complex problems on a global scale reinforced the demand for conceptualisations of security that correspond to developing suitable approaches to tackle security threats and challenges. During the Cold War, a traditional state-centred security was the dominating concept: "*For forty years, the major world powers entrusted the security of their populace, and to a certain extent of the world, to a balance of power among states. (…) This type of security relied primarily on an anarchistic balance of power (power as the sole controlling mechanism), the military build-up of two superpowers, and on the absolute sovereignty of the nation-state. (…) Security was seen as protection from invading armies; protection was provided by technical and military capabilities; and wars were never to be fought on home soil – rather, proxy wars were used if direct combat were necessary.*"[4] During the 1990s, this traditional security concept was complemented by a new approach focussing more on the individual than on the national state. In 1994 the UNDP introduced the new concept of human security as an aspect of international policy in its Human Development Report[5]. The report describes human security as having two principal aspects: the freedom from chronic threats such as hunger, disease and repression, coupled with the protection from sudden calamities. In 2000, Kofi Annan[6] highlighted human security as something that "*in its broadest sense, embraces far more than the absence of violent conflict. It encompasses human rights, good governance, access to education and health care and ensuring that each individual has opportunities and choices to fulfil his or her potential. Every step in this direction is also a step towards reducing poverty, achieving economic growth and preventing conflict. Freedom from want, freedom from fear, and the freedom of future generations to inherit a healthy natural environment – these are the interrelated building blocks of human – and therefore national – security.*"[7]

This description already pointed towards a broadened view but it emphasized reducing insecurities for ensuring human development in line with freedom and health. However, in later policy, this emphasis seems to have further broadened towards claims for a holistic concept where human security became used as "an effort to re-conceptualize security in a fundamental manner"; a framework where "(...) mitigating threats to the insecurity of individuals becomes a central goal of policy recommendations and actions."[8] The paradigm shift in security policy over the last two decades changed the role of security and related policy measures towards a comprehensive conceptualization of security. This also affected the original concept of human security as the already blurry distinction between different meanings of security related to different domains became further challenged. This transformation already occurred before the dramatic terrorist attacks on September 11 2001. However, 9/11 lead to a further change in security policy on a global scale as the US and many other governments significantly reinforced security and surveillance measures[9]. An extended view on security is visible on a global scale as well as in the European Security Strategy, which tended towards a combination of a holistic security

---

[3] Parts of this section refer to: SurPRISE Deliverable 2.3 Strauß, S & J. Čas, J (2013): D 2.3 – Major security challenges, responses and their impact on privacy – selected security-oriented surveillance technologies.

[4] T. Owen (2004): Challenges and opportunities for defining and measuring human security, in: Human Rights, Human Security and Disarmament, disarmament forum 2004 Vol 3. 15-24. p.16

[5] United Nations – UN (1994): New dimensions of Human Security. Human development report 1994, United Nations Development Programme, New York, Oxford University Press.

[6] peace nobel prize winner and former Secretary-General of the United Nations until 2006

[7] Kofi Annan "Secretary-General Salutes International Workshop on Human Security in Mongolia." Two-Day. Session in Ulaanbaatar, May 8-10, 2000. Press Release SG/SM/7382. Cited from http://www.gdrc.org/sustdev/husec/Definitions.pdf

[8] R. Jolly and D. B. Ray (2006): "The Human Security Framework and National Human Development Reports: A Review of Experiences and Current Debates". United Nations Development Programme, National Human Development Report Unit. p. 5

[9] Cf. K. Ball and F. Webster (2003): The intensification of surveillance. London: Pluto. K. D. Haggerty and M. Samatas (eds.) (2010): Surveillance and democracy. Routledge-Cavendish, Oxon. D. Lyon (2003): Surveillance after September 11. London:Polity.

concept and multilateral approach, where tackling new threats, extending the zone of security around Europe and strengthening international order are among the strategic objectives[10].

The attempt to integrate different domains and sectors into a holistic concept of security is ambitious. On the one hand, this approach corresponds to globalization and the need to cooperate beyond national borders on a supra- and international level towards common security strategies. On the other hand the conflation of intertwined but different roles and meanings of security in distinct domains complicates the efforts to develop appropriate security strategies to deal with emerging challenges. Buzan et al (1998) identified five distinct but intertwined sectors that play a strong role in the security discourse[11]: the military, political, economic, societal and environmental sector. As each of these sectors follows its own mechanisms and logics, the role, meanings, and measures in the realm of security might deviate significantly in each sector. With an integrative view on once different security concepts, these different logics are at risk of being neglected. The strive for a comprehensive security concept might complicate an informed distinction of security domains to develop appropriate measures; and together with technological push it might also entail the seductive assumption that in any case security challenges would be manageable preferably by technological means.

From a theoretical stance, this paradigm shift in security policy is the effect of what many scholars termed the process of securitization.[12] Securitization entails the framing of security towards a holistic concept that spans across a broad scope of different domains; security is conceptualized from a process view that is "marked by the intersubjective establishment of an existential threat with sufficient saliency to have political effects"[13]. In this process, security is not framed as an objective condition but is linked to political discourse[14]. Securitization makes security policy an arbitrary subject to politics. It is linked to political rhetoric and thus creates its own dynamics where the informed need for security measures to address threats becomes decoupled from serious considerations on appropriate responses. This is visible in the security strategies of many European countries as well as the European Union. The security strategies involve a broad spectrum of different security challenges such as poverty, diseases, climate change, energy supply, terrorism and organized crime. However, the focus of measures to deal with these challenges seems to lie mainly on terrorism and crime which then appear in further policy. While without any doubt each of these challenges needs to be addressed with appropriate measures, a lacking distinction between different roles of security can complicate the task to develop these measures. Due to its own particular dynamics, the process of securitization can lead to a "security continuum" addressing the problem of "political structurization or securitization of certain persons and practices as 'threats'" in a rather pragmatic manner[15]. With securitization, a broader range of political issues are framed in security terms. Securitization becomes particularly problematic if it reinforces security discourses in a way that communicates security as a dominant issue of societal concern deserving higher priority compared to other state functions and duties, and the protection of fundamental rights such as the right to privacy. Several scholars point out that the linking of security and (im)migration is a

---

10 G. Quille (2004): The European Security Strategy: A Framework for EU Security Interests? In: International Peacekeeping, Vol.11, No.3, Autumn 2004, pp.1–16 http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede20040728_ess_/sede20040728_ess_en.pdf

11 B. Buzan, O. Weaver, J. de Wilde (1998): Security: A New Framework for Analysis. Lynne Rienner: Boulder, 1998.

12 Cf. B. Buzan, O. Weaver, J. de Wilde (1998) op. cit.
D. Bigo (2000): "When two become one: Internal and external securitisations in Europe." In: International Relations Theory and the Politics of European Integration. Power, Security and Community. M. Kelstrup and M. Williams (eds.), London, Routledge, pp. 171-204.
T. Balzacq (2005): The three faces of securitization: Political agency, audience and context. In: European Journal of International Relations 11(2): 171-201.
S. Watson (2011): The 'human' as referent object? Humanitarianism as securitization. In: Security Dialogue 42(1):3-20. DOI:10.1177/0967010610393549

13 S. Watson (2011) op. cit., p. 3

14 T. Balzacq (2005): The three faces of securitization: Political agency, audience and context. In: European Journal of International Relations 11(2): 171-201. p. 173

15 E. Guild, S. Carrera, T. Balzacq (2008): The changing dynamic of security in an enlarged European Union. Research paper No. 12, The changing landscape of European Liberty and Security – www.ceps.eu http://aei.pitt.edu/11457/1/1746.pdf p. 2

prominent example for the dangerous effects of securitization.[16] In such a framing, security issues often become presented as existential threats that require particular "measures and justifying actions outside the normal bounds of political procedure"[17]. Core problems of securitization in general are that security and related measures can become equivocal and might be introduced for self-serving purposes that undermine sound evaluation of security in relation to other policy objectives. In other words: playing the "security card" tends to trump concerns about civil liberties and human rights. The result can be conflicting interests and lacking public acceptance and increasing resistance against security policy. Inherent is the danger that security becomes self-referential without focussing on reducing realistic risks and threats or is misused to justify other political objectives.

Partially related to the paradigm shift towards human-centred security there is a tendency to turn away from the traditional separation between external/foreign (e.g. peace missions, military engagement) and internal/domestic security (e.g. fighting crime, ensuring public order, political stability). The boundaries between internal and external security become increasingly blurred. This transformation of security is also visible in European security policy. In the European Union, a closer coordination and cooperation between actors from both vantage points is explicitly supported.[18] Stronger coherence between the internal and external dimensions of security and exploiting synergies between internal and external policies is highlighted in the EU security policies as an important cross-cutting issue.

2.1 The security strategies of the European Union

The European Union deals with a number of security challenges that are highlighted in the European (external and internal) security strategies[19]. The external strategy titled '*A Secure Europe in a Better World*' of 2003[20] was the Union's first attempt to define the European security environment. It highlights the following key security challenges:

- Terrorism
- Proliferation of weapons of mass destruction
- Regional conflicts
- State failure
- Organised crime.

The strategy also points out the relation between security and economic development: "Security is a precondition of development. Conflict not only destroys infrastructure, including social infrastructure; it also encourages criminality, deters investment and makes normal economic activity impossible"[21] The named challenges and the associated measures of the strategy have been widely continued. This was inter alia suggested by a review in 2008 which identified a need to be more capable, coherent and active as regards unfolding the potential of the security strategy[22]. To achieve this goal several approaches are intended such as increasing threat prevention, strengthening coherence with improved institutional co-operation, partnerships for effective multilateralism particularly the EU's strategic partnership with the NATO, more strategic decision-making and exchange of information. This course was further reinforced by increasing links between the internal and external dimensions of security and fostering data

[16] E.g. G. Karyotis (2011): "*The fallacy of securitizing migration: elite rationality and unintended consequences*". In: G. Lazaridis (ed.): Security, Insecurity and Migration in Europe. Ashgate, Surrey, Great Britain, pp. 13-30. See also M. Ibrahim (2005): "The Securitization of Migration: A Racial Discourse". In: International Migration, Vol. 43 (5), pp. 163-187.

[17] B. Buzan, O. Weaver, J. de Wilde (1998) op. cit. p. 23 f.

[18] Cf. F. Trauner (2011): "The internal-external security nexus: more coherence under Lisbon? European Union Institute for Security Studies Occasional paper 89, March 2011.

[19] http://eeas.europa.eu/csdp/about-csdp/european-security-strategy/index_en.htm

[20] European Commission (2003). A Secure Europe in a better World – European Security Strategy. http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf

[21] Ibid, p. 2

[22] European Commission (2008): Report on the Implementation of the European Security Strategy – providing security in a changing world. http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/EN/reports/104630.pdf

exchange between different law enforcement agencies to support mutual cooperation, such as between CSDP[23] police missions and Europol. This also aims at exchanging personal data between these institutions.

In line with the intention for "internal security with a global perspective" the internal security strategy[24] widely follows the direction of the external strategy. The five main issues for internal security are (1) serious and organised crime, (2) terrorism, (3) cybercrime, (4) security of EU borders and (5) natural and man-made disasters. To cope with these challenges, strategic objectives represent responses to the most urgent challenges to EU security:

- Disrupt international crime networks
- Prevent terrorism and address radicalisation and recruitment
- Raise levels of security for citizens and businesses in cyberspace
- Strengthen security through border management
- Increase Europe's resilience in crises and disasters

These issues are regarded as issues of utmost concern to any European country. Each of these domains addresses a number of different security threats and challenges to be tackled to ensure a free and secure society. Ensuring human security is essential to guarantee the development of an inclusive, active and participative society, free from fear, uncertainty, and violence. Although the urgency and relevancy of these problems may appear straightforward to many, approaches and strategies to address these matters may differ substantially across regional areas.

A variety of security measures and technologies have been developed and implemented as a response to these threats. Such as an increasing use of biometric technologies, growing amounts of databases and information systems for law enforcement (e.g. Schengen and Visa Information System, Eurodac) and increasing data exchange. In fact, each threat, which is a challenge from a policy-making point of view, has been addressed and tackled through a complex bundle of measures, some of them centred on technological tools and others on social policy actions; such as the ratification and implementation of instruments for judicial and law enforcement cooperation and information exchange, the Data Retention Directive, mutual assistance in criminal matters and the Prüm decisions.[25]

2.2 Paradigm shifts in European security policy

Seen from a wider angle, there are shifting paradigms observable in the course security policy has taken. Not least due to the Tragedy of 9/11 and other terrorist attacks, there is a growth in security and surveillance activities perceivable on a global scale. In Europe, this shift becomes particularly visible in The Hague Programme and its ideological premise[26]:

> *The security of the European Union and its Member states has acquired a new urgency, especially in the light of the terrorist attacks in the United States on 11 September 2001 and in Madrid on 11 March 2004. The citizens in Europe rightly expect the European Union, while guaranteeing respect for fundamental freedoms and rights, to take a more effective, joint approach to cross-border problems such as illegal migration, trafficking in and smuggling of human beings, terrorism and organized crime, as well as the prevention thereof… . The programme seeks to respond to the challenge and the expectations of our citizens*[27].

---

[23] CSDP stands for Common Security and Defence Policy.

[24] European Commission (2010). Communication from the Commission to the European Parliament and the Council - The EU Internal Security Strategy in Action: Five steps towards a more secure Europe. Brussels. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF#page=2

[25] European Commission (2011): First Annual Report on the Implementation of the EU Internal Security Strategy. COM (2011) 790 final. P. 5.

[26] E. Guild, S. Carrera, T. Balzacq (2008) op. cit.

[27] European Commission, Communication on The Hague Programme: Ten priorities for the next five years – The partnership for European renewal in the field of Freedom, Security and Justice, COM(2005) 184 final, Brussels. http://ec.europa.eu/home-affairs/doc_centre/docs/hague_programme_en.pdf

Together with the Treaty of Prüm[28], the Hague Programme has significantly changed the normative and political settings of liberty and security in the European Union and thus played a central role in altering how security is framed in Europe. This framing differs very much from its predecessor the Tampere Programme, where "shared commitment to freedom on human rights, democratic institutions and the rule of the law" were seen as common values that "have proved necessary for securing peace and developing prosperity in the European Union"[29]; or in other words: a complementary understanding of security in accordance with freedom (or more precisely liberty) and fundamental rights. In contrast, the Hague Programme entailed an expansion, predominance and strengthening of the security dimension over the other rationales of freedom and human rights. As a consequence, this change of strategic focus became part of a number of further policy documents among EU member states such as the currently effective Stockholm Programme[30]. These policies provided a strong political impulse towards common supranational security responses such as 'Provisions on Police and Judicial Cooperation in Criminal Matters' that is also part of the Treaty of the European Union. A significant increase of databases and information systems for law enforcement is a major part of this intensified cooperation. The Area of Freedom, Security and Justice (AFSJ) plays a particular role for European security strategy in this regard. It represents a set of policies focusing on strategic security issues and security related international data transfers. The Stockholm Programme inter alia aims at "greater coherence among external and internal elements of work in the area of freedom, security and justice" such as Europol, Eurojust, etc.[31] In line with the ongoing reform of EU data protection regulation, in 2012 the European Council brought in a proposal for data protection in law enforcement to regulate data processing 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".[32] Critics argue that while generally welcoming the reform, several rules of the proposal were insufficient and weaken the protection of personal data, e.g. as regards data transfer and profiling.[33]

In general, there seems to be a "difficult relationship between EU and intergovernmental processes in the area of security policy, which is primarily manifested in the form of challenges to the EU 'from below' by certain member states", as Guild et al (2008) argue.[34] The mentioned policies and agreements refer to this (at least to some extent) strained relationship. The AFSJ plays an important role in this regard as it reflects the shift in security framing: since its establishment in 1999 (on the basis of the Amsterdam Treaty) its foci changed significantly. Especially the Prüm treaty paved the way for intensified information exchange for law enforcement among the EU member states. It inter alia enabled the use of DNA profiling and fingerprint databases. The agreements of the Prüm treaty thus entailed a variety of critical aspects. According to Guild et al (2008) it "has created a hierarchy and a multilevel game within the EU" and "by focusing on data exchange, the Convention has provoked competition with the 'principle of availability' proposed by the Commission and The Hague Programme. By reverting to an intergovernmental arena, it excludes the European Parliament at a time when its role in democratic scrutiny is critical. (…) [B]y developing new mechanisms of security that operate above or below the EU level (or both), it has dismantled trust and confidence among member states. Finally, by establishing a framework whose rules are not subject to parliamentary oversight, the Prüm Treaty impacts on the EU

---

28 Council of the European Union, Prüm Convention Brussels January 7 2005 http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf

29 European Council, Tampere European Council 15 and 16 October 1999 Presidency Conclusions http://www.europarl.europa.eu/summits/tam_en.htm

30 European Council, Communication on Delivering an Area of Freedom, Security and Justice for European citizens - Action Plan implementing The Stockholm Programme. COM(2010) 171 http://www.statewatch.org/news/2010/apr/eu-com-stockholm-programme.pdf

31 Ibd

32 Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 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, Brussels, 25.1.2012, 2012/0010 (COD)] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF

33 See e.g. EDRI (2012): European Digital Rights (EDRI) EDRi's Position on the Directive https://dpreformlawenforcement.files.wordpress.com/2012/12/edri-position-papers-directive1.pdf

34 E. Guild, S. Carrera, T. Balzacq (2008) op. cit. p. 6

principle of transparency"[35]. Transparency and accountability are key principles to enable public scrutiny. A lack of such in security policy makes it difficult to scrutinize and evaluate security measures and whether they are in accordance with privacy and other fundamental rights.

2.3 Overview on privacy regulation and oversight[36]

While the previous sections deal with security policy this section now provides a brief overview on privacy regulation and oversight bodies. In Europe, fundamental rights protection is based on three complementary frameworks: the European Convention on Human Rights (ECHR)[37], the Charter of Fundamental Rights of the European Union (EUCFR)[38] and the general principles of the EU Treaty (TEU) (Article 6 refers to the ECHR and the EUCFR). At national level, European countries implemented their own laws, which in case of EU member states refers to these frameworks and most non-member states at least refer to the ECHR[39].

As a fundamental right, privacy is naturally part of these legal frameworks. The right to privacy was established as a fundamental right for the first time in 1948 in Article 12 of the Universal Declaration of Human Rights (UDHR): *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*

While the core of the right to privacy to protect from interference remains, the role of privacy and data protection has changed in the course of time. Technological progress has increased the demand for privacy regulation in accordance with the requirements of the information society. Law makers have tried to respond accordingly to the changing legal requirements. This is visible in the EUCFR which widely corresponds with ECHR but incorporates more the technological changes of the last 60 years. Attempts to cope with technological progress were already made much earlier: in 1981 the Council of Europe adopted the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) which was and still is "the only legally binding international instrument in the data protection field."[40] Thus, Convention 108 bears potential for creating an international data protection standard at a global scale. Efforts in this regard are currently in progress.[41]

The main legal instrument for privacy and data protection in the EU is Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (data protection directive)[42]. The data protection directive was adopted in 1995 in order to harmonize data protection law in the EU and to substantiate and expand the principles of Convention 108. It determines a minimum standard for all member states that their national laws have to fulfil. The EU law defines personal data as information that relates to an identified or identifiable person.[43] This means that either a person's identity is clear or can be ascertained by gathering additional information. Hence, for the data protection law to be applicable it is sufficient that a person concerned of data processing (data subject) is identifiable, directly or indirectly. In line with the principle of limited retention of data the EU law obliges to store data "in a form which permits identification of data subjects for no longer than is necessary for the

35 ibd. p. 8

36 For a detailed analysis of legal aspects see SurPRISE D3.2: M. G. Porcedda, M. Scheinin, M. Vermeulen (2013): D3.2 – "Report on regulatory frameworks concerning privacy and the evolution of the norm of the right to privacy".

37 Council of Europe: European Convention on Human Rights http://www.echr.coe.int/Documents/Convention_ENG.pdf

38 Charter of Fundamental Rights of the European Union http://ec.europa.eu/justice/fundamental-rights/charter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF

39 In 1953, the ECHR came into force which states have to comply with. In order to have a judicial institution for safeguarding the ECHR the European Court of Human Rights (ECHR) was created in 1959. The Court safeguards that states act in compliance with the ECHR; in case of human rights violations, individuals, groups of individuals, NGOs or legal persons can bring in complaints to the ECHR.

40 European Union Agency for Fundamental Rights – FRA (2014): Handbook on European data protection law, p. 16.

41 ibid

42 Data protection directive http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=DE

43 Data protection directive Art. 2(a)

purposes for which the data were collected or for which they are further processed."[44] This implies that data that does not serve its initial purpose has to be deleted or otherwise has to be anonymized[45]. Data are anonymized if all identifying elements are eliminated and none of the information left allows re-identifying the person concerned.[46] Regarding the type of personal data the law distinguishes between different categories. In the Convention 108 (Article 6) and the Data Protection Directive (Article 8) the following categories are named: personal data revealing racial or ethnic origin; personal data revealing political opinions, religious or other beliefs; trade union membership, personal data concerning health or sexual life. These sensitive data need special protection and processing is thus only allowed under specific safeguards as "by their nature, may pose a risk to the data subjects, when processed"[47]. Electronic data processed in the electronic communications domain are protected by a particular law, the e-privacy directive (2002/58/EG, last amendment with 2009/136/EC) which complements the data protection directive. It applies to the processing of data falling within the scope of EU law, in the context of publicly available electronic communications services, in public communications networks only, and thus undermines its potential scope of protection (as opposed to including a wider scope of internet services), further challenged by the repealing Data Retention Directive.[48] The data protection directive does not include issues regarding law enforcement. Hence, data protection in the AFSJ is addressed through other regulatory mechanisms mainly referring to Convention 108 as a basic benchmark[49]. The complex set of regulations includes the creation of different structures to monitor the implementation of data protection, such as data protection officers and different joint supervisory bodies for Europol[50] or Eurojust[51].

As regards the users of personal data the EU law distinguishes between data controller and processor. A data controller is an entity that "alone or jointly with others determines the purposes and means of the processing of personal data."[52] A data processor is a (legally separated) entity processing personal data on behalf of a controller. If a processor uses data for his/her own purpose then it becomes a controller as well. Third parties are natural or legal persons that use data but without acting on behalf of a controller. The law also foresees the possibility of a joint controllership but only under special legal conditions (i.e. where a legal basis for a common purpose of processing exists). An example for a joint controller is SWIFT (Society for Worldwide Interbank Financial Telecommunication) which represents a broader interpretation of the joint controllership by the Article 29 Working Party: SWIFT initially acted as processor for European banking institutions to handle banking transactions. As SWIFT disclosed transaction data to US located institutions (US Treasury department) it acted unlawfully as a controller. The Working Party concluded that the banking institutions as well as SWIFT represent joint controllers.[53] This case is particularly interesting as with the increasing information exchange between different (public and private) authorities also in international contexts, it becomes further complicated to ensure privacy and data protection.

---

44 Data protection directive Art. 6 (1) (e)

45 Anonymized data is not to confuse with pseudonymised data which only means that identifiers are replaced by pseudonymous information.

46 European Union Agency for Fundamental Rights (2014): Handbook on European data protection law, p. 44ff.

47 FRA (2014) p.43

48 M. G. Porcedda, M. Scheinin, M. Vermeulen (2013), op.cit. p. 13

49 http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

50 Europol (2012): Data protection at Europol. https://www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf

51 http://www.eurojust.europa.eu/Practitioners/Data-Protection/Pages/data-protection-officer.aspx

52 Data protection directive Art. 2 (d)

53 FRA (2014) op.cit., p. 49ff.

For safeguarding privacy and controlling the proper processing of personal data the following key principles of European privacy and data protection are crucial:[54]

- Lawful processing, i.e. the processing of personal data is in accordance with the law, for a legitimate purpose and necessary in a democratic society to realise the legitimate purpose.
- Purpose specification and limitation, i.e. the purpose of processing has to be defined before the processing begins and further use for other purpose must be based on additional legal basis (transfer of data to third parties is another purpose).
- data quality, i.e. relevancy (only data that are adequate, relevant, and not excessive related to the purpose), accuracy (data shall be accurate and up to date), limited retention (data have to be stored in a form permitting identification and for no longer than necessary) and fair processing of data (transparency of processing) have to be implemented in all processing operations.
- Accountability, i.e. controllers acting in compliance with data protection law and actively implementing measures to promote and safeguard data protection in their processing activities.

To ensure that these principles are respected and privacy is not abused, the law foresees supervisory bodies. On the European level, the following institutions are of particular relevance:

The **European data protection supervisor (EDPS)**[55] is the main oversight body created under regulation (EC) No. 45/2001. The EDPS has the responsibility to ensure that all EU institutions and bodies respect the right to privacy and process personal data within the legal frameworks. It advises EU institutions on all aspects of personal data processing and also promotes good practice in EU institutions. Individuals concerned of privacy abuse can bring in complaints to the EDPS.

The Data Protection Working Party on the protection of individuals with regards to the processing of personal data, i.e. the **Article 29 Working party (WP29)** was implemented in 1995 with Article 29 of the data protection Directive 95/46/EC. It is an independent advisory panel that has the main task to interpret "questions covering the application of the national measures adopted under the Directive". It issues opinions and gives (non-binding) recommendations about the applicability of the regulations defined in the directive. It consists of a representative of the supervisory authorities of each EU country, a representative of the authorities established for the EU institutions and bodies and a representative of the European Commission.[56]

The **European Union Agency for Fundamental Rights (FRA)**[57] was established by Council Regulation 168/2007. The FRA provides evidence-based expert advice to EU bodies and EU member states in issues regarding ensuring compliance with European fundamental rights. Its tasks also include information and awareness-raising of the public, and formulation of opinions related to privacy and data protection. The FRA also cooperates with European and international organizations such as the UN, OSCE or national human rights institutions.

The **Committee for Civil Liberties, Justice, and Home Affairs** (LIBE) is a parliamentary panel that supports the EU Commission in legislation concerning fundamental rights, justice and home affairs. LIBE is responsible for a number of legal and policy issues in these fields. It aims "at tackling issues of a common interest at the European level, such as: the fight against international crime and against terrorism, the protection of fundamental rights, ensuring data protection and privacy in a digital age, fighting against discrimination based on racial or ethnic origin, religion, belief, disability, age or sexual orientation".[58] As other parliamentary committees, the LIBE examines proposals for the commission and produces reports to be discussed in plenary sessions. It works closely with the commission, the council

---

54 Ibid, pp. 61ff.

55 European Data Protection Supervisor (2013) Annual report 2013 http://europa.eu/about-eu/institutions-bodies/edps/index_en.htm

56 http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

57 http://fra.europa.eu/en/about-fra

58 http://www.europarl.europa.eu/committees/en/LIBE/home.html LIBE newsletter 07 2014 http://www.europarl.europa.eu/document/activities/cont/201407/20140725ATT87324/20140725ATT87324EN.pdf

of ministers and national parliaments as well as representatives from judiciary, law enforcement, academics and civil society. According to its website the LIBE committee aims at establishing "fruitful dialogue with all interested parties and especially with citizens."[59]

While these public authorities deal with privacy and data protection in the European Union, the data protection authorities at national level in the countries mostly remain the major contact point for citizens and fulfil a crucial function for the effective implementation of the right to privacy and information. The resources of the DPAs in the countries are quite different as the following table shows:

Country	Population (Mio)	Personal resources federal DPA 2007	Personal resources (full-time equ.) federal DPA 2013	Approx. annual budget (federal DPA) 2013	Additionally, DPAs available at provincial level
Switzerland	8	20	28.5	€ 4.5 Mio	Yes
Norway	5.1	33	41	€ 4.7 Mio	No
Denmark	5.6	26	30	€ 2.8 Mio	No
Germany	80	67	86.5	€ 9 Mio	Yes
United Kingdom	58.8	265	360	€ 25.5 Mio	Yes[60]
Austria	8.4	20	22	€ 960.000[61]	No
Hungary	9.9	45	56	€ 1.6 Mio	No
Italy	59.7	100	104	€ 23 Mio	No
Spain	46.6	115	158	€ 15 Mio	Yes[62]

Table 1: Overview on resources of national DPAs[63]

While this overview on the resources does not give insights into the effectiveness of the DPAs a lack of resources has been identified for several years across the different countries. Despite of the increasing complexity of data protection issues, in some cases, there is no significant change in staff from 2007. The national DPAs themselves argue that this makes it increasingly challenging to fulfil their tasks. In a report the European Fundamental Rights Agency points out several problematic issues that complicate data protection in Europe:[64] as regards regulation, legal insufficiencies such as problems regarding compliance, lacking sanctions, compensation and legal consequences in case of privacy abuse were identified. These legal deficiencies affect the role and functioning of the DPAs and their limited scope of actions. Furthermore, a number of deficiencies are directly related to the structure, function and operation of the DPAs. Structural problems are given due to a lacking and complicated independence of

[59] ibid

[60] The Information Commissioner's Office (ICO) is the main authority for freedom of information and data protection. It also has offices in each province in UK that serve as local point of contact for the public and local organisations.

[61] Figures based on information from the Austrian Federal Chancellery https://www.vibe.at/node/131. In their annual reports, the Austrian DPA repeatedly argued to have lower resources than other European countries.

[62] Besides the federal DPA there are currently two at regional level, one in Catalonia and one in Basque Country. The Data Protection Agency of Madrid (APDCM) was terminated in 2012 as a result of the austerity measures adopted by the Regional Authority of the Madrid Community. Its competences and functions, as well as part of its staff, have been transferred to the Spanish Data Protection Agency.

[63] Figures provided by the consortium members gathered from their national DPAs and https://privacyassociation.org/media/pdf/knowledge_center/DPA11_Survey_final.pdf

[64] European Union Agency for Fundamental Rights - FRA (2010): Data protection in the European Union: the role of national Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II.

several bodies in the member states which raises concerns about the "effective capability of the officers of DPAs to perform their tasks in complete autonomy"[65] Similar to the DPAs themselves the FRA also highlights that "understaffing and lack of adequate financial resources among several supervisory bodies constitutes a significant problem"[66]. This also affects the operational level, where a lack of power and limited scope of actions hampers the DPAs across Europe to fulfil their tasks such as conducting investigations, effecting interventions during data processing operations, offering legal advice and engaging in legal proceeding, as foreseen in the Data Protection Directive. Recent studies conducted in the IRISS project dealing with transparency issues of the practices of data controllers and the role of DPAs in Europe revealed several problematic aspects and challenges towards a more effective implementation of the right to data protection and information such as lacking or insufficient responses to requests regarding the right to information and access to one's personal data.[67]

2.4 General public perceptions on major security challenges

In 2011, a Special Eurobarometer survey was devoted to the public perception of internal security. It serves as a starting point for identifying security challenges in the perception of citizens of the European Union. Special Eurobarometer 371[68] on Internal Security from November 2011 had the specific aim to compare the results from open and unprompted answers of European citizens with the security agenda set out in the EU Internal Security Strategy.[69] Each of the five challenges listed in the EU security strategy (serious and organised crime, terrorism, cybercrime, security of EU borders and natural man-made disasters; as outlined in the previous section) is included in the top-ranking perceived challenges of the citizens as shown in the figures below.

What do you think are the most important challenges to the security of (NATIONALITY) citizens at the moment?

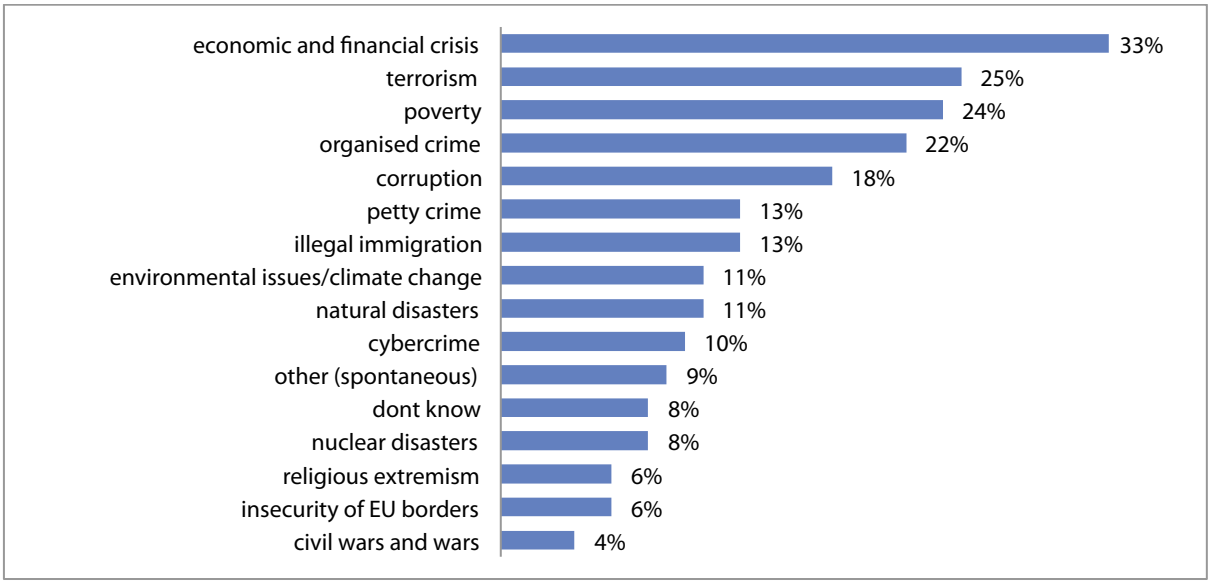

Figure 1: Europeans' views on challenges to national security

65 Ibid p.42
66 Ibid p.42
67 http://irissproject.eu/wp-content/uploads/2014/06/IRISS-WP5-Summary-Meta-Analyses-for-Press-Release.pdf
68 European Commission (2011). Special Eurobarometer 371 - INTERNAL SECURITY. Report Number 371.
69 European Commission (2010). Communication from the Commission to the European Parliament and the Council - The EU Internal Security Strategy in Action: Five steps towards a more secure Europe. Brussels. Op. cit.

What do you think are the most important challenges to the security of EU citizens at the moment?

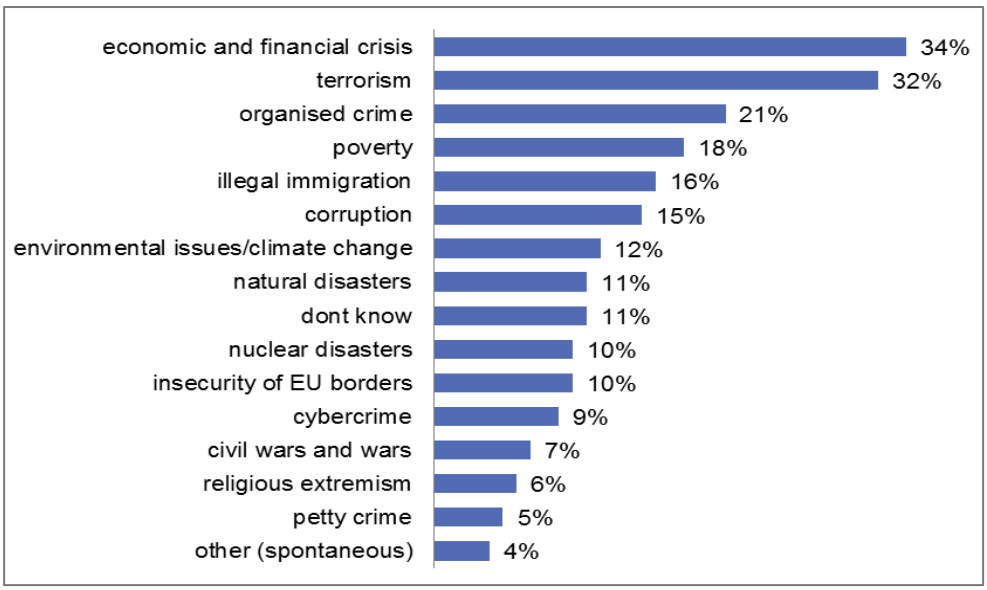

Figure 2: Europeans' views on challenges to EU security

As these figures reveal, the most relevant security challenges in the view of the citizens are similar on national and EU level and they differ from the prioritized challenges in the security strategy. The economic and financial crisis receives the highest ranking in both, the national and the EU perspective, and also poverty and corruption are rated as very important issues. Challenges on the environment and climate change also play an increasing role in EU member states. The dominance of economic challenges is confirmed by data from open surveys, which provide data over longer periods of time. The following graph shows an overview on how the most important issues from the EU citizens' point of view developed from 2003 to 2014.

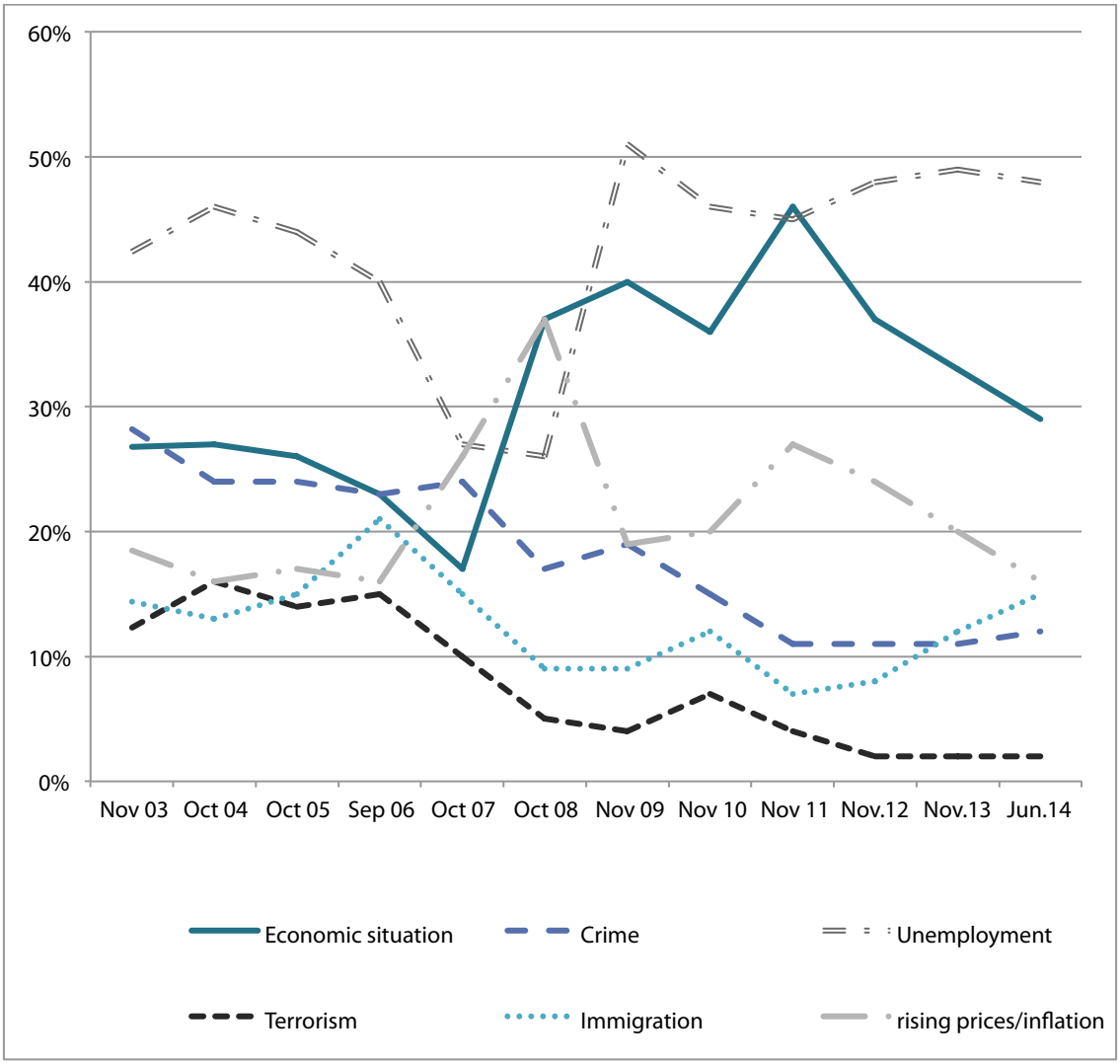

Figure 3: Long term perspective of Europeans on most important issues [70]

According to these time series, crime and terrorism have been relevant issues in the medium range but with a relatively constant fluctuation downwards. Crime has considerably diminished in importance (from 28 to about 12%), and also terrorism became less relevant and ranges between 4 and 2% since 2011. Immigration shows a rather similar development downwards in the range between 20% and 10%. Different trends are observable as regards economic issues such as the state of the economic situation (always being approximately in the range between 20 and 40%) or the levels of unemployment (in the range between 25 and 50%) which were continuously assessed as most important. Over the years a decrease of concerns regarding terrorism and crime is observable while economic issues are increasingly problematic in the perception of the EU citizens. Against the background of the financial crisis triggered in 2007/08, the entailed fluctuating economic situations and the high unemployment rates in Europe (see tables and figures below), the growing concerns in this regard are reasonable and obvious. Figure 4 shows how unemployment in Europe developed in the last fifteen years with a

[70] The chart is based on the responses to the question "What do you think are the two most important issues facing (OUR COUNTRY) at the moment? (MAX. 2 ANSWERS POSSIBLE)" from the Eurobarometer Interactive Search System results http://ec.europa.eu/public_opinion/cf/showtable.cfm?keyID=2212&nationID=16,&startdate=2003.11&enddate=2014.06 The presented issues are based on their average percentage value during the period from 2003 to 2014.

significant increase since the financial crisis. The vast importance of economic and societal challenges is also in line with the assessment of experts from different fields in the Global Risk Report of 2014[71]

Country	Unemployment rate 2014[72]
Switzerland	3.4
Norway	3.8
Germany	5.0
Austria	4.9
United Kingdom	5.9
Denmark	6.4
Hungary	7.4
Italy	13.4
Spain	23.9

Table 2: Unemployment rate in the countries involved in SurPRISE

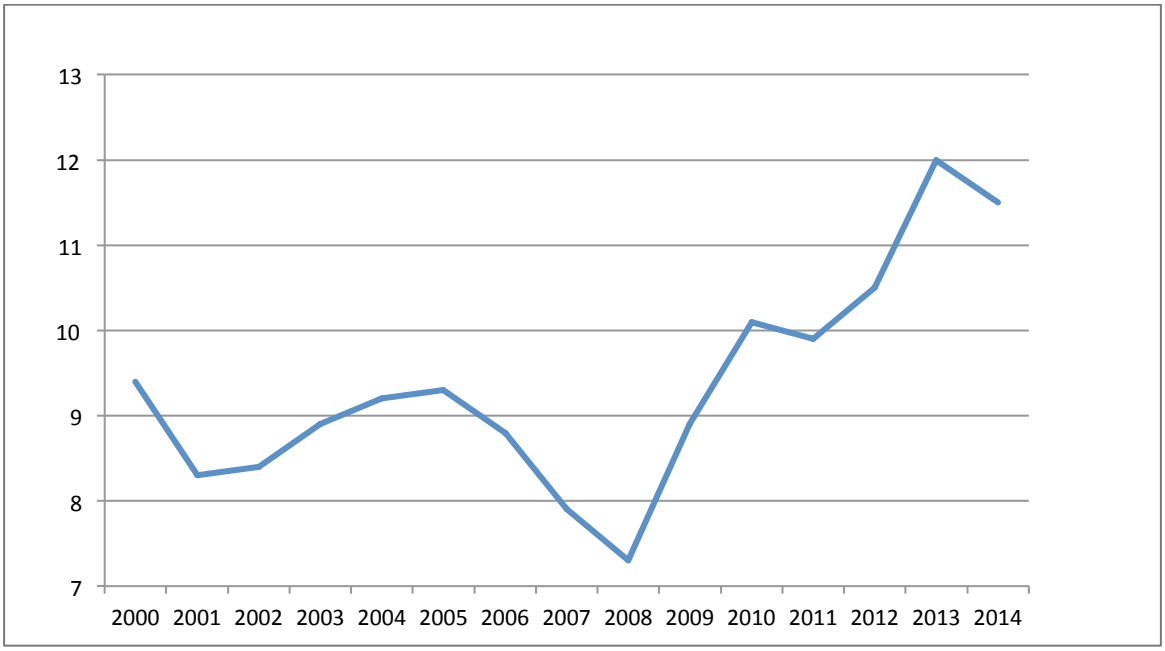

Figure 4: Unemployment rate in Euro area[73]

[71] World Economic Forum (2014): Global Risks 2014. Geneva, Ninth Edition. http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf

[72] Source: Eurostat news release euro indicators January 2015 http://ec.europa.eu/eurostat/documents/2995521/6454659/3-07012015-AP-EN.pdf/f4d2866e-0562-49f5-8f29-67e1be16f50a For Switzerland, rates based on http://ieconomics.com/unemployment-switzerland

[73] Source: http://ieconomics.com/europe-unemployment-rate Figures similar to Eurostat op. cit.

3 Methodology and process design of the citizen summits

At the core of SurPRISE is the implementation of large scale participatory processes in each of the nine countries (Austria, Denmark, Germany, Hungary, Italy, Norway, Spain, Switzerland, United Kingdom) involved in the project. The methodology is an innovative technology assessment approach that combines qualitative and quantitative data gathering to get a bigger picture of citizens' perceptions: citizens are not only asked to express preferences among a set of predetermined options based on a questionnaire but can also voice their own views, ideas, knowledge and proposals during thematic table discussions rounds. This setting enables getting a deeper understanding of the rationale behind the citizens' views and gathering valuable input for policy makers and stakeholders to improve the quality of decision-making processes with respect to the views and concerns of the general public.

The citizen summits[74] were organised as full day events with alternating phases of information, an interactive survey combined with face-to-face discussions. The main aim of this setting was to explore the views of European citizens on the interplay between surveillance, privacy and security in relation to the employment of surveillance-oriented security technology (SOST)[75]. To learn more about citizens' perceptions on these issues three different SOSTs (smart CCTV, deep packet inspection – DPI and smart phone location tracking – SLT), were considered at the citizen summits. In order to avoid overburdening the participants with a large number of questions the SurPRISE consortium decided to focus on two (randomly selected) SOSTs per summit as follows:

Country/SOST	Smart CCTV	DPI	SLT
Austria	X	X	
Denmark	X		X
Germany	X		X
Hungary	X		X
Italy		X	X
Norway		X	X
Spain	X	X	
Switzerland		X	X
United Kingdom	X	X	

Table 3: SOSTs per country

The processes in each country followed a similar design. To gain deeper insights into participants' opinions, the SurPRISE summits were based on a mixed approach combining quantitative and qualitative elements. This combined approach allows exploring not merely the views on particular questions in the first place but also the rationale behind the different views.

The methodological approach is based on three major strands: as a starting point, basic information (booklet and films)[76] was provided to the participants to ensure a some common level of knowledge for

[74] All summits were held in the first half of 2014 and had 200 participants each. Further information about these national participation processes is available at http://surprise-project.eu/events/citizen-summits/

[75] The exploration of the technological, legal, political and societal challenges in the privacy-security discourse was part of work package 3. A synthesis of the key findings can be found in: R. Kreissl, R. Berglez, M. G. Procedda, M. Scheinin, M. Vermeulen, E. Schlehan (2013): D3.4 – „Exploring the challenges – synthesis report".

[76] More information about this information package can be found in: K. Ball (2013): D 4.3 –Information material and documentary films, http://surprise-project.eu/wp-content/uploads/2014/04/SurPRISE-D4.3-Information-

the summit; at the core, a predefined survey developed by the SurPRISE consortium served as a tool for quantitative data gathering; and finally, three thematic group discussion rounds linked to the qualitative part in order to get deeper insights into people's opinions. In detail, a set of pre-defined questions and statements clustered around different topics was complemented by discussion rounds relating to such thematic blocks. Participants were divided into groups of 6-8 people and sat at tables facilitated by a moderator. At each summit, the methodology was integrated by two interactive components: (1) the survey was linked to an electronic polling system that allowed participants to immediately answer the questions via keypads, whereas the results were presented right after the polling; (2) to stimulate discussions, for each of the two SOSTs, a short film was presented where experts from different backgrounds gave their assessments of the corresponding SOST. Prior to attending the summit, participants received an information brochure. The mix between written (brochure) and visual (films) information helped to establish a common foundation for the issue knowledge among the participants which enabled discussions on relatively equal footing. For each table, a moderator facilitated the discussion rounds and supported participants if necessary in case of general requests. In preparation for the summit, table moderators received guidelines about the process design, and were trained to perform their tasks. In total, three discussion rounds were conducted. Two - one for each SOST, focussed on the perceived benefits and risks in relation to the particular form of surveillance, in order to gain more insights into the participant's views. The third and final discussion round aimed at participants developing suggestions and recommendations to policy makers at national as well as European level.

The recruitment of participants was conducted differently in each country. In Austria, Italy, Hungary, Spain and UK, external contractors were commissioned with this task. In Denmark, Germany, Norway, and Switzerland participants were recruited without a professional contractor via different channels such as postal invitation letters, announcements in the web and releases in online and offline media. In order to widely achieve a heterogeneous group of citizens reflecting in the total sample, the SurPRISE consortium defined the following criteria which were considered for the recruitment in each case:

- **Age:** Citizens from various age groups, which illustrate a representative picture of the population in the different countries.
- **Gender:** about equal numbers, (50% women and 50% men)
- **Geographical zone:** a mix of urban and rural population
- **Educational level**: categories ranging from primary, middle school and high school, to university education.
- **Occupation**: a mix of participants with different working backgrounds and without expertise in topics related to the SurPRISE project (such as privacy, security, surveillance, technical experts, policy experts, etc.) to grasp perceptions of the wider public.

material-and-documentary-films.pdf The individual country reports, material as employed in the different countries as well as impressions of the summits are available at http://surprise-project.eu/events/citizen-summits/

3.1 Structure of the citizen panels

1780 persons were present at the events with N=1772 valid responses. The table below shows the number of participants in the nine countries:

Country	Invited/registered	Participants
Austria	260	234
Denmark	227	169
Germany	221	190
Hungary	257	215
Italy	250	193
Norway	186	126
Spain	220	185
Switzerland[77]	330	254
United Kingdom[78]	400	214

Table 4: Number of participants per country

The panel structure was relatively balanced regarding age, gender, education as well as citizens from urban (36%), metropolitan (36%) and rural (27%) areas (see the Figures below). With 46% (Female) and 52% (male) participants the gender distribution was relatively but not fully balanced in the total sample (Figure 6). Some countries had a notably higher share of male participants mainly in Denmark, Germany and Switzerland while in Hungary, Spain and UK more female citizens participated in the summits. Regarding age, there were several differences in the countries. However, in the total sample the panel was relatively evenly distributed in the different age categories with a slight majority of participants (44%) belonging to middle-aged groups (between 40-59) as shown in Figure 5.

[77] In Switzerland, 3 summits were held due to the three national languages (German, French, Italian).
[78] In UK, for practical reasons two summits were held.

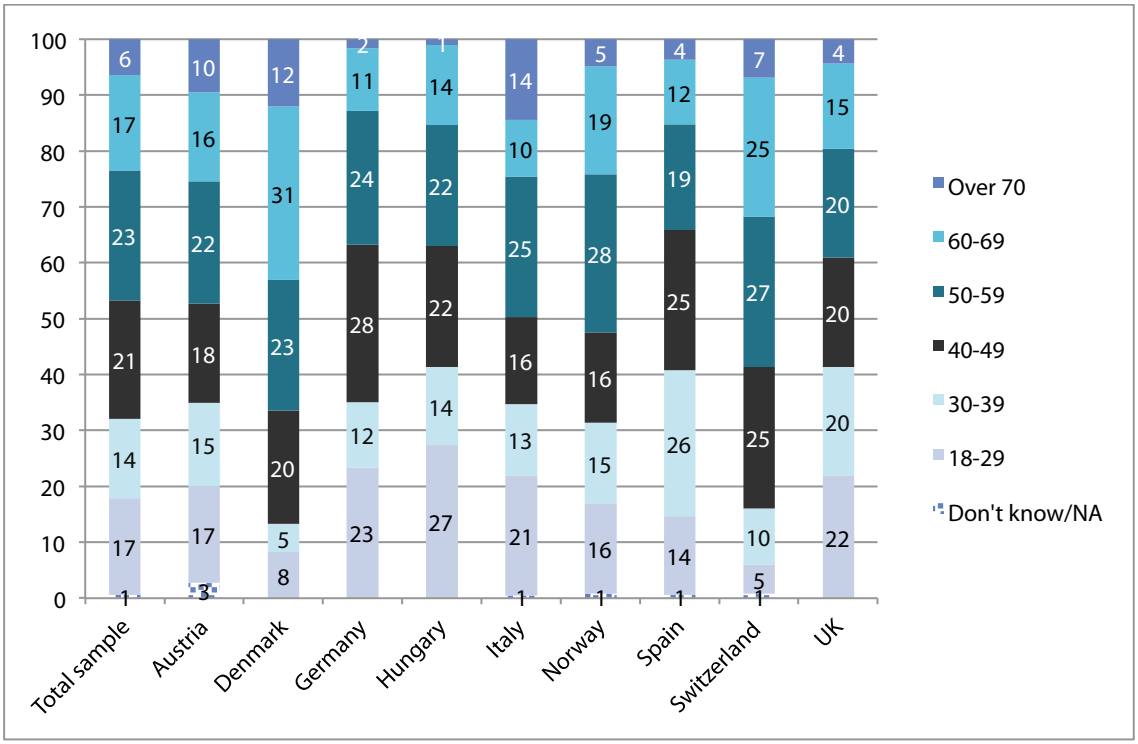

Figure 5: Age distribution per country (percentages)

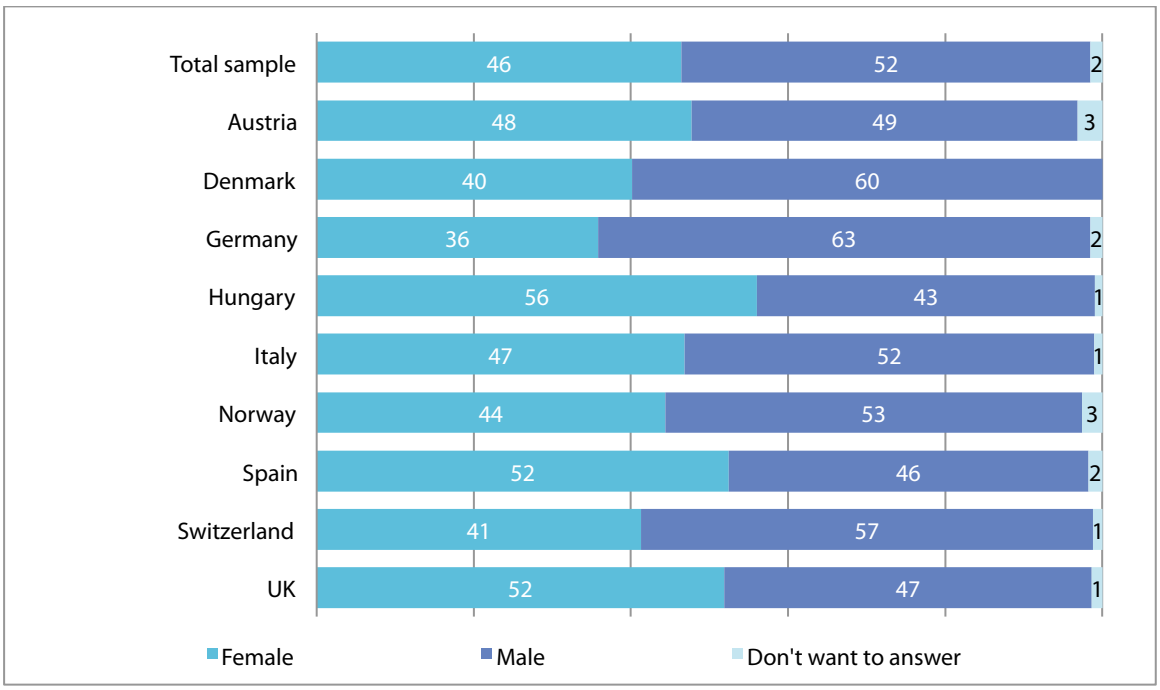

Figure 6: Gender distribution per country (percentages)

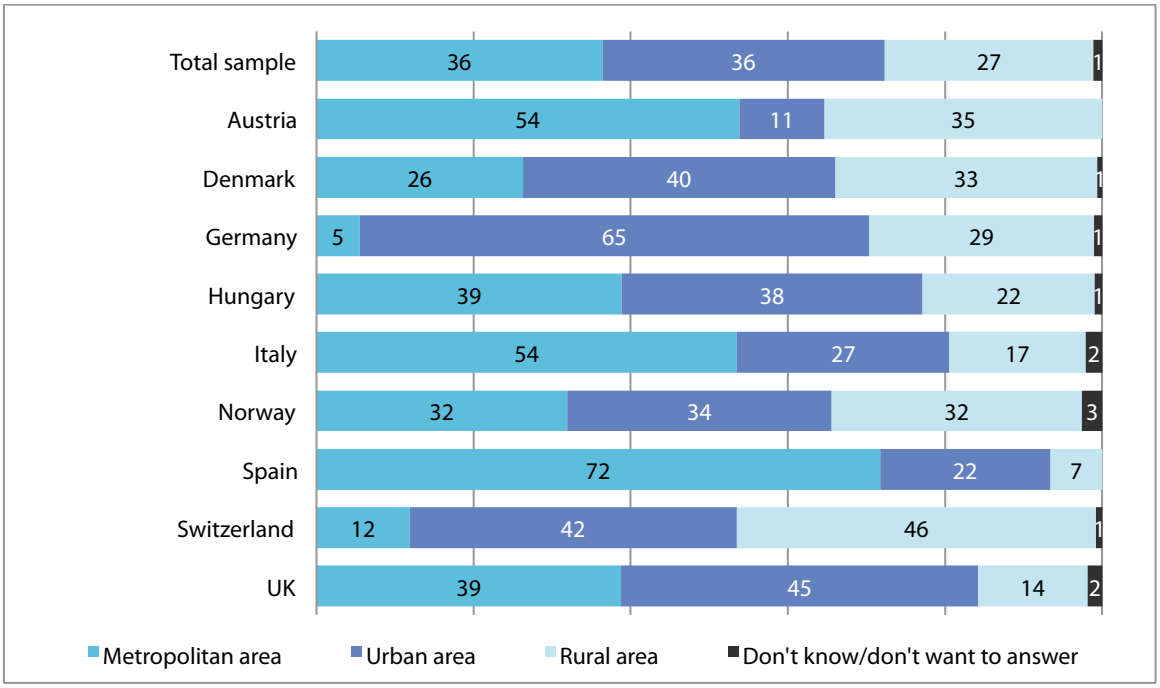

Figure 7: Area of living (percentages)

3.2 How citizens assess the summit

The summits in the different countries received very positive feedback from the participants. In the total sample 79% stated to have gained new perspectives on privacy, security and surveillance by participating in the event. With 60% the clear majority also shared the opinion that the summits generated valuable knowledge for policy makers.

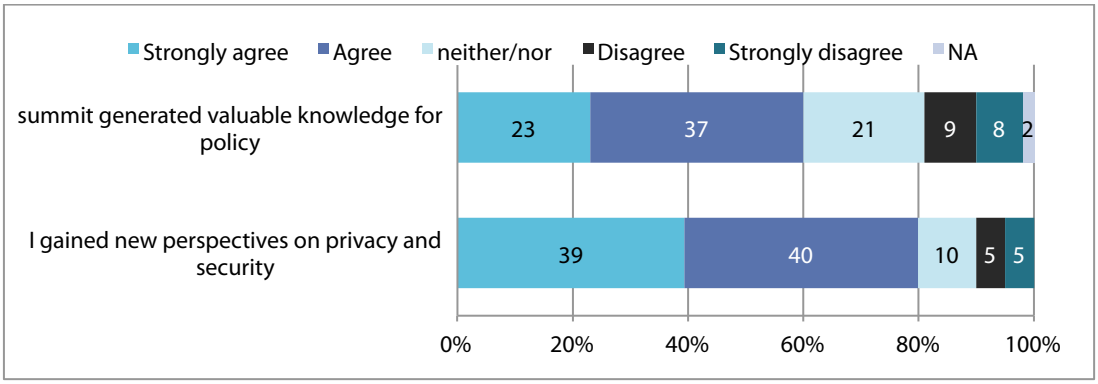

Figure 8: Attitudes on knowledge gain and new perspectives

The summits were also an opportunity for citizens to learn about SOSTs, express and discuss informed opinions in relation to both the privacy and security implications. The setting combining quantitative and qualitative elements contributed to a fruitful and informative experience. The atmosphere was mostly very positive and the participants vividly discussed their views during the different table discussion rounds. During the discussions a variety of issues were addressed about surveillance, security and privacy underlining the importance of these issues for the participants. At the beginning of the

event only 31% of the people considered themselves to be fairly or very knowledgeable about SOSTs without the information material, while at the end of the summit 64% stated to be knowledgeable.

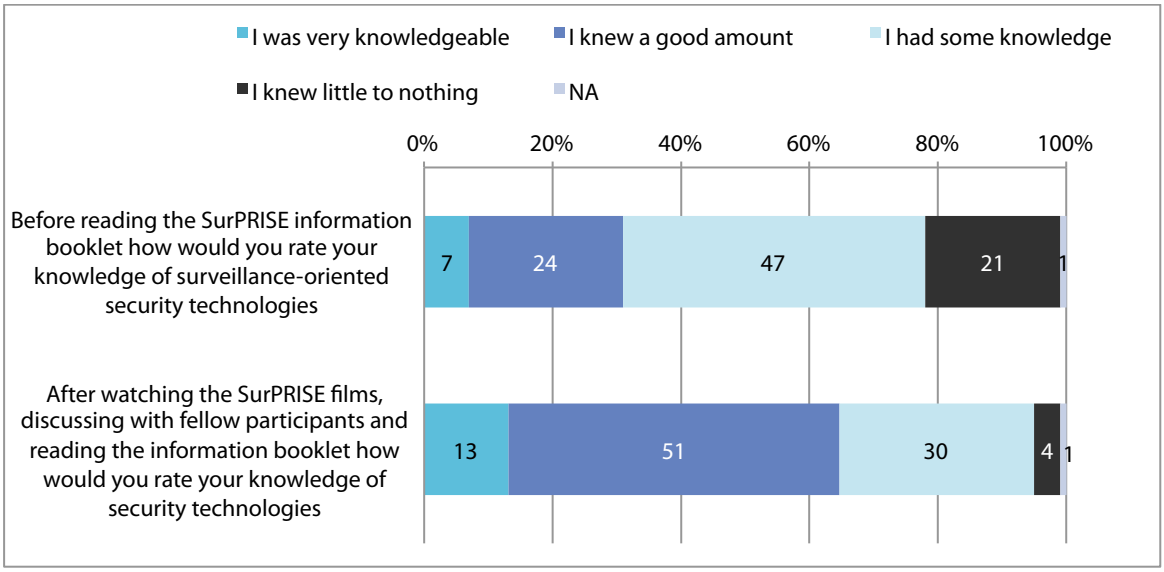

Figure 9: Issue knowledge related to information material

4 Citizens' perceptions on privacy, security and surveillance[79]

This section presents the main outcome of the citizen summits. Based on the results of the surveys as well as the three thematic group discussion rounds in each country, the analysis sheds light on the perceptions and opinions on the complex interplay between privacy, security and surveillance of the European citizens participating in the SurPRISE summits. The questions and statements asked during the summits represent a mix between general and specific aspects to explore general attitudes and opinions on security and privacy as well as how these are linked to specific perceptions regarding the three SOSTs – smart CCTV, DPI and SLT. These emerging forms of surveillance-oriented technologies represent issues affecting different types of privacy such as visual, communicational and locational privacy that are and can be expected to become issues of wider societal concern.

4.1 Security in every day life

With near to 70% in the total sample the clear majority of citizens feels quite secure in their daily lives with some considerable differences in the involved countries (see Figure 10). In this regard, it is interesting to consider the unemployment rates and economic situation in the different countries which gain increasing relevance in Europe (as shown in Section 2) and are perceived as very important for security and safety by the citizens. Especially in the Scandinavian countries, the perception of security seems to be slightly higher compared to the other countries (90% in Denmark, 82% Norway). The lowest perceptions of security are given in Italy (38%) and Hungary (45%). In some countries, there are relatively high rates in the category "neither agree nor disagree", namely in Italy, Hungary, Germany and Spain. With the exception of Germany[80], one possible explanation is that the negative societal effects of financial and economic crisis[81] in these countries reinforce the perceptions of insecurity. Spain, Italy and Hungary have the highest unemployment rates in Europe (see section 2.4)[82]. To some extent this seems to be further confirmed by the answers to the question whether the country is perceived as a safe place to live (Figure 11). Here, values are more distinctive in Hungary, Italy, Spain and UK, where citizens mostly tend towards a middle-position concerning the statement to feel their country is a safe place in which to live.

[79] The percentage values in the presented charts are rounded for better readability. In some cases marginal rounding differences can occur.

[80] According to the German national report, cultural aspects and its historic past namely the Nazi regime and the SED dictatorship might play a role.

[81] Cf. I. Ötker-Robe, A. M. Podpiera (2013): The Social Impact of Financial Crises - Evidence from the Global Financial Crisis. Policy Research Working Paper 6703. Background Paper to the 2014 World Development Report, The Worldbank

[82] Issues related to economic insecurity and unemployment were also raised in the national reports of these countries.

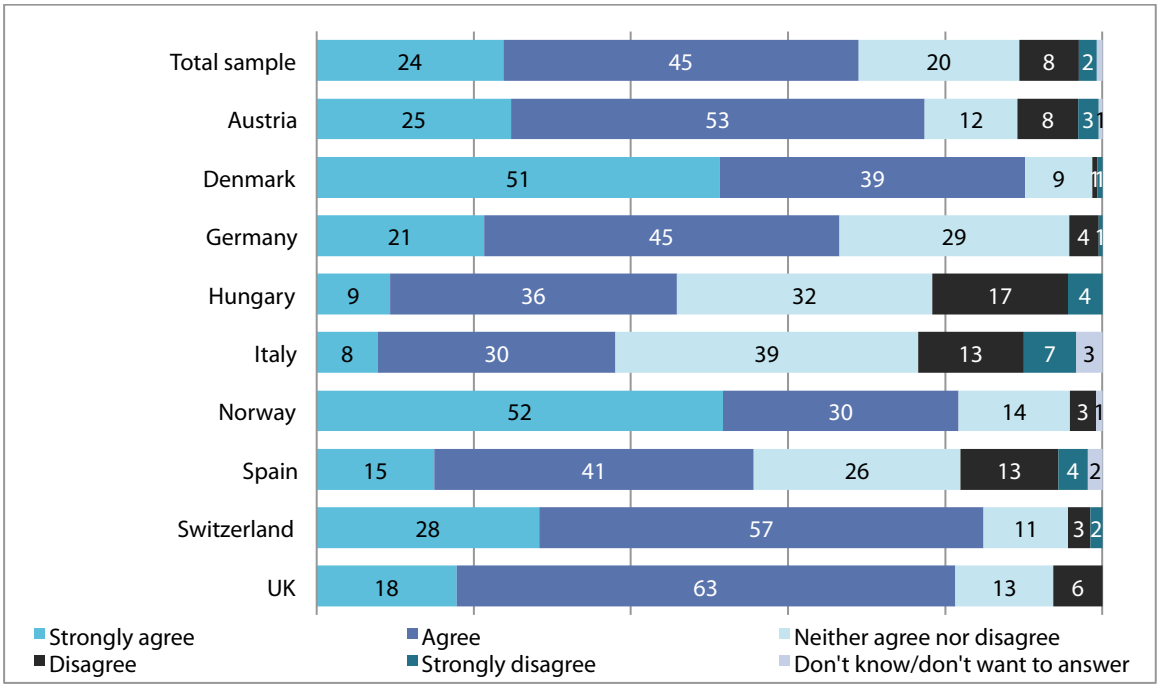

Figure 10: "I generally feel safe in my daily life" (percentages)

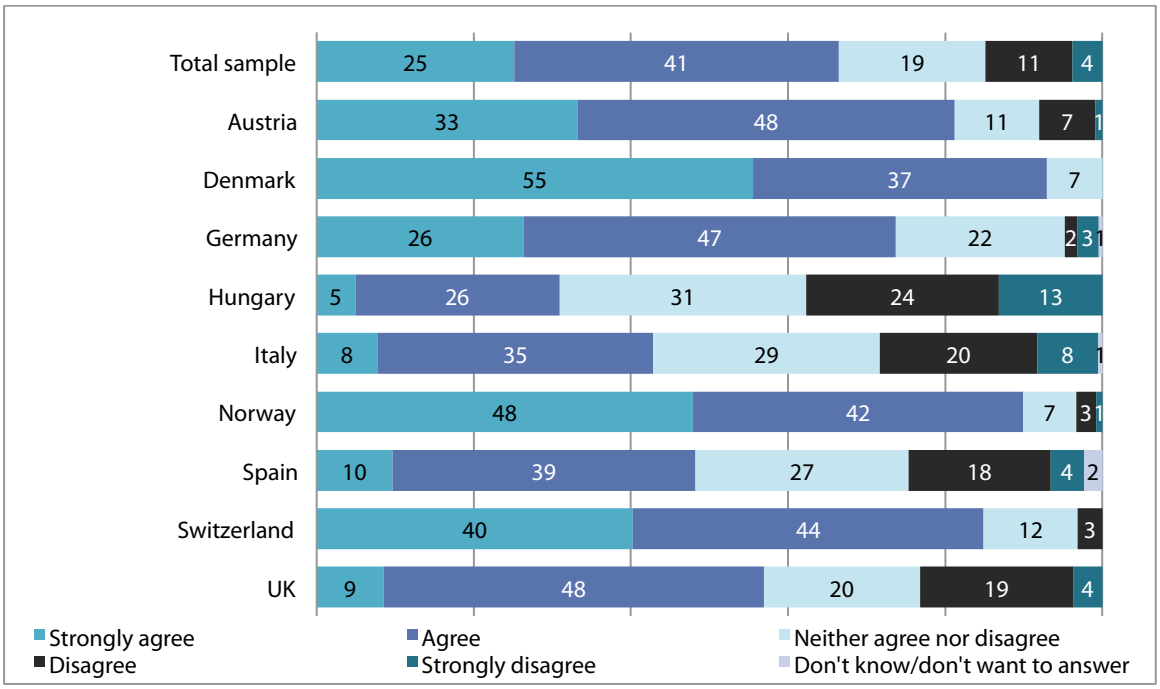

Figure 11: "I feel that this country is a safe place in which to live" (percentages)

61% of the respondents are worried about their security online, while 20% do not share this concern. This suggests that privacy and security on the internet plays some particular role in the citizens' view; and that technology usage might have particular impact on the perceptions of privacy and security. This also mirrors in the more technology-specific questions that were asked to grasp the different attitudes about the privacy/security trade-off and potential changes in this regard (in the next sections).

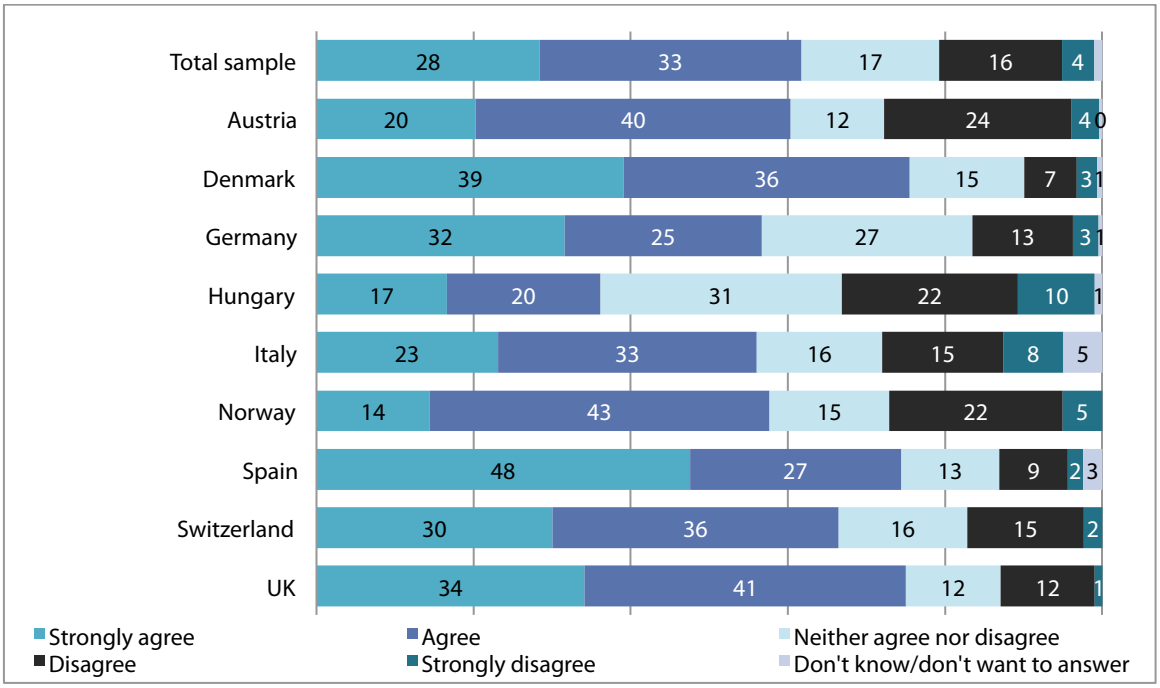

Figure 12: "I worry about security when I am online" (percentages)

Security perceptions related to education and financial situation

There is a significant correlation between the perception of security and education: higher educated persons expressed a higher perception of security (Figure 13). A strong correlation is also given regarding the financial situation: those respondents with an income equal or higher than the national average have a significantly higher perception of security (see Figure 14).

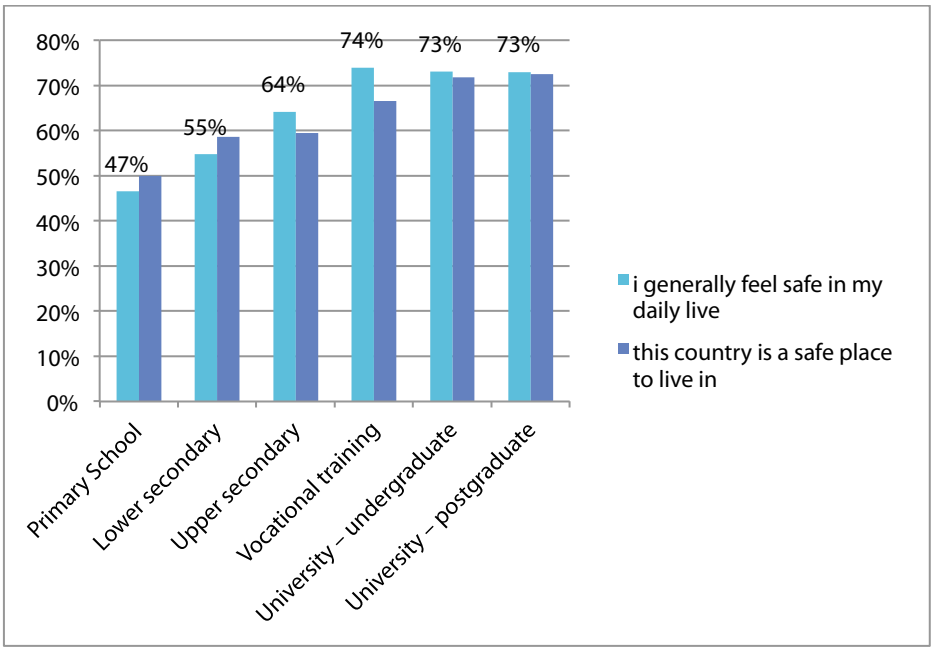

Figure 13: Security perceptions related to education

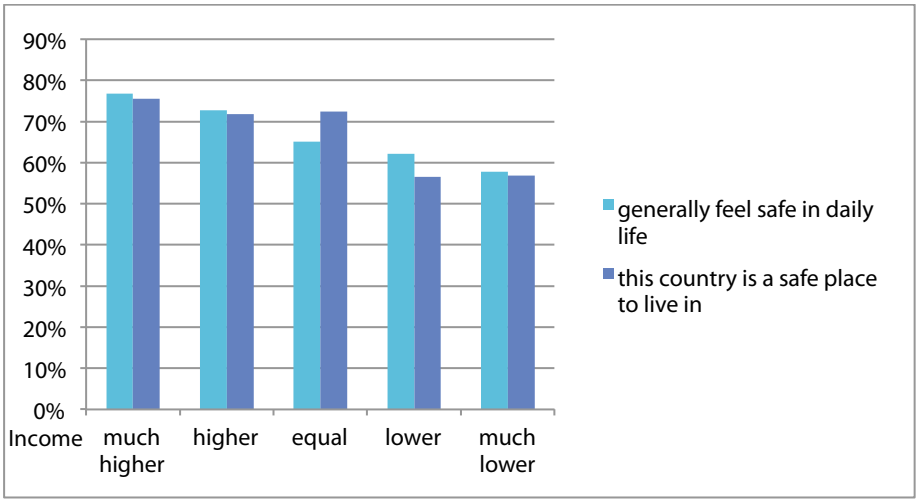

Figure 14: Security perceptions and average income compared to average national (per person/year)

4.2 General privacy perceptions

For different people privacy can have different roles and meanings. For some it is mainly about the "right to be left alone"[83] so one's individual domains and issues of private life that one would like to have protected. Others understand it as an achievement of society and a high public value that contributes to a modulated interplay between private and public spheres. According to the results the participants consider both dimensions – their personal privacy as well as privacy in general as societal value - important whereas a slight majority sees the latter even more threatened by security and surveillance measures and technologies: 68% are concerned that SOST usage leads to an erosion of personal privacy (Figure 15) while 72% fear that SOST usage undermines privacy in general (see figure 16). In some countries, particularly in Germany and Spain, privacy concerns were highly expressed and clear-cut. One explanation for Germany is a very long tradition in privacy and data protection and a similar culture. In Spain, a general displeasure with the difficult social and economic situation might be one explanation as the well-expressed position seems to be a pattern in the survey. Despite of different results in the countries there is a similar tendency observable that the societal value of privacy is perceived as somewhat more important than merely one's own. This indicates a more differentiated view of privacy that goes beyond a traditional understanding of privacy as an issue that separates from public domains of life. Hence, citizens consider privacy as valuable for the individual as well as for the society.

[83] S. D. Warren and L. D. Braneis (1890): "The Right to Privacy". In: Harvard Law Review 193 (1890) Vol. IV Dec. 15 1890, No. 5 http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm

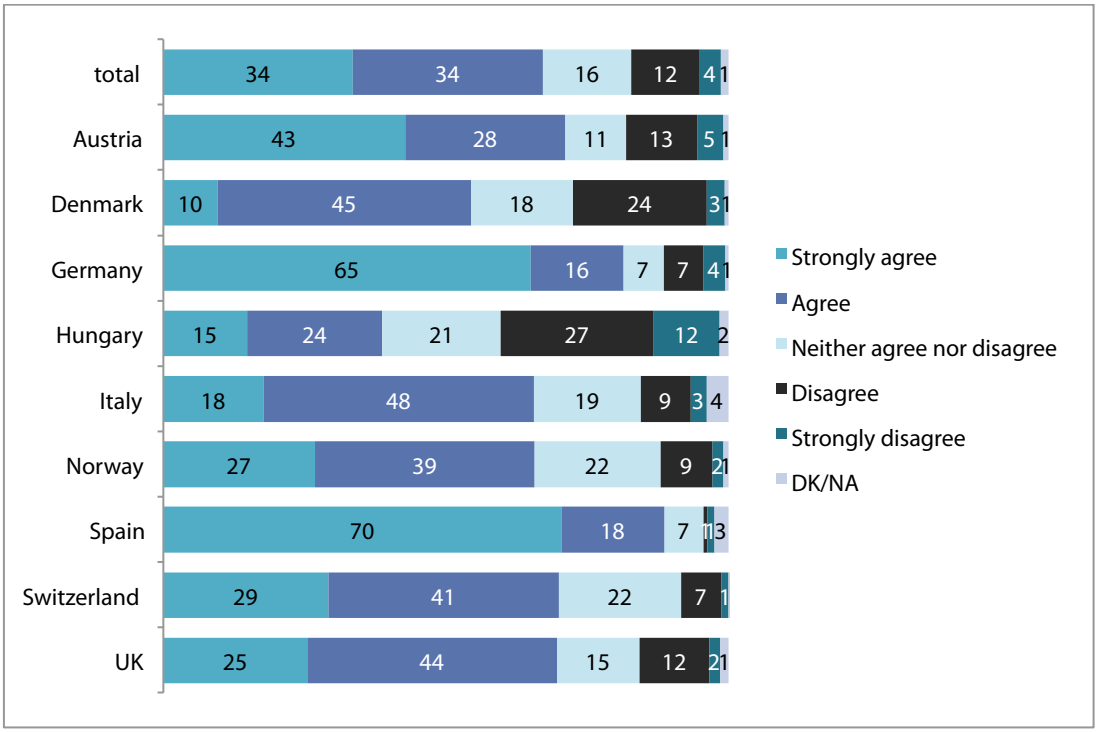

Figure 15: "I am concerned that the use of surveillance-oriented security technologies is eroding ***my privacy***" (percentages)

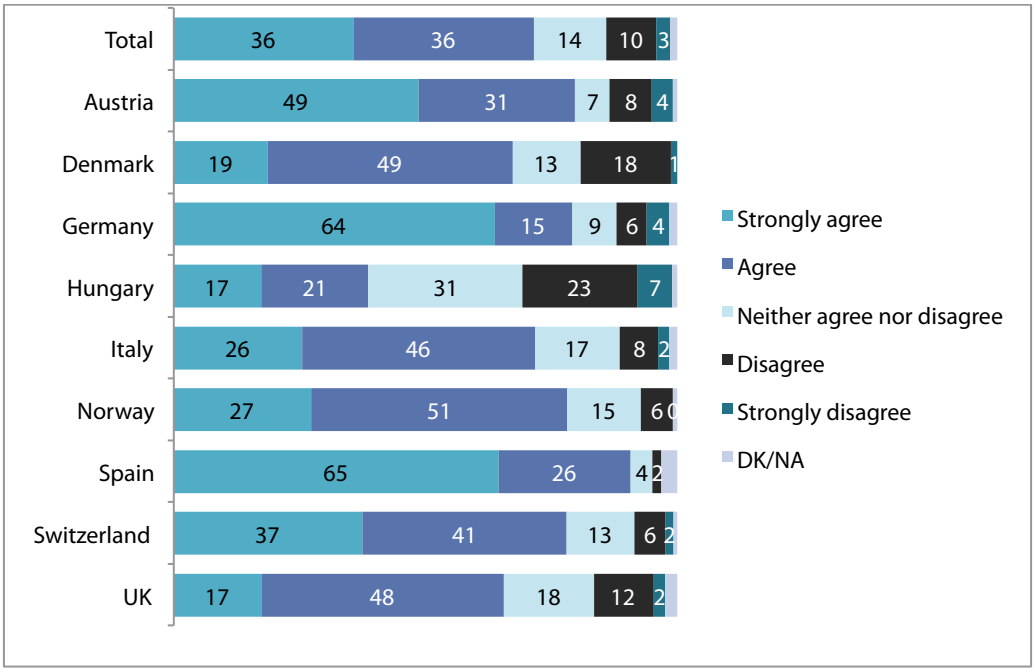

Figure 16: "I am concerned that the use of surveillance-oriented security technologies is eroding ***privacy in general***" (percentages)

Privacy perceptions related to age and education

There are some differences regarding age observable in the perception of privacy concerns: middle-aged citizens (30-39ys, 40-49ys) seem to worry about their privacy more (beyond 70%) than the younger (between 18 and 29) and elderly persons (over 60). However, also in these categories, the concerns are near to 60%. Hence this is not an indicator that elderly and younger persons generally care less about privacy. Concerns about an erosion of privacy in general are less distinct among the different age categories indicating that the collective value of privacy for society is important across the generations.

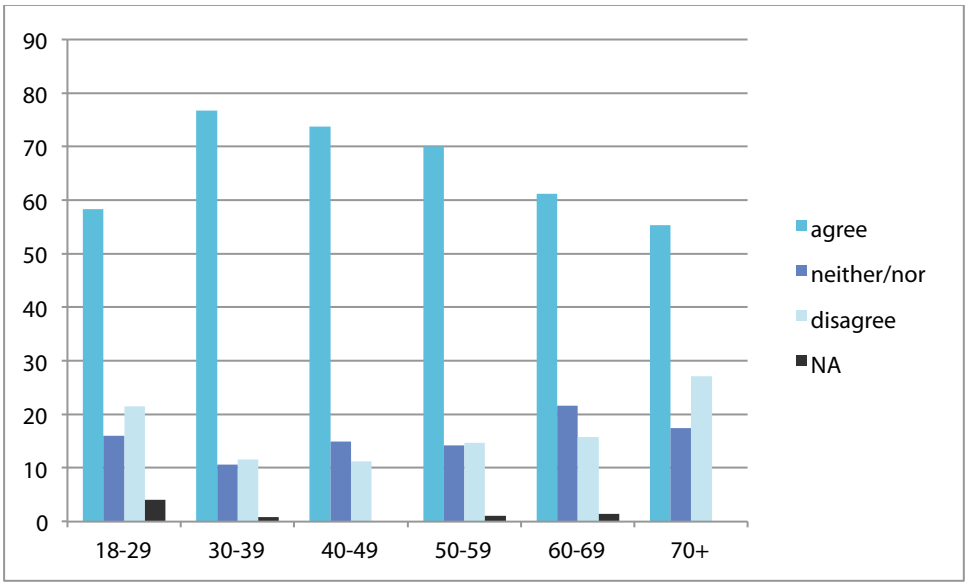

Figure 17: Concerned about erosion of my privacy according to age (percentages)

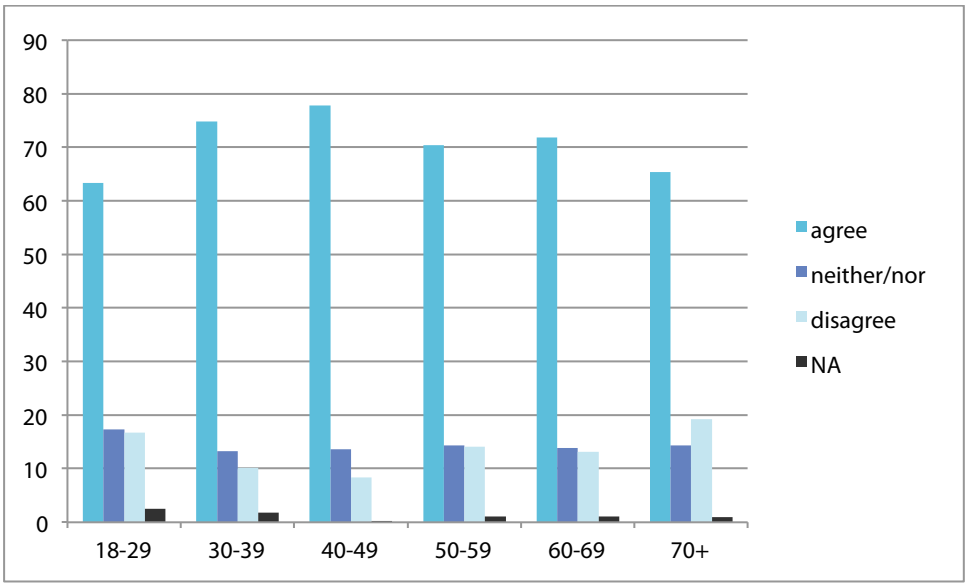

Figure 18: Concerned about erosion of privacy in general according to age (percentages)

The perception of privacy concerns on both general and personal level is not so much influenced by education and concerns people with a basic level of education as well as those with university degrees as the following tables show:

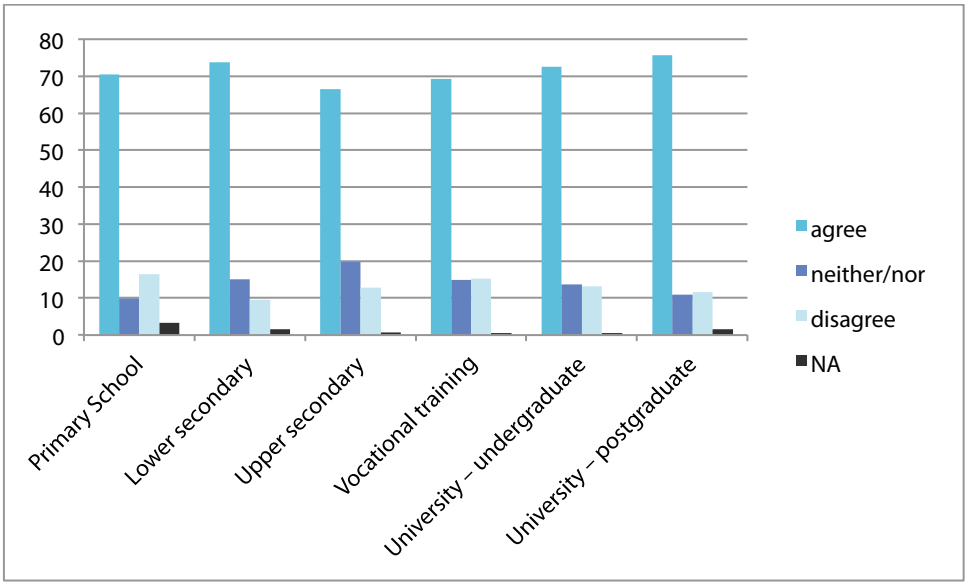

Figure 19: Concerned about erosion of privacy in general according to educational levels (percentages)

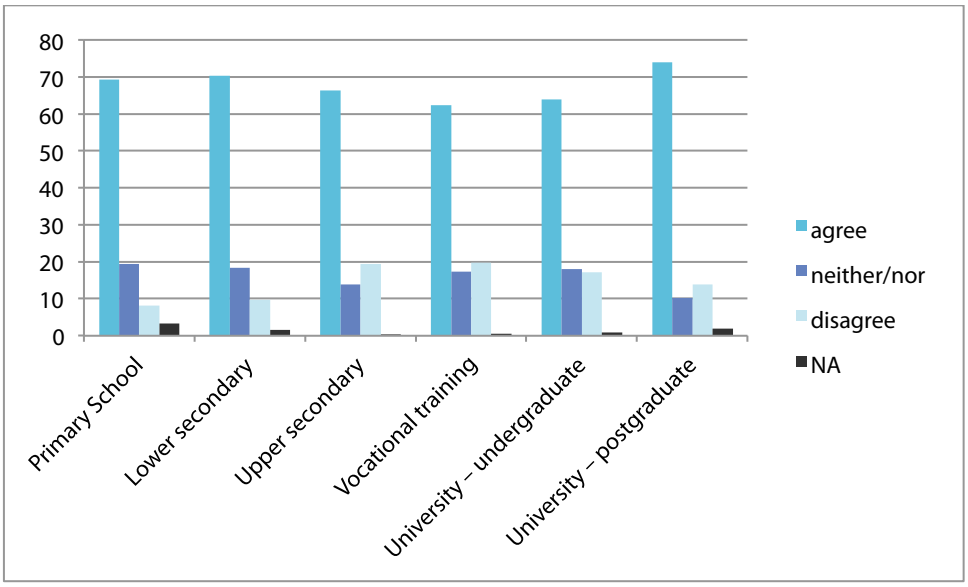

Figure 20: Concerned about erosion of personal privacy according to educational levels (percentages)

4.3 Perceived effectiveness and intrusiveness

The following sections take a more specific perspective and also deal with the different perceptions regarding the three SOSTs – smart CCTV, Deep Packet Inspection (DPI) and Smart Phone Location Tracking (SLT). The relation between the effectiveness and intrusiveness of a SOST is a very important aspect for acceptability. Being asked directly to assess the perceived intrusiveness and usefulness of the SOSTs in each case the option useful but highly intrusive is clearly expressed. 38% perceive this for smart CCTV, 56% for SLT and 66% for DPI. The visible differences between the SOSTS point towards a certain distinction among the respondents between the levels of intrusiveness represented by these technologies. In other words: the intrusiveness affects the perceived effectiveness.

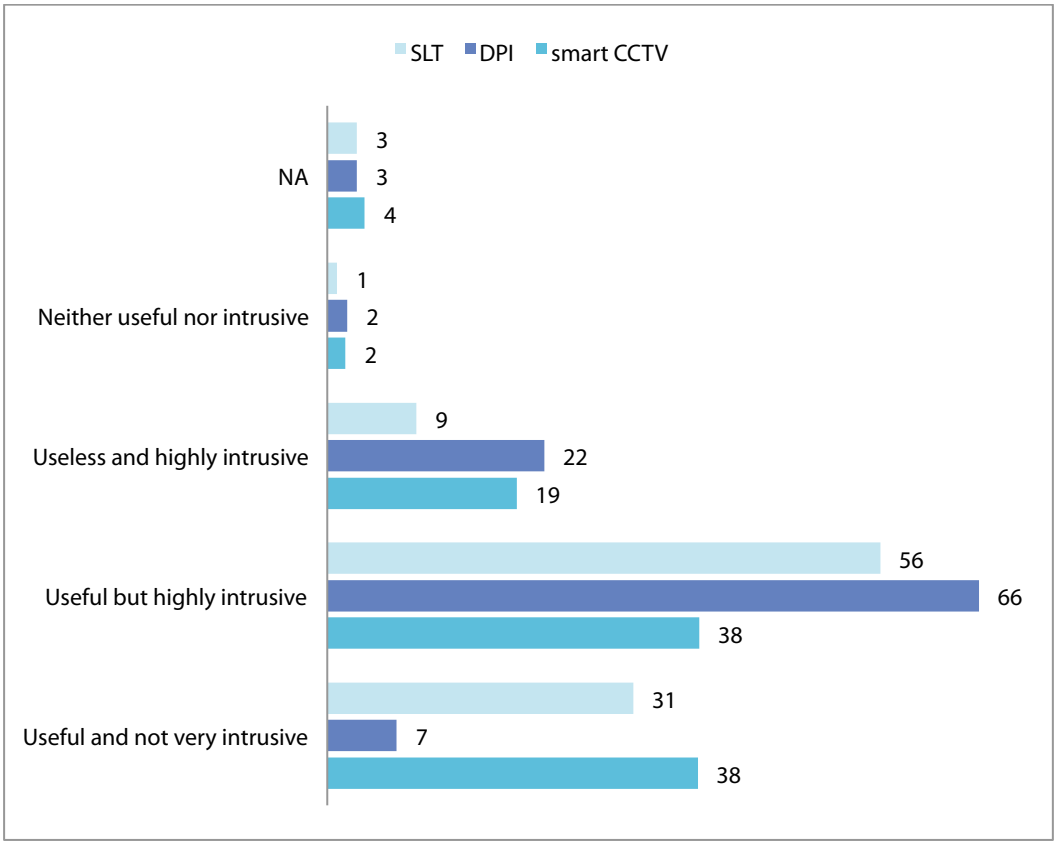

Figure 21: Intrusiveness and usefulness (percentages)

Considering the trade-off model between privacy and security in this assessment, only the position "useful but highly intrusive" corresponds with a trade-off view[84]. In the other options trading would make no sense. At first glance, one could now assume that, as this position (useful but highly intrusive) mostly receives the highest values, the respondents share a trade-off view on privacy and security in their assessment. However, the following results provide more insights into this assessment and reveal a higher complexity than a trade-off suggests. As shown in Figure 22, in general the participants show a tendency to perceive the usage of SOSTs as effective means for national security. Hence, the citizens are aware of some necessity of SOSTs on a general level. Regarding the particular SOSTs the answers vary: while 64% agree that smart CCTV is an effective security tool this perception decreases to 55% in case of SLT and to 43% for DPI. As regards the question of whether the SOSTs are appropriate means to address national security threats, the agree position receives lower values: in case of SLT and DPI about 40% and smart CCTV 51%. This indicates what is confirmed in the further results: that the perceived effectiveness of SOSTs is linked also to their intrusive capacity. The respondents feel quite uncomfortable with the use of each of these technologies, 66% in case of DPI, 45% regarding SLT and 39% regarding smart CCTV.

[84] As suggested by earlier exploratory analysis in the PRISE project (http://www.prise.oeaw.ac.at/) that showed that the question of such kind of trade-off is relevant only in case if citizens perceive SOSTs both security enhancing and privacy infringing.

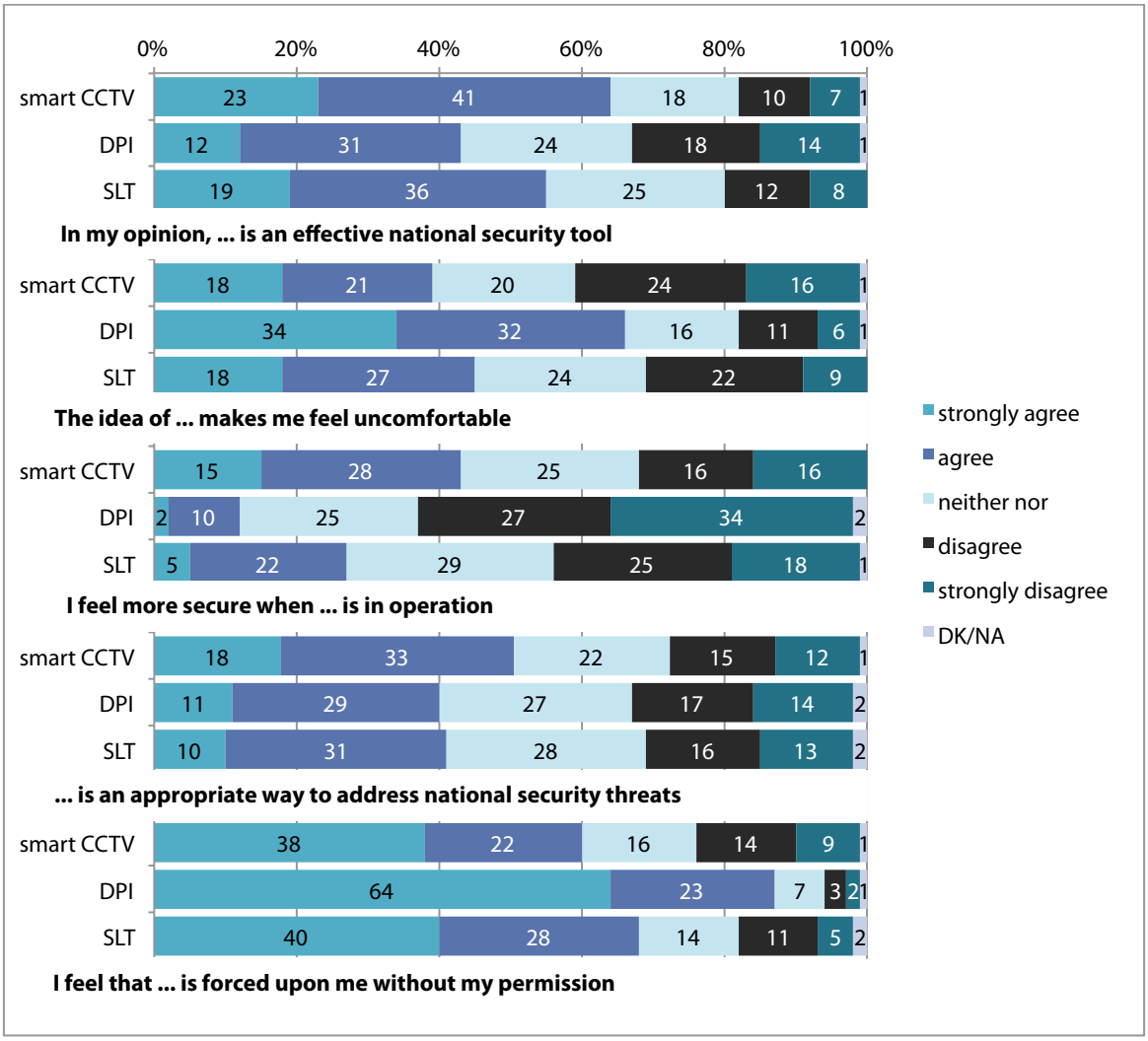

Figure 22: Major attitudes regarding particular SOST usage

Compared to smart CCTV and SLT, DPI raised the highest concerns and receives the lowest rates regarding effectivity and appropriateness to handle national security threats. Despite of the differences in particular, the effectiveness and intrusiveness of the SOSTs are interrelated: those technologies perceived as highly intrusive are also perceived as less effective. Furthermore, also the mode of implementation, i.e., how security and surveillance measures and SOST usage are implemented and employed raises high concerns: the clear majority (in each case over 60%, regarding DPI even near to 90%) perceives that the SOSTs are forced upon them which also indicates that the participants do not accept how SOSTs are implemented and perceive a lack of transparency and accountability of the authorities using these SOSTs as well as difficulties regarding trust (see Section 4.7).

As Figure 23 shows, the intrusive capacity of the technologies also makes a difference for their acceptability. On a general level a certain amount of intrusion seems to be accepted among the respondents. However, this is only valid for the participants under certain conditions. For the participants it is not sufficient that a SOST improves public security. If it is too intrusive it is not accepted as a security measure. This is not only a matter of the technology itself and its functioning but also of the related practices, i.e. its usage. SOST usage is particularly perceived as too intrusive if it intrudes into privacy of persons without concrete suspicion and without appropriate legal mechanisms to ensure that the technologies are used in a lawful way. In the table discussions the need for judicial orders and legal

control mechanisms that ensure that SOSTs are only used for plausible reasons, i.e. concrete suspicion, was often mentioned and is very important for the citizens. In this regard there were strong concerns expressed that legal regulations are not sufficient to ensure that SOSTs are not misused. Only a minority in each case has an opposing opinion (28% regarding SLT, 24% regarding smart CCTV, and 19% regarding DPI). Hence, people have little trust in laws and regulations protecting them from misuse of SOSTs. In general, regulation and oversight were seen as crucial elements in the relation between effectiveness and intrusiveness.

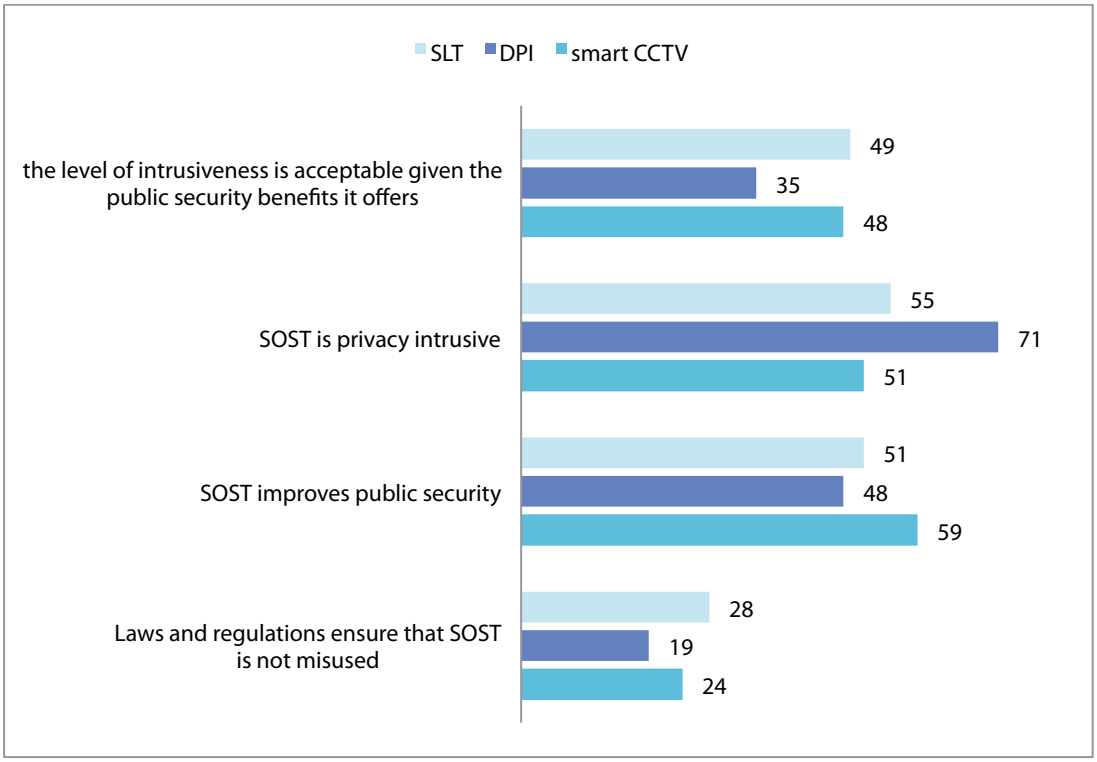

Figure 23: Intrusiveness and acceptability (percentages)

4.4 Different qualities of privacy intrusion and related concerns

The perceptions of the participants about three different SOSTs were gathered in order to explore potential differences regarding privacy types and related concerns. The selected SOSTs thus represent different qualities of privacy intrusion referring to the privacy typology of Finn et al (2013) which allows to to reconsider and reflect upon different kinds of SOSTs and their impingement on privacy and how particular SOSTs cross the boundaries between different privacy types. They distinguish between seven different types[85], privacy of: (1) *the person:* the protection of body functions and characteristics, such as biometrics or genetic codes; (2) *behaviour and action:* this type addresses the "ability to behave in public, semi-public or one's private space without having actions monitored or controlled by others", including "sensitive issues such as sexual preferences and habits, political activities and religious practices"; (3) *communication:* the ability to communicate freely via different media and without interception including the avoidance of different forms of wiretapping and surveillance of communication; (4) *data and image* to ensure that one's data and images are not automatically available to other individuals and organizations; individuals should have "a substantial degree of control" over their data and its usage;

[85] Rachel L. Finn, David Wright, and Michael Friedewald (2013) "Seven Types of Privacy" in Gutwirth, S.; Leenes, R.; de Hert, P.; Poullet, Y. (Eds.), "European Data Protection: Coming of Age", Chapter 1, Dordrecht: Springer. DOI 10.1007/978-94-007-5170-5_1

image is a particular "form of personal data can be mined for biometric data and used to identify, monitor and/or track individuals as they move about public or semi-public space"; (5) *thoughts and feelings*: one's freedom to think and feel whatever he/she likes to without restriction; this type differs from behaviour as thoughts do not necessarily translate into behaviour and vice versa; (6) *location and space:* one's right to move freely in private, public or semi-public space without being identified, tracked or monitored; (7) *association (incl. group privacy):* addresses the right to associate with whomever they wish without being monitored. This includes no monitoring of groupings or profiles over which one has no control (e.g. involvement in discussion groups).

The table below shows the SOSTs treated at the SurPRISE summits in relation to the different privacy types. A small "x" marks that the according privacy type is affected, "(x)" means a privacy type is potentially affected and a large "X" indicates that the according privacy type is mainly affected.

Privacy type / **SOST**	Person	Location and space	Behaviour	Communi cation	Data & image	Thoughts & feelings	Association
Cyber-surveillance/ DPI		x	x	X	x	x	X
(Smart) CCTV	X	x	X	(x)	x		x
Smart phone location tracking		X	X	(x)			X

Table 5: SOSTs related to different types of privacy

This (approximated) picture points out the different intrusive capacities of these technologies which plays an important role for their perceived effectiveness and acceptability. The empirical results indicate that the form and level of privacy intrusion of a SOST also makes a difference in the perceptions of the citizens and partially entails different privacy concerns.

Taking a closer look at the major concerns reveals some differences regarding the intrusive quality of the SOSTs as shown in the figures below. Citizens expressed quite pronounced worries about privacy infringements and misuse of personal information that may lead to misinterpretations of one's behaviour. These concerns were not only related to potential privacy impacts in the participants' personal domains. In general there are the high concerns about how surveillance-oriented technologies might develop in the future: Two-thirds of the participants fear about an extension of smart CCTV usage and 60% are concerned about future usage of SLT. With 84%, worries about DPI in this regard are even stronger underlining the extraordinarily high perceived intrusiveness of this SOST. These significantly higher fears about internet surveillance are also visible in the different table discussions.

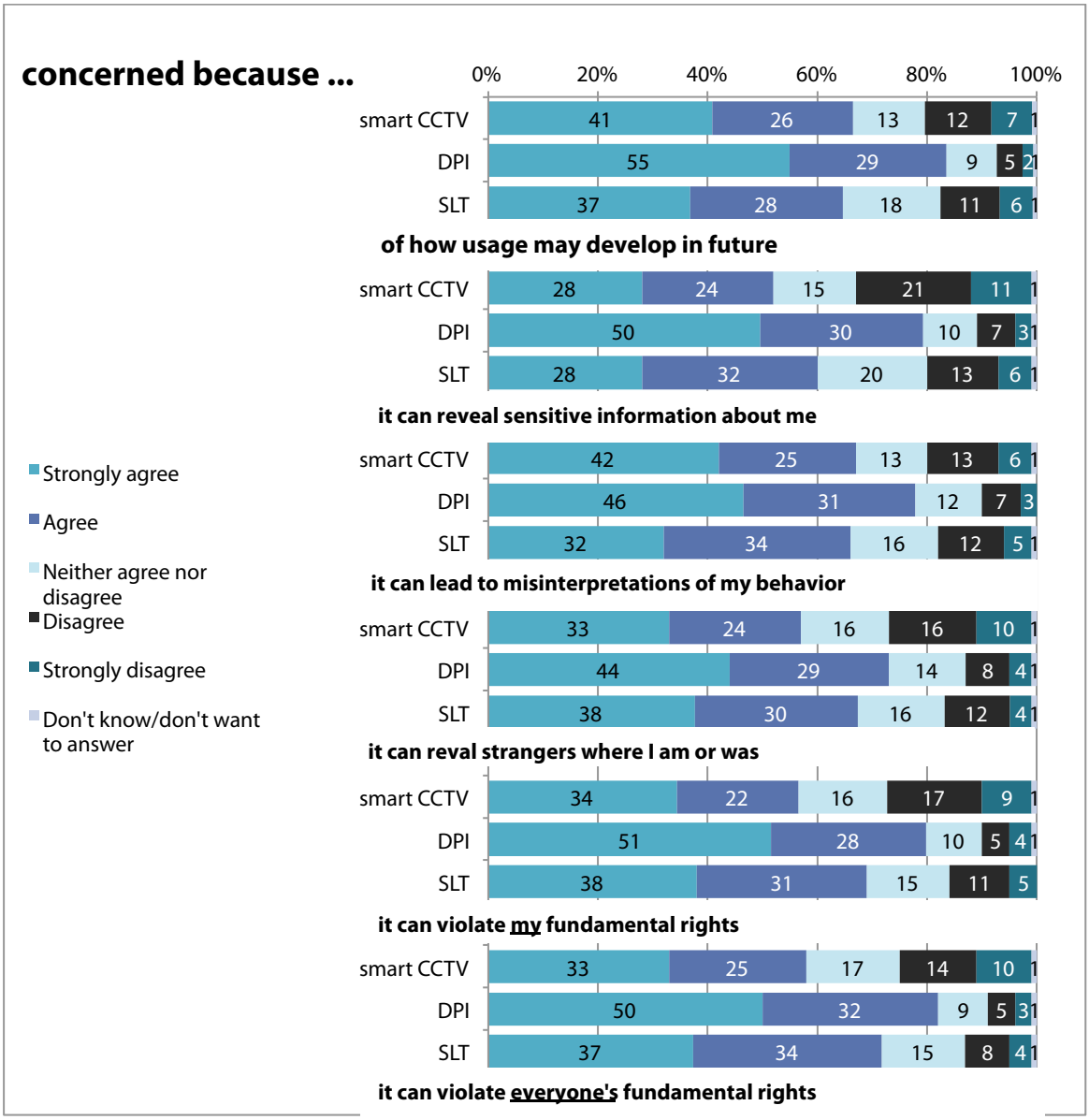

Figure 24: Major concerns regarding particular SOSTs

It is conspicuous that (taking the opposing categories together) the results reveal a specific order regarding the perceived concerns expressed: in the case of DPI the concerns are apparently highest, followed by SLT and then smart CCTV. This indicates that the respondents perceive different levels of intrusiveness represented by these SOSTs. Smart CCTV is linked to visual surveillance which has at least some conceivable purpose for the participants while the other two SOSTs entail a number of purposes and affect different contexts that are elusive and hardly recognizable. At the same time these technologies intrude deeper into the private sphere. DPI affects common every day information and communication behaviour and SLT everyday movements. Hence, for the participants the intrusive capacity and the related concerns are linked to the different types of privacy affected by the SOSTs (as shown in table 5). Despite of the particular SOSTs the results also shed new light on (spatial and temporal) proximity as an important factor regarding the perceived privacy intrusions: while in risk literature, proximity literally means the closeness to a risky technology, the meaning of proximity becomes more abstract with virtual technologies such as SLT and DPI. Spatial proximity here means not necessarily that the SOST is in the same geographical area as the individual but that the SOST can

constantly gather information about the individual. In other words: the SOST is capable of monitoring even though it is not in the same area. This obscurity of virtual technologies might affect the perception of intrusiveness. Temporal proximity includes potential misuse of personal information by SOSTs as well as how the SOSTs may develop in the future.

The clear majority expressed high concerns about SOST usage not merely because surveillance affects them personally. There seem to be high worries about potential violations of human rights due to SOST usage on a personal (smart CCTV 56%, SLT 69%, DPI 79%) as well as on a collective level, i.e. about everyone's human rights being affected (smart CCTV 58%, SLT 71%, DPI 82%). These concerns also reflect in most of the table discussions where untargeted SOST usage and mass surveillance were controversially debated: while the effectiveness of such measures was doubted it was at the same time perceived as highly intrusive. Hence, the level of intrusiveness also affects the acceptability of a SOST. According to the results there seems to be a critical level which, if reached leads to a strong resistance and rejection of the SOST (see next section). In other words: If a SOST reaches a critical level of intrusion it might not be accepted. This is particularly the case for DPI forms of monitoring private communication and information usage which was widely rejected by the participants across the countries. Main reasons for this strong opposition lie in its deeply intrusive capacity and the accordingly enormous potential for abuse. Many discussants critically argued that this kind of technology intrudes everything, can be manipulated, misused for suppression and cannot be controlled. At several table discussions (e.g. in Austria, Germany, Italy, Spain) the fear of political control by suppressing regimes such as fascist states, the STASI or regimes in some Arab countries were mentioned in this context. Many fears of function and mission creep were expressed by the participants. In relation to this clear opposition participants were more ambivalent as regards smart CCTV and to some extent SLT although strong concerns were also expressed here. In this regard social, spatial and temporal proximity plays an important role which is also confirmed by the discussion outcomes. If a SOST is very close to monitor individual behaviour covering a broad and elusive scope of purposes it is less acceptable. The use of SOSTs for limited, clearly defined purposes and the controllability of proper usage were considered as very relevant. For several participants the use of CCTV makes sense in some known contexts such as airports, large-scale events and other public places with particular safety requirements.

The concerns about the technologies in particular are consistent with the major attitudes and concerns in general as shown in Figure 25 and further highlight the interrelations between intrusiveness and effectiveness. In total, 64% share the opinion that the use of SOSTs contributes to improving public security and the majority does not think that SOSTs are only used to demonstrate action against crime. However, if the achievement of security by a SOST is acknowledged this does not imply that also the privacy intrusion of that SOST is accepted as the results show. At the same time, 70% share the opinion that SOSTs are likely to be abused and there are a number of high concerns about the abuse of personal information: 70% are concerned about extensive information collections, 63% that the information held about them might be inaccurate, near to 80% fear that their personal information might be used against them and 91% are concerned that their information is shared without their permission[86]. Compared to the answers referring to effectiveness, the concerns and fears about abuse of information and power dominate the assessment of the citizens. These results thus indicate that the intrusiveness of SOSTs and security measures has a negative effect on their acceptability. For the citizens, the modalities of security and surveillance have reached a level where the gathering and processing of personal information is not in accordance with the interest of the public.

[86] This fear of not permitted information usage also refers to the problematic aspects of informed consent as one cornerstone of privacy. While consent is essential for legal data processing, from the individuals' point of view it is often complicated not least due to a lack of alternatives.

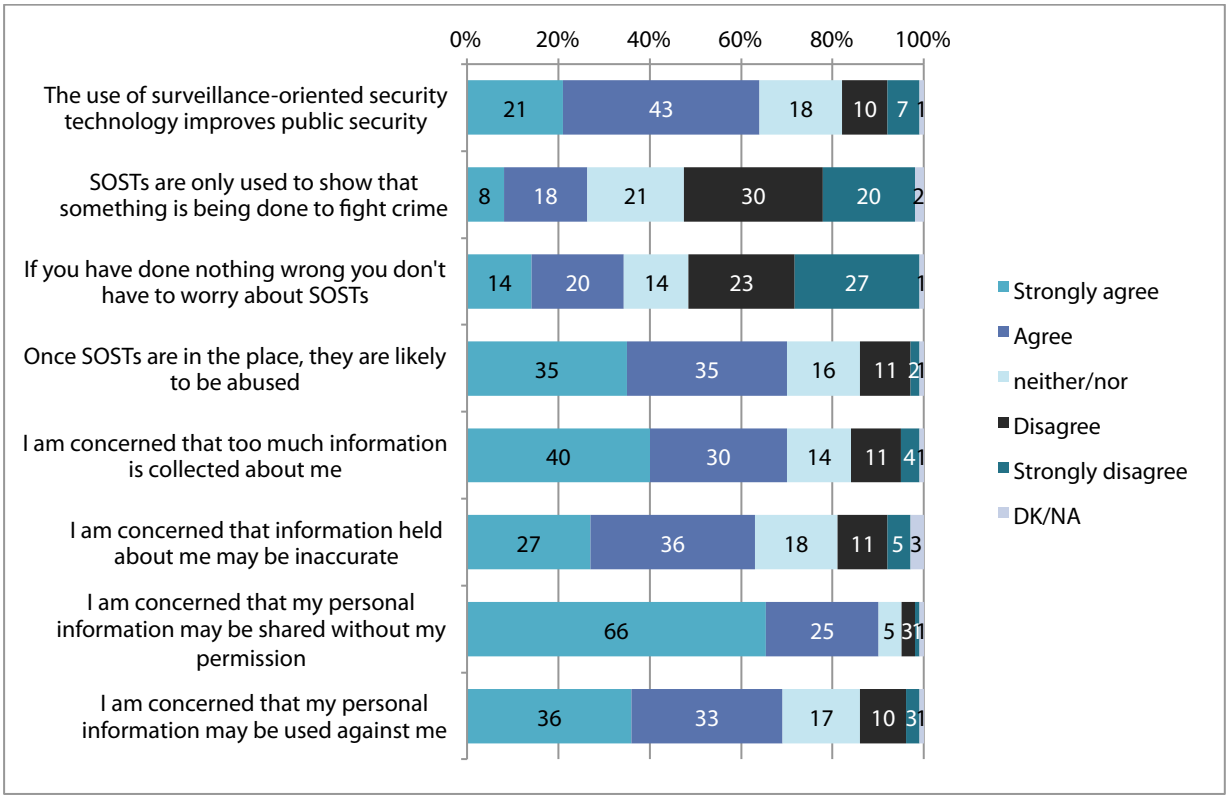

Figure 25: Major attitudes about SOST usage

4.5 Resistance against surveillance

Above all, the expressed concerns and the high perceived intrusiveness of SOSTs on a general as well as on a specific level refer to a strong demand for privacy protection and the according information in this regard as the Figure 26 below shows. This is the case for each of the SOSTs although regarding smart CCTV there is some lower amount of opposition. According to the national reports this is mainly the case in Denmark, UK and Hungary which are those countries where CCTV is relatively widespread.[87] The relatively low rates regarding protest and opposition partially derive from a perceived lack of options to effectively change the use of the SOSTs which was also raised in some table discussions. At the same time, the sheer opposition does not seem to be enough for the majority of participants. Instead, they also wish more information about privacy protection, transparency and scrutiny of SOST usage.

[87] Denmark and UK have the highest CCTV density in Europe and also in Hungary, the number of cameras is increasing. Cf. C. Norris, M. McCahill, D. Wood (2004): The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space. Surveillance & Society 2(2/3), pp. 110-135.
Budapest recently announced plans to extend the use of CCTV on public transports http://www.eltis.org/discover/news/security-cameras-green-lighted-budapest-public-transport-hungary-0

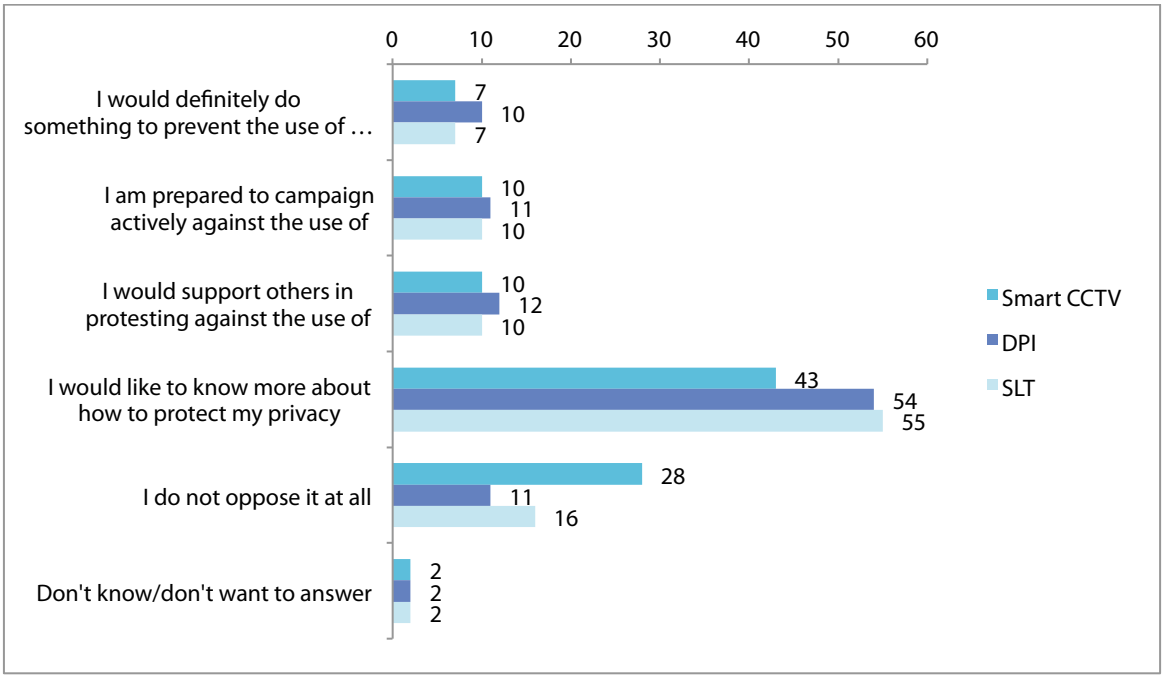

Figure 26: Actively challenging SOSTs[88] (percentages)

Being asked about taking measures to avoid being subject to the SOSTs these were not highly expressed among the participants: less than 10% in the case of smart CCTV and DPI, and 12% would actively avoid SLT. This indicates some uncertainty about the realistic odds to avoid SOSTs. A slightly different impression is given regarding altering behaviour. Overall there is a rather clear tendency among the participants opposed to behavioural changes with the outlier given in case of DPI as 30% stated that they would change their behaviour followed by 18% regarding SLT. This significantly higher value compared to the other two SOSTs is explainable considering that DPI is the most intrusive technology deeply affecting one's information and communication behaviour which mirrors also in the qualitative results, as many discussants argued in this regard. In total this links back to the different levels of intrusiveness represented by the SOSTs as there seems to be some hierarchical order in the expression to change or not change behaviour related to the intrusive capacity of the technologies: behavioural changes due to DPI are highest, followed by SLT and lowest in the case of smart CCTV where participants were most certain not to behave differently. In the discussions it also was raised that these technologies progress very rapidly and develop faster than society which also leads to mistrust and concern. Several participants expressed a demand for more information about bringing in complaints in case of privacy violations and about how citizens can use information about themselves e.g. in trials or civil litigations.

[88] The first statement was asked differently in the UK: "I am prepared to use any means I can to prevent the use of …"

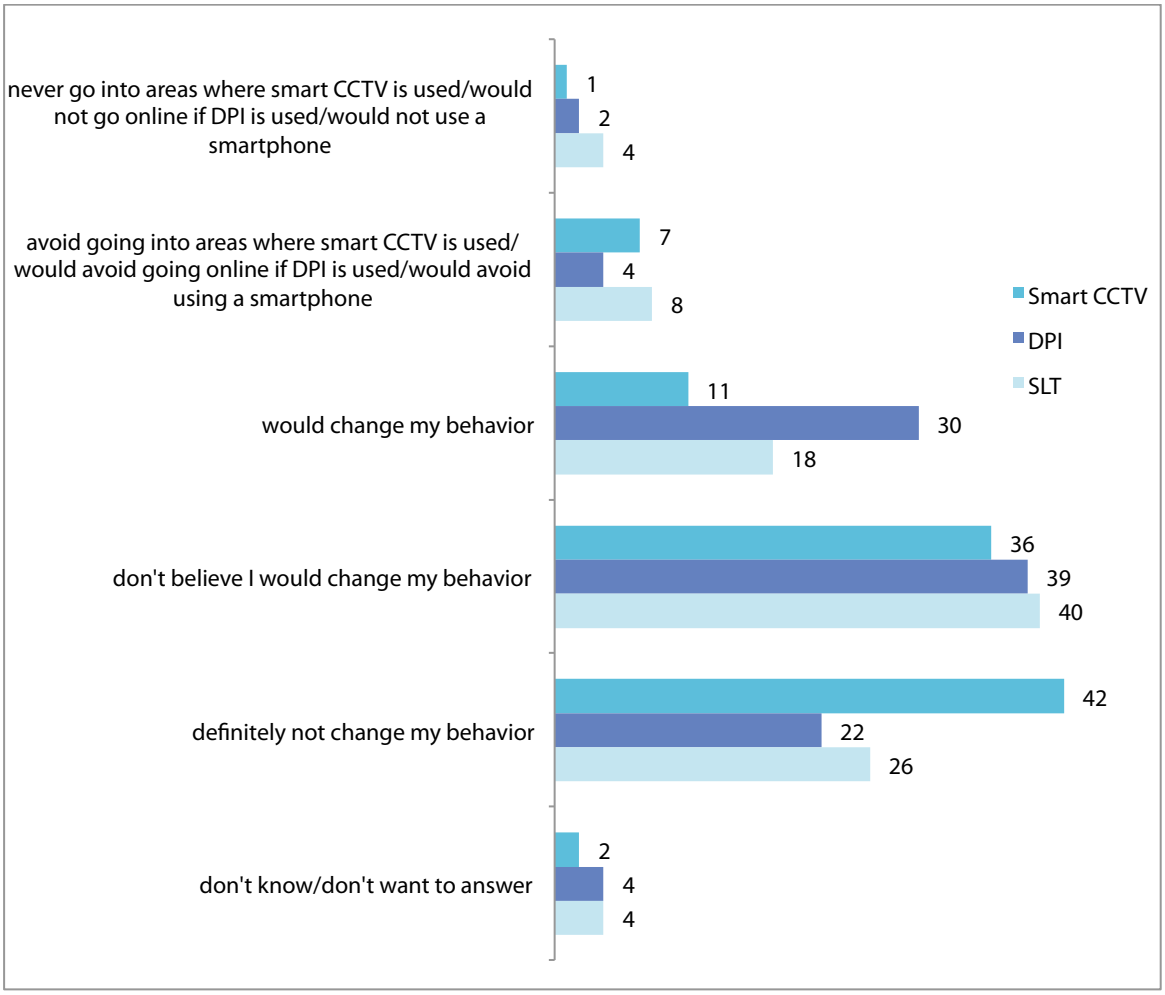

Figure 27: Actively avoid being subject to SOSTs (percentages)

4.6 "Nothing to hide" unscrambled

A prominent argument to justify security and surveillance measures that intrude into privacy is the statement "those who have nothing to hide have nothing to fear" indicating that one does not need to worry about privacy infringement and surveillance if one behaves correctly. This argument falsely reduces privacy to a form of secrecy aiming at hiding things. At the same time, it neglects that surveillance can also do harm to a variety of activities that are lawful and essential in a democratic society such as freedom of thought, expression, religion, free association, etc. [89] In order to explore the citizens' perceptions in relation to this line of argumentation a similar statement was asked (as shown in Figure 28). This line of argument is not shared by 50% of the participants in the total sample as well as in most of the countries with the strongest opposition in Germany. The exception here is given in Hungary and UK, where the respondents tended to agree with this statement. However, also in these two

[89] Cf. B. Schneier (2006): The eternal value of privacy. In: Wired. https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html
C. Bennett (2008): The privacy advocates: resisting the Spread of Surveillance. MIT Press, Cambridge and London.
D. Solove (2007):'I've got nothing to hide,' and other misunderstandings of privacy. San Diego Law Review Vol. 44 p. 745- http://tehlug.org/files/solove.pdf
D. Solove (2011): Nothing to hide: the false tradeoff between privacy and security. Yale University Press, New Haven and London.

countries, the participants expressed their concerns that too much information is collected about them. In the total sample, 70% of the participants are concerned, with two-thirds in the UK and also in Hungary, there is a clearly expressed fear that too much personal information is being collected, as shown in the figures in section 4.6.2.

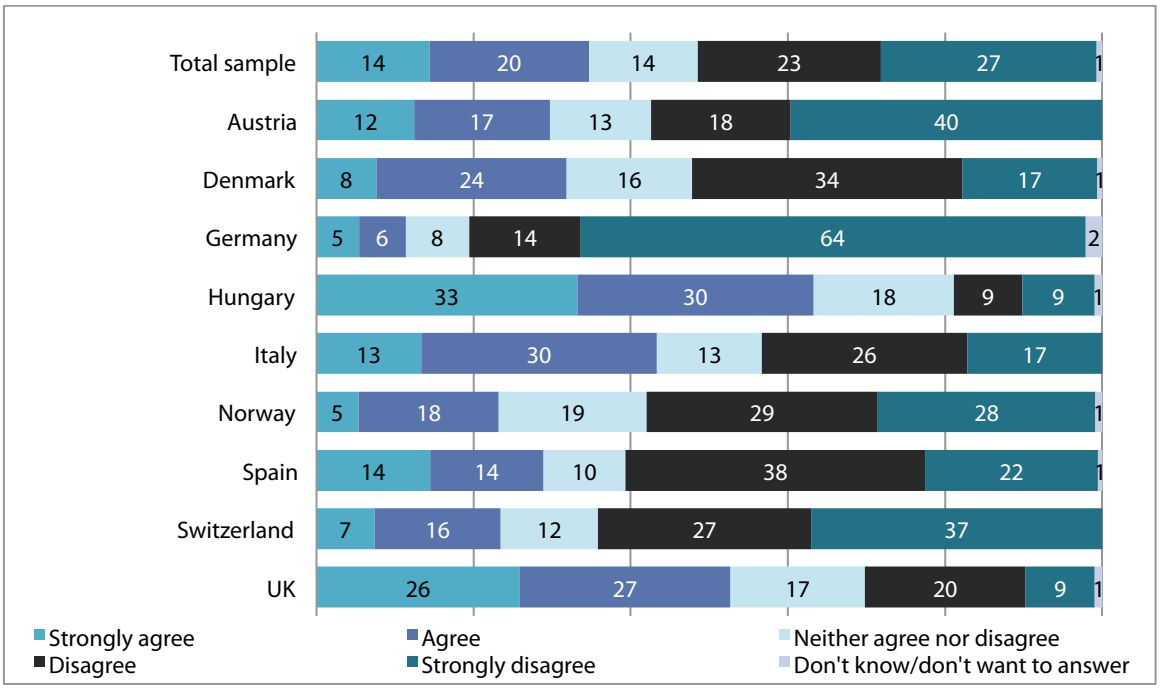

Figure 28: "If you have done nothing wrong you do not have to worry about surveillance-oriented security technologies" (percentages)

4.6.1 Demographic relations

Regarding age and the nothing to hide perception elder persons between 60 and over 70 somewhat tend to agree more; while in total values this is only visible in the age category over 70. The highest disagreement to the "nothing to hide" argument is given in the age groups between 30 and 49.

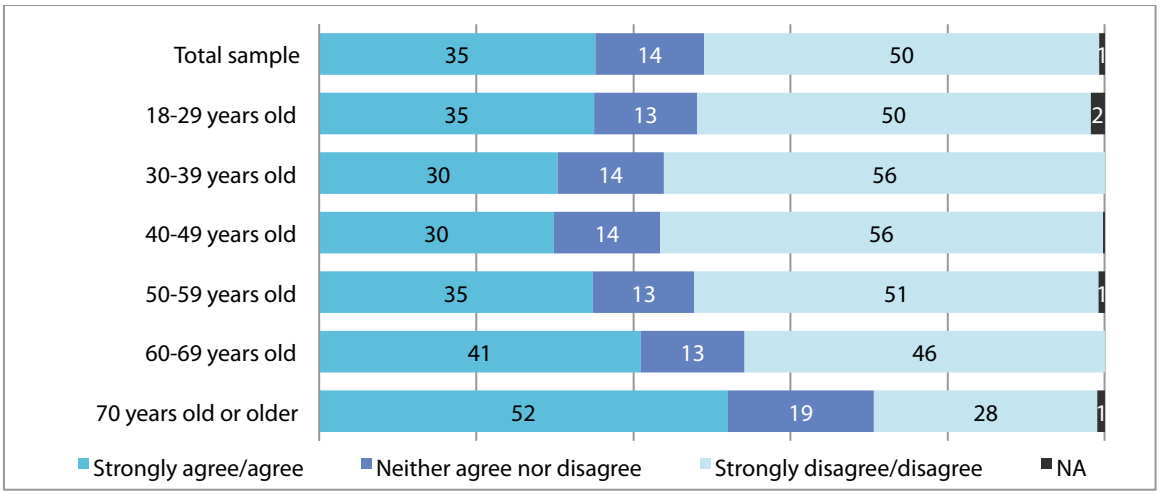

Figure 29: Nothing to hide (dis-)agreement related to age (percentages)

Education makes a difference for the dis/agreement: the amount of "nothing to hide" opponents significantly increases with the level of education.

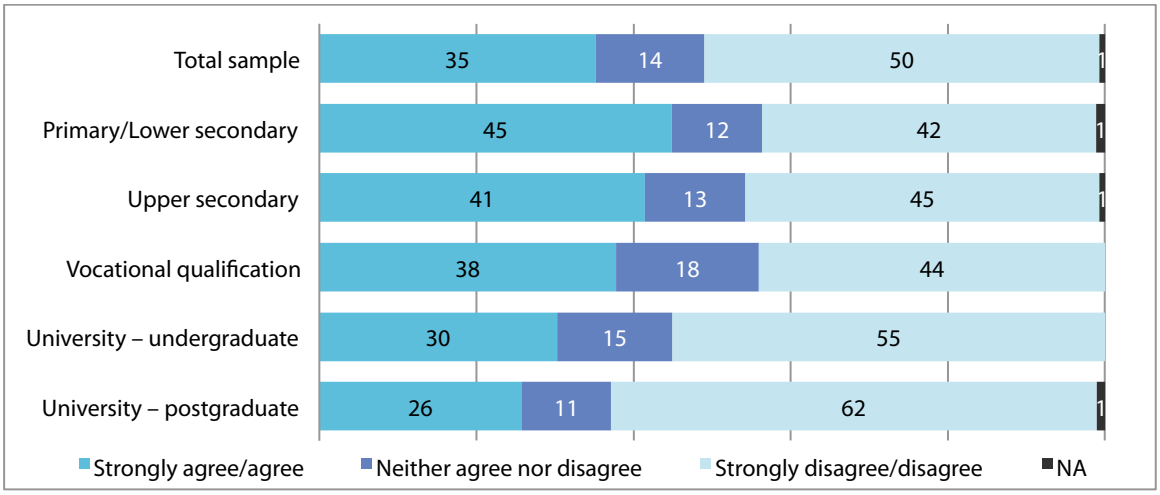

Figure 30: Nothing to hide (dis-)agreement according to highest level of education (percentages)

4.6.2 Nothing to hide but high concerns about information abuse

As mentioned above, 50% of the participants disagree with the statement "If you have done nothing wrong you do not have to worry about surveillance-oriented security technologies" and only 34% share this view (Figure 28). At the same time, there are high concerns expressed about the misuse of personal information such as too much information is being collected (see figure below), information used against them and information shared without the permission of the concerned individuals (see the figures in section 4.4).

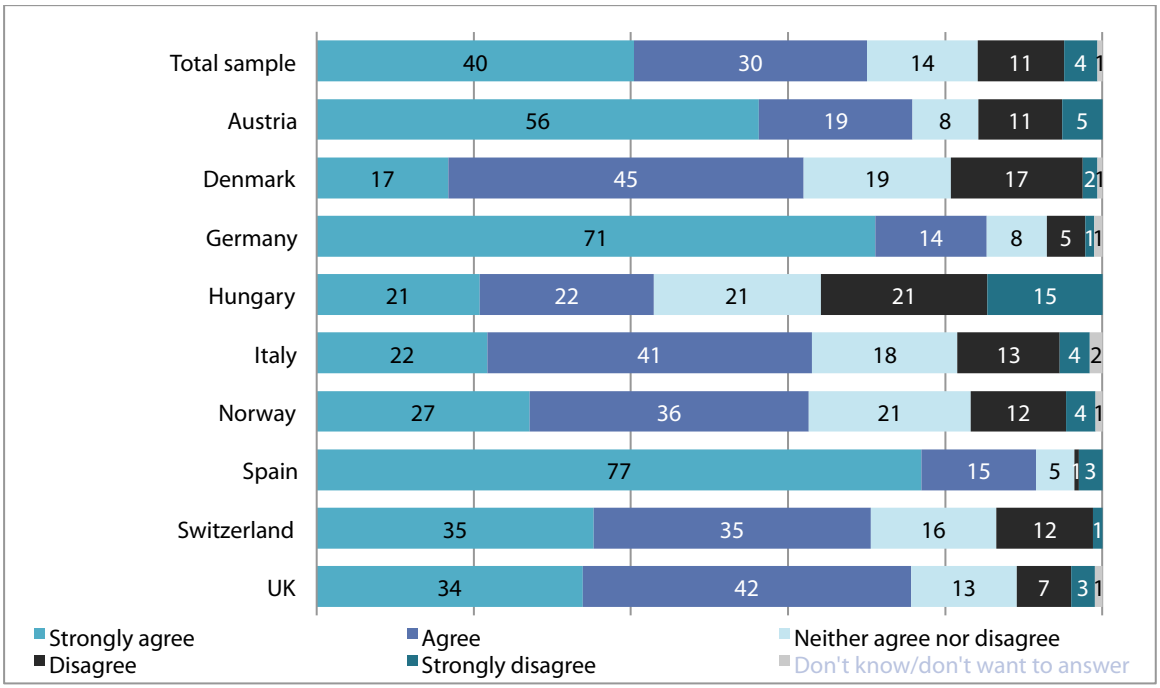

Figure 31: "I am concerned that too much information is collected about me" (percentages)

To explore further whether there are differences in the perceptions of the agreers and opponents of the "nothing to hide" argument, we cross-linked these results with those about the concerns about information misuse. This reveals some contradictions in those agreeing to the "nothing to hide" argument: on the one hand, with about 85% there is an expected correlation between the "nothing-to-hide" opponents (i.e. participants worried about SOSTs also when perceiving to have nothing done wrong) and participants concerned about extensive information gathering. However, more than half (52%) of the "nothing-to-hide" supporters (i.e. those participants agreeing to have nothing to fear from SOSTs if they have done nothing wrong) are at the same time concerned that too much information is collected about them. Hence, even those believing to have nothing to hide in the first place are concerned about extensive information gathering.

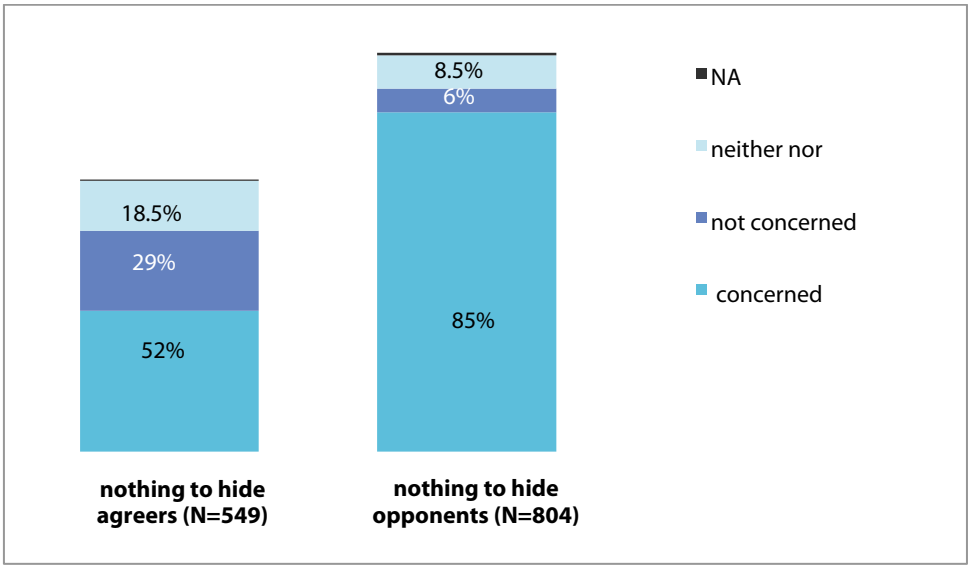

Figure 32: Nothing to hide and concerns about information collection

Figure 33 underlines the point as 54% who claim not to be worried if nothing is done wrong at the same time are concerned that their information is used against them.

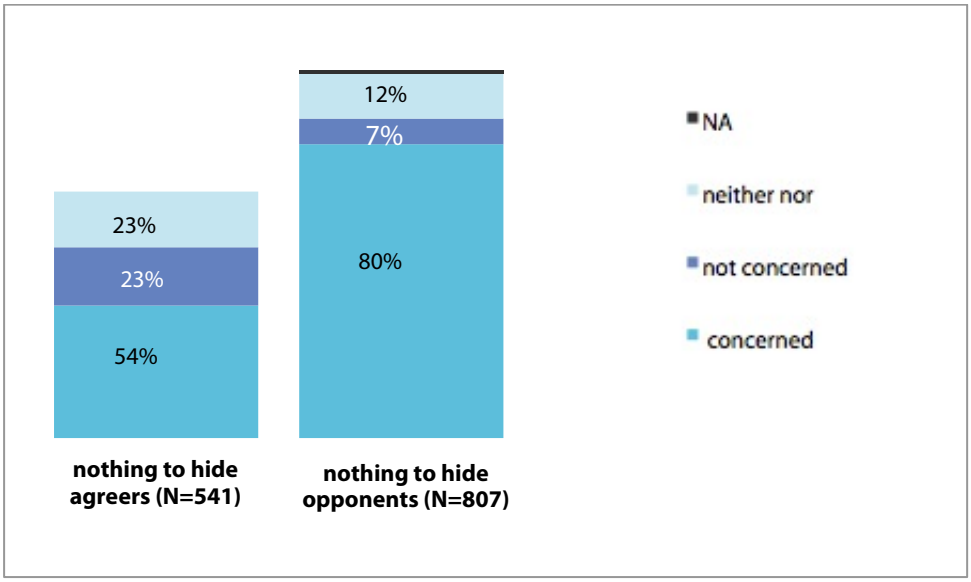

Figure 33: Nothing to hide and concerns about information might be used against me

The very high rate of 83% being concerned that their information might be shared without their permission (Figure 34) further indicates that the "nothing to hide" argument is not appropriate for the participants to deal with the relations between surveillance, security and privacy. Such a line of argument seems to be neglected also because it is perceived as rhetoric that rather veils than reveals the reasons for the use of SOSTs. The argument narrows privacy to hiding personal information. However, privacy is not least also linked to trust that others respect private life and do not intrude into it against the will of the individual. It does not matter if one has things to keep secret or not, but it does matter if personal information is collected and for what purpose. If this is opaque this then triggers more insecurity and mistrust (see section 4.7.).

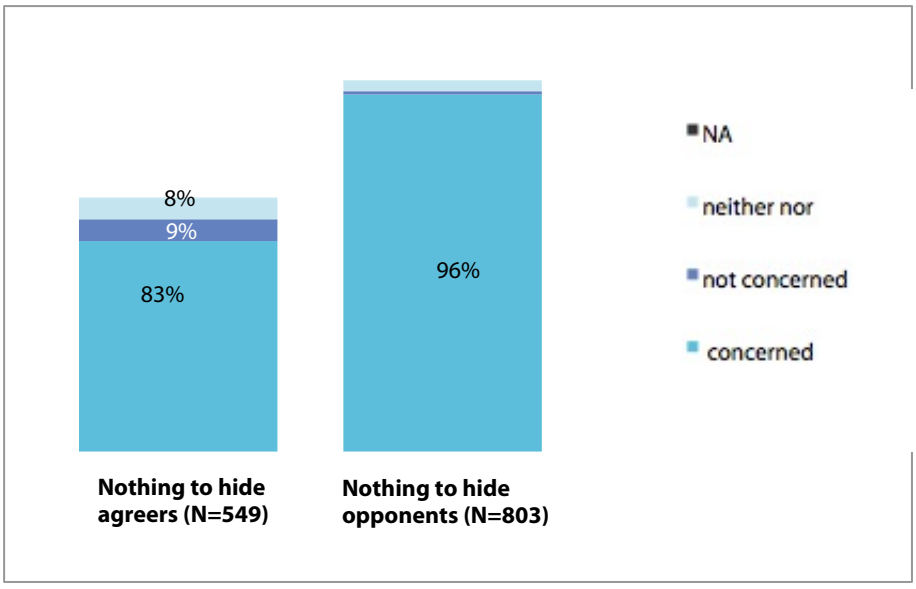

Figure 34: Nothing to hide and concerns about information might be used without my permission

4.7 Remarks on the privacy-security trade-off

One aim of SurPRISE was to re-examine the role of a trade-off between privacy and security that sees infringement of individual privacy as an acceptable cost of enhanced security. Similarly, citizens are assumed as willing to trade their privacy for enhanced personal security in different settings. This trade-off operates on two levels: on a political level it frames privacy as a barrier to effective security measures and justifies privacy intrusions as necessity to improve security; on an individual level, it suggests that individuals gain more security but only if they accept privacy intrusions.[90] While security policy and technology developments are often based on this trade-off model, the validity of such a model is increasingly questioned, suggesting that it over-simplifies the relationship between privacy and security.

Several scholars have pointed out that the framing of a trade-off between privacy and security complicates the task of developing approaches that consider that both concepts are related in a complementary way to some extent.[91] A trade-off in general implies a contradiction between two items indicating that one is given up in order to gain the other.[92] The privacy-security trade-off is based on the assumption that the implementation of security measures makes a certain amount of privacy intrusion per se necessary in order to come to a certain level of security. In this sense it reduces the relation between privacy and security in general to a state of permanent conflict. Privacy intrusions are presented as the only option to improve security. In this sense it narrows the view on security measures as it neglects to consider that there might be options that do not intrude into privacy. Thus, the trade-off is based on a misleading assumption which is also not determined in legal regulations and fundamental rights catalogues. As a norm, privacy defines a state where an individual is free from interference and legal norms[93] only allow interference of privacy under certain conditions, i.e. to fulfil public interest and this must be in accordance with the law and necessary in a democratic society to protect its foundations. In short, interfering into privacy is foreseen by the law as a possibility but always as the exception to the rule but by no means as permanent option.[94] Thus, a setting in which the implementation of security always entails privacy intrusions as standard mode is misleading as it falsely frames security as a concept that has to intrude into privacy without assessing alternative options. To this end such an assumption would raise the exception to the rule to the norm, (i.e. privacy interference as inevitable for security). To some extent such a trade-off is also linked to the transformation of security policy towards a broad understanding of security that spans across a variety of domains in line with securitization (as outlined in Section 2). Particularly, securitization can lead to an increase of exceptional security states where more intrusive security actions (e.g. dragnet investigations, mass surveillance, cooperation between military and police forces) are justified than in normal, rule based situations.[95] The broad interpretation of

---

90 EGE - European Group on Ethics in Science and New Technologies (2014): Ethics of Security and Surveillance Technologies. Opinion No. 28 of the European Groups on Ethics in Science and New Technologies. Brussels, 20 May 2014. P.79

91 Cf. D. Solove (2011): Nothing to hide: the false tradeoff between privacy and security. Yale University Press. New Haven and London.
H. Nissenbaum (2010): Privacy in context – technology, policy, and the integrity of social life. Stanford University Press. Stanford, California.
Pavone, V. and S. Degli Esposti (2012) "Public assessment of new surveillance-orientated security technologies: Beyond the trade-off between privacy and security " Public Understanding of Science 21(July): 556-572.

92 Cf. EGE - European Group on Ethics in Science and New Technologies (2014): Ethics of Security and Surveillance Technologies. Opinion No. 28 of the European Groups on Ethics in Science and New Technologies. Brussels, 20 May 2014.

93 Such as Article 8 of the European Convention on Human Rights, Article 12 of the Universal Declaration of Human Rights or Article the European Fundamental Rights Charter

94 The European Court of Human Rights declared that "[m]ere storage of information about an individual's private life amounts to interference within the meaning of Article 8 (right to respect for private life) of the European Convention on Human Rights. European Court of Human Rights (2014): Factsheet - data protection http://www.echr.coe.int/Documents/FS_Data_ENG.pdf

95 Cf. B. Buzan, O. Weaver, J. de Wilde (1998): Security: A New Framework for Analysis. Lynne Rienner: Boulder, 1998.
T. Balzacq (2005): The three faces of securitization: Political agency, audience and context. In: European Journal of International Relations 11(2): 171-201

security that leads to a limitation of privacy is a worrying development, "which risks becoming a 'catch-all' clause"[96]. This fosters a conflicting view on the relation between privacy and security and therefore liberty and security suggesting that tensions between these concepts would inherently exist. Such a view dismisses that liberty is the defining value for privacy and security: "democracy, the rule of law and fundamental rights are designed to protect the liberty of the individual within the society."[97] Thus security is only a tool to support freedom and liberty but can never be a value on an equal or superior level and privacy understood as a state free from interference represents a form of liberty, namely autonomy.[98] Against this background, a trade-off model based on this assumption that privacy has to be weighed against security risks neglecting the fact that security is subordinate to liberty and liberty is the superior linkage between both – privacy and security. The prominent role of liberty and freedom in legal frameworks is thus no coincidence but underlines this aspect.[99] The individuals' "rights must not be 'traded' but, quite the contrary, must restrict the trade-off".[100] Thus a model is needed "that does not give up any of the rights, even though it acknowledges that priorities may differ not only between individuals but also differ in different contexts"[101]. The important questions therefore are about how privacy and security can both be respected. In those cases where conflicts occur, it is not a matter of giving up privacy or security but of prioritizing rights in a way that considers different contexts and the individuals concerned.

It is thus important to come to a better understanding of how individuals perceive the interplay between privacy and security. The results of the SurPRISE citizen summits presented in the previous sections contribute to that and draw a different picture than the dichotomized view of the trade-off suggests. First of all, the assumption of a trade-off makes sense only if an inherent conflict between intrusiveness and effectiveness of a security measure is assumed. In other words: If there is no privacy intrusion resulting from a security measure then there is no trade-off. If there is a privacy intrusion and no effectiveness of a security measure there is also no trade-off. A trade-off only occurs if the effectiveness of a security measure cannot be gained without privacy intrusion. However, in this case, it needs to be assessed whether there are no other options to receive the effectiveness and to what extent privacy intrusion is necessary and if it is in accordance with the law. The results regarding intrusiveness and effectiveness of the SOSTs indicate that this is a crucial issue for citizens. Even if it is assumed that SOSTs benefit security, the concerns about privacy intrusions are mostly rated higher than their effectiveness. The high concerns about information collection and abuse of personal information indicate that people are more greatly concerned about trading their information than accepting such a trade. This is also the case among those people who seemingly agree to the "nothing to hide" statement as the same concerns were expressed. Even those who share the opinion, that if one has not done anything wrong there is no need to fear SOSTs do not want to be subject to surveillance. On the contrary, they are greatly concerned about information abuse and privacy infringements. All together, these results indicate that there is a need to move beyond a trade-off framing. The exploration of the citizens' perceptions on SOSTs from an angle that considers the relation between effectiveness and intrusiveness enabled a more differentiated perspective on privacy and security than the trade-off model. Because it allows us to take a closer look at the potential effects of SOSTs: SOSTs can have different levels of effectiveness for security with different levels of intrusiveness for privacy, both or neither but there is no inherent necessity to intrude privacy to improve security. Such a more differentiated view is crucial but hindered by a trade-off framing. Further research is needed to explore this more in-depth and gain additional insights into how effectiveness and intrusiveness relate in the privacy-security domain in order to develop approaches that better correspond with the privacy-security interplay. The high number of privacy concerns expressed in the results clearly shows that privacy intrusions are not per se acceptable to citizens. Here, the "why" is important: the fears and concerns about privacy infringement, abuse of power and the lack of trust underlines the crucial role of

96 EGE 2014 op. Cit. P. 38.
97 Guild et al 2008, 9
98 Cf. Nissenbaum o.p. cit. P. 81
99 For a legal (US-based) discussion on the roles of so-called "preferred freedoms" to ensure a social and democratic state of law, see The Oxford Companion to the Supreme Court of the United States, 2nd edition, K. L. Hall (ed.), Oxford University Press, New York, 2012.
100 EGE 2014 op. Cit. P. 84
101 ibid. P. 85

transparency and accountability in the relation between privacy and security. Hence, transparency and accountability might be linking concepts to overcome the dichotomized view on privacy and security and the trade-off. Because effectiveness of SOSTs is not just believed but needs to be verifiable and their intrusiveness needs to be controlled with respect to fundamental rights. Closely related to this is the role of trust which is dealt with in the following section.

4.8 Trust and trustworthiness

Several of the views and concerns presented in the previous sections underline that trust is an essential aspect also strongly linked to the acceptability of technologies and measures. Trust is a mutual and complex concept that needs a strong foundation to prosper. If this foundation gets shocked or irritated then trust can be cut back to a relatively low level. The results shown in figure 33 reveal some amount of insecurity and uncertainty among the participants as regards how to establish trust. While several respondents perceive security authorities as trustworthy (36% smart CCTV, 36% DPI, 46% SLT), there is a strong tendency to disagree with the statement that security authorities do not abuse their power, 46% in case of smart CCTV, 34% for SLT and 52% regarding DPI. Thus, the participants expressed a high fear about the authorities abusing their power and infringing fundamental rights.

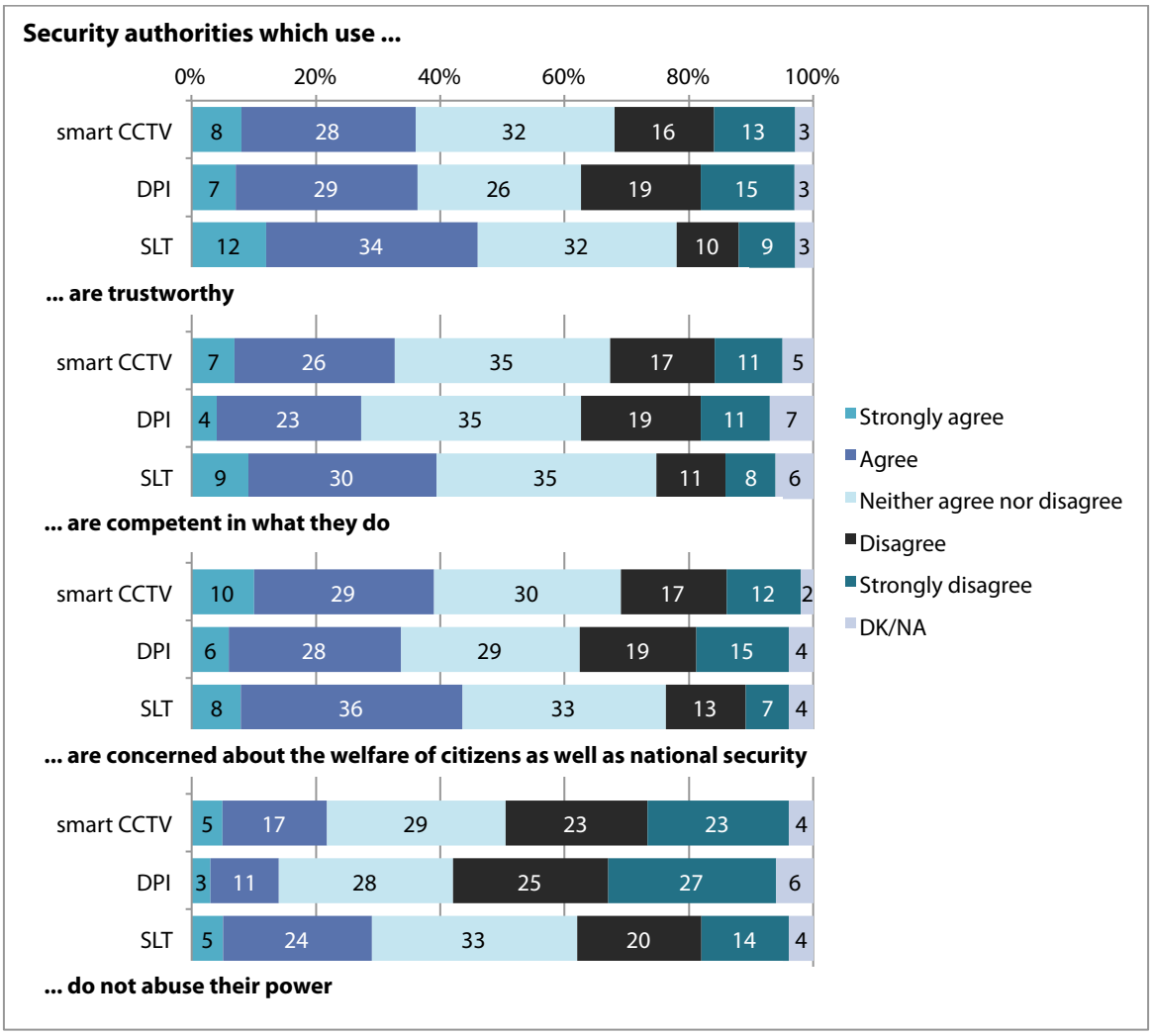

Figure 35: Trustworthiness of security authorities (percentages)

Besides the high concerns, with over 30% in most of the items this set of results shows the highest "neither/nor" values in the whole survey. This underlines that trust and trustworthiness are highly controversial issues for the citizens in the context of SOSTs and related practices. Some explanations can be found for these controversies in the table discussions: as shown in the previous sections, the majority of participants perceive the use of SOSTs as very intrusive and (linked to that) as rather ineffective. The high concerns about the misuse of information gathered by surveillance technologies also raise according concerns about function creep and security authorities conducting these technologies abusing their power. For the participants trust is tightly related to a perceived lack of accountability and oversight of security authorities and surveillance practices. People would like to trust but perceive a lack of common grounds on which to build their trust. This is aggravated by perceptions that security and surveillance measures implemented by the according authorities are based on mistrust in the citizens. As a consequence, citizens feel more insecure and uncertain about SOSTs and security authorities themselves.

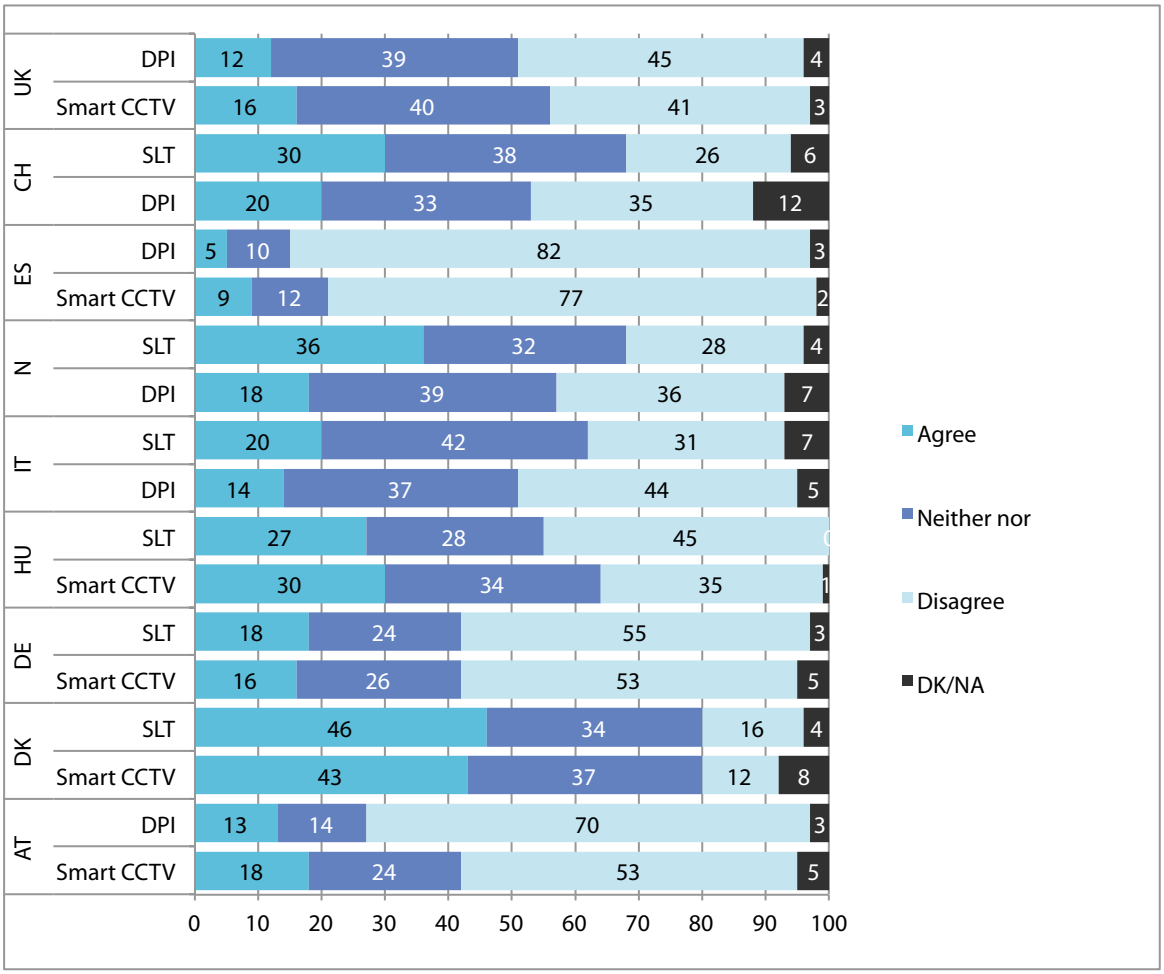

Figure 36: "Security agencies which use ... do not abuse their power" (percentages) country results (percentages)

A look at national results reveals an even more controversial picture as the neither/nor positions here are in some cases near to 40% and more distinct concerns about power abuse are visible. Here also cultural differences play a role with a somewhat higher amount of trust in Scandinavian countries Denmark and Norway where the fear of abuse seems to be lower than in other countries. However, at the same time, these countries are among those with the highest neither/nor values. Hence, the higher basic level of trust in these countries seems to be not least a cultural phenomenon while the privacy

concerns remain relatively similar to those in other countries. Despite of the national peculiarities these results clearly point out that trust is among the core issues in the privacy-security discourse.

The role of alternatives

In line with the high concerns about fundamental rights abuses and complicated situations regarding trust and trustworthiness the participants expressed a need for alternative approaches without surveillance. A comparison between the perception in this regard in the beginning and the end of the summit was conducted to explore whether the qualitative parts of the summit brought new perspectives in this regard. In the total sample the perceived need for alternatives increased from 61% in the beginning of the summits to 67%. An according tendency is also visible in the countries although with different characteristics due to cultural peculiarities. The only exception is Italy, where the expressed need for alternatives slightly decreased. This is explainable with increased uncertainty and perceived lack of options to come to alternatives. Widely similar to the items on trust in these results the neither/nor positions are also relatively high. This is no coincidence as these are interrelated issues: if there are insecurities regarding trust in the security authorities then it is likely that insecurities also occur regarding the realization of alternatives by these authorities. The national differences also widely correspond with those in the items on trust and trustworthiness. During the discussions, a certain feeling of desperation and perceived lack of ability to act against surveillance was expressed by several participants. Some discussants were angry and worried about surveillance and SOST usage without even considering what people think. In the discussions it also became clearer that alternatives are not merely meant in a technical or operational sense but also imply a need for change in the way security policies and measures are developed and enforced. For a number of participants this is also related to a need for more social responsibility and solidarity among the citizens as well as the authorities.

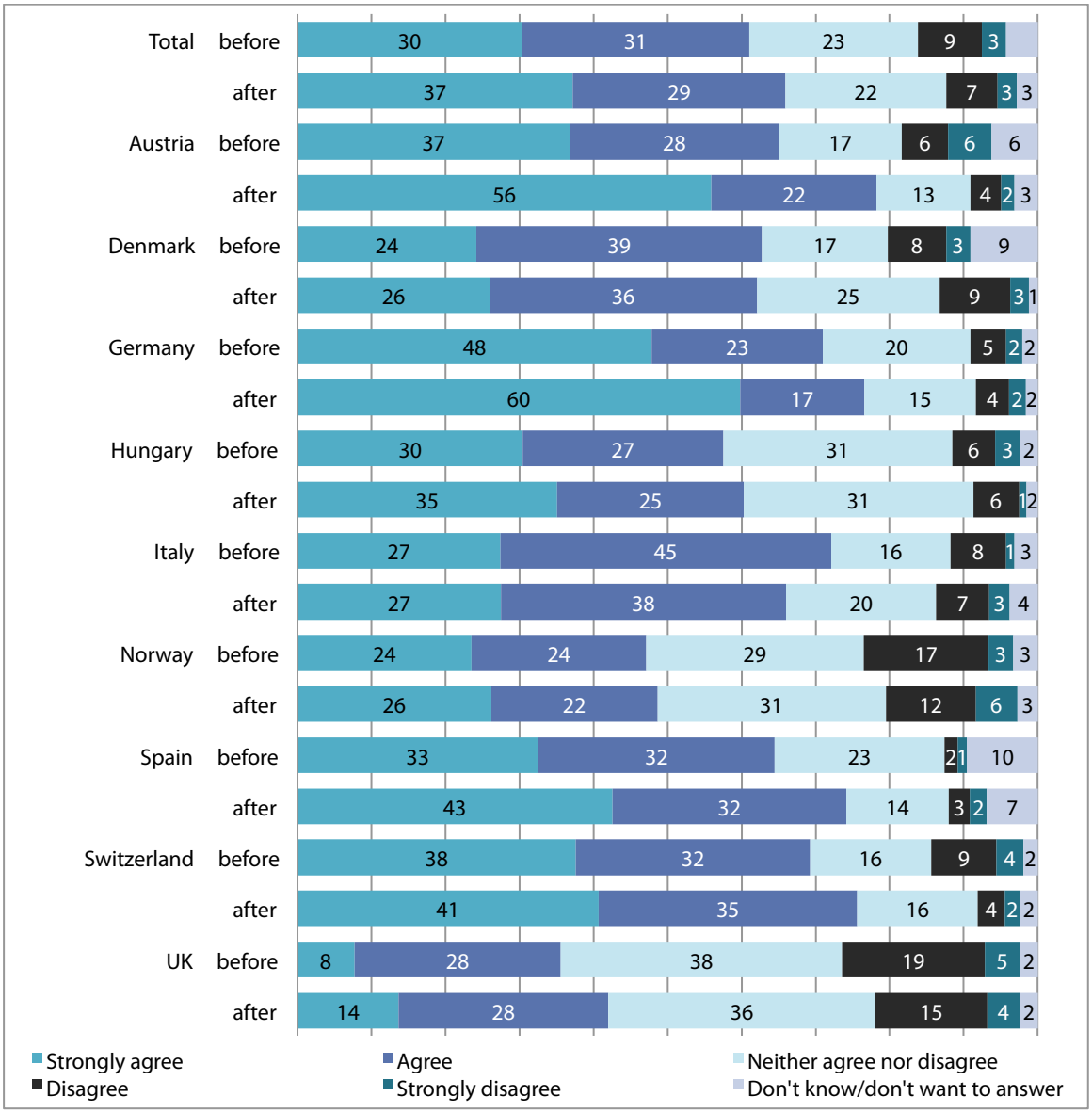

Figure 37: "Alternative approaches to security, which do not involve surveillance-oriented security technologies should be given higher priority" – answers given before and after the event (percentages)

5 Major outcome of table discussions and recommendations to European policy makers

The qualitative data gathered at the citizen summits enrich the statistical results presented in the previous sections and mirror the opinions and concerns of the quantitative data. Despite the national peculiarities and the different results in the nine countries the participants of the SurPRISE citizen summits discussed and elaborated a variety of similar issues and recommendations relevant to policy makers. The main implications of these discussions and recommendations presented in this section are the outcome of the iterative analysis and synthesis based on the following major elements: the quantitative and qualitative data gathered during the nine citizen summits, i.e., the general and specific perceptions of the summit participants on privacy, security and surveillance; the factors and criteria developed in the analytical framework and the technological, legal and political issues relevant in the security-privacy-surveillance discourse explored in SurPRISE. To get additional perspectives on policy-relevant issues the recommendations were also discussed with international experts from different fields during a stakeholder workshop. The investigation of the recommendations also included a reduction of redundancies which were naturally given as the majority of participants in each of the participatory events dealt with similar problems and challenges. This section now presents a summary of the core issues identified in the analytical process combing citizens' and policy perspectives.

Above all, the major recommendation and demand of the citizens includes a reduction of surveillance, improvement of transparency, accountability and democratic scrutiny of SOSTs and practices, of the involved authorities as well as more checks and balances.

Beyond the trade-off - both privacy and security matter

The trade-off model is based on the assumption that the employment of security measures requires privacy intrusion in order to come to a certain level of security. This logic inherently operates as if privacy intrusions would be the only and inevitable option to effectively improve security. Consequently, the view of security measures is also narrowed, as it is neglected that there might be options that do not intrude into privacy. In short, this suggests that if one accepts security and surveillance measures, one has also to accept privacy intrusions. The results of the summits in total show that participants do not follow this argumentation: citizens neither want to fear security measures nor lose their privacy. Hence, they deem the view on a trade-off between privacy and security inappropriate because both the effectiveness of security measures and the protection of privacy suffer from such a view as the perceived high intrusiveness of SOSTs decreases its effectiveness. Citizens are aware that SOSTS are to some extent important and necessary to ensure public security. The effectiveness of SOSTs was not thoroughly doubted but is overshadowed by scepticism and uncertainties due to a perceived lack of control, accountability, fears about abuses of power and function creep. As for the citizens, it remains widely unclear in which contexts security and surveillance measures are used and it is also unclear whether these measures effectively contribute to public security. At the same time, the intrusiveness of the technologies and measures is perceived as very high and reinforces the risks of erosion of privacy for the individuals as well as society as a whole. Thus, the citizens expressed a need that the purpose and usage of SOSTs needs to be based on plausible reasons and backed by objective and comprehensive evaluation. Instead of trading one against the other they highlighted a demand for effective security measures that are in accordance with an effective protection of their privacy. In this regard, citizens favour security policies that do not entail untargeted surveillance practices and avoid the extensive use of surveillance-oriented security technologies. This request mainly addresses a demand for a limitation of pre-emptive measures that put individuals under suspicion without concrete and plausible indications.

Regaining trust with limitations to surveillance

Along these lines, a variety of recommendations and suggestions aim at improving mechanisms to control the work of security authorities and ensure that their actions are in compliance with fundamental rights. A great degree of uncertainty regarding trust in institutions employing SOSTs also derives from the discussions and recommendations as the vast majority expressed unease and concerns about information abuse as well as extensive and uncontrolled power. A number of citizens stated to feel exposed to mass surveillance. Many concerns relate the tenet whereby innocent people should not be subjected to intrusive measures, referring to the presumption of innocence, which is a core principle of justice systems. Participants expressed fear that mass surveillance may erode this principle, and that, as a consequence, everybody could become suspicious. Hence, a gap between surveillance under known or plausible suspicion and untargeted surveillance of the masses was seen as critical problem. To deal with this problem, many argued there ought to be more control over surveillance activities, and they demanded justified grounds for surveillance in order to target real suspects and criminals instead of the general public. Mass surveillance is also perceived as inefficient, in that it raises costs and errors, and brings few security benefits. Citizens request greater prior evaluation (and accordingly information) of purposes, appropriateness, costs and impacts of SOSTs and surveillance practices, pursuant with the principle of proportionality. Hence participants request investing more in transparency and accountability in order to control and verify what data and information is being collected, who is responsible and allowed to gather and use it and for what purposes they are intended and why.

Strengthening accountability and effective enforcement of privacy legislation

To reduce the risks of privacy infringement, citizens called for regulatory measures limiting the use and collection of data gathered through SOSTs to an acceptable level, and only allowing access to data following a court's decision. In general, a need for stricter laws to control the implementation of SOSTs and practices was raised many times. In this regard, more severe punishment was recommended for authorities and commercial actors breaking the law. For the enhancement of transparency and accountability of SOSTs and the authorities using them, citizens suggest more information to be provided to the public as well as evaluation of surveillance measures to verify if they are necessary and in accordance with legal principles. In a number of discussions the participants argued that information to the public should include information about the source, scope and purpose of personal data collection, means of data processing, retention period, who/which institutions are involved in the processing and who can access it for what purposes; to reduce the risk of abuse legal limits should be set for the timely duration of processing and storage of information; without concrete suspicion, data should be deleted and only data on proven criminals should be stored. In line with informational self-determination a number of participants also expressed a desire to more information and control about their personal data that security authorities and other institutions hold about them.

The problems of different legal frameworks for privacy and data protection and the gathering of digital information were also addressed. A need was identified for an international or at least European law to ensure that fundamental rights are enforced more effectively also beyond national borders and to restrict the commercial use of personal data. It was also expressed that private companies should not be involved in operating SOSTs and not allowed to access and use data produced by these technologies. Citizens are in favor of a privacy framework that includes sanctions in case of privacy infringement. To some extent this demand for a legal framework is in line with the ongoing data protection reform in the European Union. Several participants also voiced concern that the law often lags behind the technology. Reasons mentioned for this were that technologies are rapidly developed and introduced without considering the law. Here a certain demand was identified to also ensure that the development and implementation of technologies respects privacy and remains within the rule of law. To fill this gap between laws and technology across all countries citizens would like to see independent authorities that effectively control the implementation and use of SOSTs and ensure that privacy is respected and not undermined. In order to cope with technological development also laws should be regularly checked to establish their appropriateness to cope with emerging technologies. Regular evaluations prior to technology usage, i.e. already during the development process of technologies, were identified as meaningful to reduce the risk of technologies that go beyond legal regulation.

Reconsidering the role of public security authorities and root causes of security matters

Although citizens voiced strong concern, they did not reject SOSTs per se, but rather insisted that police and other security authorities work properly on behalf of the interest of the public with means that are in accordance with the law and privacy principles. Security and surveillance measures were perceived as being too extensive and untargeted. Thus, citizens demand less surveillance, and more focus on effective and less intrusive security measures that do not undermine collective and individual privacy. In this respect, participants recommend to improve the capability of security authorities to deal with contemporary security problems. In the views of citizens, this also requires more training and qualified security forces instead of an extensive use of SOSTs. Some citizens criticized the often unconditional faith in technology and were in favour of less technocratic and more humanistic approaches. In this regard, the citizens are in favour of more investment in social justice and education. Instead of deploying more surveillance-oriented technology, issues were raised that the qualification and training of staff of security authorities should gain higher priority.

This prioritization is not just meant in a sense that security forces can better react to security threats but in a wider sense to enable incorporating also the root causes of security problems in order to come towards more constructive security approaches. In several discussions a need for change in security policy was expressed that does not threaten privacy of the general population. Instead security policy should be more open to public scrutiny and should consider positive measures to understand and combat the reasons for crime and security threats. Besides this general need some participants also discussed and suggested focusing more on combating large-scale financial fraud and tax crimes instead of untargeted mass surveillance. For the majority of citizens, issues such as economic stability, employment, social coherence and solidarity are of vast importance for security and safety. In this regard, they identified a need for measures to deal more with these issues as SOSTs do not eradicate social and economic problems.

Greater transparency and oversight as alternatives

In a similar vein, citizens recommend the adoption of alternatives, not only understood as replacements of SOSTs, but also as strategies to minimize the unease brought about by surveillance activities. The majority of participants lament the lack of information on the rationale behind the employment of SOSTs, the way in which they are used, and the authorities making use of them. Hence, citizens strongly demand improving accountability and responsibility of public security authorities for the employment of SOSTs.

In a sense of "who watches the watchers?" the responsibility of the authorities to operate SOSTs and treat the gathered data in an ethical way within the rule of law was emphasized. This also implies that SOST usage should be based on proven evidence for its efficacy so that it is comprehensible why and for what purposes the technologies are used. In relation to this it was also mentioned that the costs of security and surveillance should be controlled and made available to the public.

To improve accountability and transparency, citizens demanded the creation of independent oversight bodies able to scrutinize the proper use of security technologies and related practices within the limits of the law and to ensure the implementation of the principle of proportionality. In particular, several participants recommend creating ethic commissions and reinforcing authorities that ensure privacy and data protection, in order to reduce privacy intrusion and implement security measures in accordance with fundamental rights. Some participants suggested that these bodies should consist of different experts (such as legal and technical experts, scientists, sociologists, philosophers etc.) and members of the civil society. As regards the tasks of the oversight bodies it was argued that they should be in charge of overseeing the processing of personal data for public security purposes, and entrusted with the power to sanction violations of citizens' rights. Most recommendations proposed the creation of a European institution, whereas some suggested locating it at the international level. Some suggested that the processing of personal data should be authorized by a judicial authority and surveillance limited to cases where concrete suspicion of criminal activities is proven. In addition it was voiced that this institution should also be protected against political power in order to remain independent. To effectively safeguard citizens' privacy, such a supervisory authority should be well equipped in

competences and resources. These demands for effective oversight widely address the role of data protection authorities and the lack of knowledge about these institutions in the public.

The recommendations that were proposed cluster around major themes, synthesized in the following:

- Reducing and constraining surveillance technologies and practices
- Improving checks and balances and prohibiting mass surveillance
  - Security measures must be limited and targeted, and the use of SOST must be backed by judicial authorizations
  - Enhancing compliance of law enforcement authorities with fundamental rights principles
  - Reinforcing independent data protection authorities to scrutinize security and surveillance measures
- Enhancing transparency, information and participation
  - Increasing accountability of bodies pursuing security and implementing surveillance measures
  - Involving civil society and human rights bodies in the elaboration of security policies
- (Re-)considering the human factor
  - Strengthening social cohesion, economic justice and social responsibility of institutions and individuals
  - Raising awareness and education among the public on privacy and security issues
  - Investing in training and greater expertise of security authorities and personnel
- Fostering privacy research and innovation
  - Fostering innovation for privacy by design as integral components of technologies
  - Strengthening security and privacy standards (e.g. encryption) in technology development and usage
  - Fostering the role of science and research particularly as regards alternative approaches

6 Summary and Conclusions

The roles and meanings of both privacy and security have been confronted with several challenges in different but closely linked domains. An increasingly complex global security landscape has triggered paradigm shifts in international and European security policies including a number of security measures trying to cope with new challenges. At the same time, also the landscape for privacy expands rapidly and leads to increasing complexity of fundamental rights and data protection in the information society. While the claim for an extended, more holistic security approach is partially reasonable to deal with complex threats, it also reinforces and complicates possible tensions between security measures and privacy. A strong shift is observable towards more pre-emptive security measures and technology-aided surveillance practices that are amplified by political, economic and societal issues. That these shifts are also perceived by the European citizens is reflecting in the results of the SurPRISE summits which highlighted a number of concerns and fears about security and surveillance, extensive privacy intrusions and data collections that seem to have reached a level that is no longer acceptable for many citizens. The results do not indicate a general undifferentiated rejection of security measures: the participants expressed understanding for a certain need of measures that to some extent include the use of SOSTs. In this regard, the relation between the effectiveness and intrusiveness of surveillance-oriented security technologies as an important aspect coming into play which is a key issue also for acceptability: Firstly, if a technology is perceived as too intrusive then the perceived effectiveness also decreases. SOSTs and security measures are not perceived as means that certainly lead to more security. On the contrary, the extensive use of SOSTs can also entail a state of increasing insecurity in the public. Here, the intrusive capacity of a technology and the associated practices affecting different types of privacy play a crucial role. Secondly, this then also leads to a decrease in the acceptance and acceptability of the technology. Considering this relation between technology and practices is important as the enormous concerns raised go beyond a simple concern about technologies. Instead, serious criticism was expressed at the summits about security policies following a path that led to a deeper intrusion of privacy and reinforces the framing as a trade-off with security. The assumption that the trade-off framing to some extent oversimplifies the relations between security and privacy is widely confirmed with the results. Citizens understand that privacy intrusion is not always avoidable and sometimes necessary for security and surveillance measures to be effective. However, *not* as a default practice and *by no means* in every case but *only* if no other option is available. A number of concerns expressed relates to fears about a loss of autonomy such as the perception that "SOSTs are forced upon me", information being shared "without my permission", or "used against me" and the fear of authorities abusing their power. This points out that privacy is closely linked to autonomy and the risks caused by intrusive security and surveillance measures thus go deeper than a narrow view on privacy (as the right to be left alone) suggests. In the trade-off model privacy intrusion is framed as something that is simply inevitable and that does not really put much at stake. However, there is much at stake if a trade-off between security and privacy, hence liberty, is simply accepted and not scrutinized: It is nothing less than the cornerstone of a free and democratic society.[102] Scrutinizing the costs and the effectiveness of security and surveillance is a minimal requirement that is often not even met. Hence, there is need for assessment that addresses questions such as: "What is gained, what is lost, by whom, how is this framed, measured and shared, by whom, and how is this articulated to decision-making processes[?]"[103] Hence, reinforcing privacy by design and by default in SOSTs and fostering privacy impact assessments are important measures to reduce privacy intrusions and limit the accordingly high risks.

Besides the identified need for change in security policy and the implementation of the associated measures it also became apparent that there is a need also to focus on the root causes of security matters. As outlined in Section 2, European citizens are mostly concerned about the economic crisis and the related instabilities in national and international economies as well as social insecurity. While pre-emptive security and surveillance measures gain high priority, measures to tackle issues on root causes, social and economic inequalities seem to be underestimated and not sufficiently addressed by policy makers in the views of the citizens. This was particularly underlined in those countries affected more by

[102] EGE 2014 op. Cit. P. 79
[103] Ibid p. 84

the economic crisis (such as Italy or Spain). To some extent this refers to a spill over effect in a sense that the despair and anger about the difficult economic situation in the countries was also expressed in the summits. However, this by no means implies that the expressed concerns and fears about privacy abuse can be relativized. Especially not because these privacy concerns are widely similar across all countries; including those that encounter less serious economic issues. What this implies is that, for citizens, issues such as economic stability, employment, and social coherence are of vast importance for security and safety. Citizens identified a need for more political actions on these issues that can contribute to reducing social insecurity.

Several doubts and uncertainties among the citizens are also visible as regards the work of security authorities, their practices and technologies referring to a perceived lack of transparency, accountability and trust. Trust is a core achievement of democratic societies that plays an essential role in the relations between privacy and security. The results of the SurPRISE citizen summits highlight that the current course in security policies and the use of surveillance technologies and practices hampers the formation of trust. The complex results on trust and trustworthiness in security authorities indicate that for the citizens, trust cannot simply be taken for granted at any point in time. It needs to be regularly negotiated based on a solid foundation. The abuse of power is among the most expressed fears and the rule of law is perceived as highly important to prevent from power abuse but it is barely trusted in terms of its effectivity. With lack of trust in laws and regulations, and a strong need for more information, transparency and accountability of SOSTs and the security authorities conducting these the participants pointed out that they neither want to fear security measures nor lose their privacy. Instead, there is a strong demand for a reconsideration of different perspectives that respects privacy and security more as complementary issues that are not in a natural conflict. If there are plausible reasons for some intrusive security measures they have to be communicated and open to scrutiny as demanded by the citizens. Furthermore, a need for more strict laws to control the implementation of SOSTs and practices was identified. This also refers to an implementation of evaluation frameworks for security and surveillance measures to check these against the rule of law and accordance with fundamental rights. More precisely, there is a need for privacy by design and default as a pivotal technology feature and privacy impact assessment prior to technology usage. The demand for more effective legal privacy frameworks in Europe supports the adoption of the proposed data protection reform in the European Union. The expressed need for more checks and balances and effective control mechanisms to ensure that SOSTs and related practices are in line with fundamental rights indicates some need to reinforce already existing safeguards and the institutions in charge of implementing existing regulations. In this regard national and European DPAs play an important role. The outcome of the citizen summits provide support to facilitate the partially difficult situation of DPAs regarding competences and resources and upgrade the capacities of DPAs and other oversight bodies. In general, a turn-away from mass surveillance and a reinforcement of checks and balances with more effective oversight are core issues to bring back security measures to a more acceptable level and regain the trust of the citizens to come towards approaches that consider the complementary character of privacy and security.

7 Bibliography

K. Ball and F. Webster (2003): The intensification of surveillance. London: Pluto.

K. Ball (2013): D 4.3 – "Information material and documentary films". SurPRISE Deliverable 4.3. http://surprise-project.eu/wp-content/uploads/2014/04/SurPRISE-D4.3-Information-material-and-documentary-films.pdf

D. Bigo (2000): "When two become one: Internal and external securitisations in Europe." In: International Relations Theory and the Politics of European Integration. Power, Security and Community. M. Kelstrup and M. Williams (eds.), London, Routledge, pp. 171-204.

T. Balzacq (2005): The three faces of securitization: Political agency, audience and context. In: European Journal of International Relations 11(2): 171-201

B. Buzan, O. Weaver, J. de Wilde (1998): Security: A New Framework for Analysis. Lynne Rienner: Boulder, 1998.

Charter of Fundamental Rights of the European Union http://ec.europa.eu/justice/fundamental-rights/charter

Council of Europe (2010): European Convention on Human Rights http://www.echr.coe.int/Documents/Convention_ENG.pdf

European Commission (2003). A Secure Europe in a better World – European Security Strategy. http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf

European Commission (2005): Communication on The Hague Programme: Ten priorities for the next five years – The partnership for European renewal in the field of Freedom, Security and Justice, COM(2005) 184 final, Brussels. http://ec.europa.eu/home-affairs/doc_centre/docs/hague_programme_en.pdf

European Commission (2008): Report on the Implementation of the European Security Strategy – providing security in a changing world. http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/EN/reports/104630.pdf

European Commission (2010): Communication from the Commission to the European Parliament and the Council - The EU Internal Security Strategy in Action: Five steps towards a more secure Europe. Brussels. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF#page=2

European Commission (2011). Special Eurobarometer 371 - INTERNAL SECURITY. Report Number 371.

European Commission (2011): First Annual Report on the Implementation of the EU Internal Security Strategy. COM (2011) 790 final.

European Council (1999): Tampere European Council 15 and 16 October 1999 Presidency Conclusions http://www.europarl.europa.eu/summits/tam_en.htm

European Council (2010): Communication on Delivering an Area of Freedom, Security and Justice for European citizens - Action Plan implementing The Stockholm Programme. COM (2010) 171 http://www.statewatch.org/news/2010/apr/eu-com-stockholm-programme.pdf

Council of the European Union (2005): Prüm Convention Brussels January 7 2005 http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf

ECHR - European Court of Human Rights (2014): Factsheet - data protection http://www.echr.coe.int/Documents/FS_Data_ENG.pdf

European Data Protection Supervisor (2013) Annual report 2013 http://europa.eu/about-eu/institutions-bodies/edps/index_en.htm

EDRI (2012): European Digital Rights (EDRI) EDRi's Position on the Directive https://dpreformlawenforcement.files.wordpress.com/2012/12/edri-position-papers-directive1.pdf

EGE - European Group on Ethics in Science and New Technologies (2014): Ethics of Security and Surveillance Technologies. Opinion No. 28 of the European Groups on Ethics in Science and New Technologies. Brussels, 20 May 2014.

European Parliament and Council of the Commission (2010): Charter of Fundamental Rights of the European Union. Official Journal of the European Union, 30.3. 2010. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF

European Parliament and Council of the EU (1995): Directive 95 / 46 / EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities, 23.11.1995. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=DE

Europol (2012): Data protection at Europol. https://www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf

Eurostat (2015): Eurostat news release euro indicators, January 2015 http://ec.europa.eu/eurostat/documents/2995521/6454659/3-07012015-AP-EN.pdf/f4d2866e-0562-49f5-8f29-67e1be16f50a

European Union Agency for Fundamental Rights - FRA (2010): Data protection in the European Union: the role of national Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II. Publications Office of the European Union, Luxemburg. http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf

European Union Agency for Fundamental Rights – FRA (2014): Handbook on European data protection law. Publications Office of the European Union, Luxemburg.

Rachel L. Finn, David Wright, and Michael Friedewald (2013) "Seven Types of Privacy" in Gutwirth, S.; Leenes, R.; de Hert, P.; Poullet, Y. (Eds.), "European Data Protection: Coming of Age", Chapter 1, Dordrecht: Springer. DOI 10.1007/978-94-007-5170-5_1

K. D. Haggerty and M. Samatas (eds.) (2010): Surveillance and democracy. Routledge-Cavendish, Oxon.

R. Kreissl. R. Berglez, M. G. Procedda, M. Scheinin, M. Vermeulen, E. Schlehan (2013): D3.4 – „Exploring the challenges – synthesis report".

D. Lyon (2003): Surveillance after September 11. London:Polity.

C. Norris, M. McCahill, D. Wood (2004): The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space. Surveillance & Society 2(2/3), pp. 110-135

I. Ötker-Robe, A. M. Podpiera (2013): The Social Impact of Financial Crises - Evidence from the Global Financial Crisis. Policy Research Working Paper 6703. Background Paper to the 2014 World Development Report, The Worldbank.

Pavone, V. and S. Degli Esposti (2012) "Public assessment of new surveillance-orientated security technologies: Beyond the trade-off between privacy and security " Public Understanding of Science 21(July): 556-572.

M. G. Porcedda, M. Scheinin, M. Vermeulen (2013): D3.2 – "Report on regulatory frameworks concerning privacy and the evolution of the norm of the right to privacy". SurPRISE Deliverable 3.2

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL 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, Brussels, 25.1.2012, 2012/0010 (COD)] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF

E. Guild, S. Carrera, T. Balzacq (2008): The changing dynamic of security in an enlarged European Union. Research paper No. 12, The changing landscape of European Liberty and Security - www.ceps.eu http://aei.pitt.edu/11457/1/1746.pdf

G. Karyotis (2011): "*The fallacy of securitizing migration: elite rationality and unintended consequences*". In: G. Lazaridis (ed.): Security, Insecurity and Migration in Europe. Ashgate, Surrey, Great Britain, pp. 13-30.
See also M. Ibrahim (2005): "The Securitization of Migration: A Racial Discourse". In: International Migration, Vol. 43 (5), pp. 163-187.

K. L. Hall (ed.) (2012): The Oxford Companion to the Supreme Court of the United States, 2nd edition, Oxford University Press, New York, 2012.

T. Owen (2004): Challenges and opportunities for defining and measuring human security, in: Human Rights, Human Security and Disarmament, disarmanet forum 2004 Vol 3. 15-24. p.16

G. Quille (2004): The European Security Strategy: A Framework for EU Security Interests? In: International Peacekeeping, Vol.11, No.3, Autumn 2004, pp.1–16
http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede20040728_ess_/sede20040728_ess_en.pdf

International Association of Privacy Professionals – IAPP (2011): Data protection authorities global survey. https://privacyassociation.org/media/pdf/knowledge_center/DPA11_Survey_final.pdf

R. Jolly and D. B. Ray (2006): "The Human Security Framework and National Human Development Reports: A Review of Experiences and Current Debates". United Nations Development Programme, National Human Development Report Unit. p. 5

Kofi Annan "Secretary-General Salutes International Workshop on Human Security in Mongolia." Two-Day. Session in Ulaanbaatar, May 8-10, 2000. Press Release SG/SM/7382. Cited from http://www.gdrc.org/sustdev/husec/Definitions.pdf

H. Nissenbaum (2010): Privacy in context – technology, policy, and the integrity of social life. Stanford University Press. Stanford, California.

B. Schneier (2006): The eternal value of privacy. In: Wired. https://www.schneier.com/essays/archives/2006/05/the_eternal_value_of.html

D. Solove (2007):'I've got nothing to hide,' and other misunderstandings of privacy. San Diego Law Review Vol. 44 p. 745- http://tehlug.org/files/solove.pdf

D. Solove (2011): Nothing to hide: the false tradeoff between privacy and security. Yale University Press. New Haven and London.

Strauß, S & J. Čas, J (2013): D 2.3 – Major security challenges, responses and their impact on privacy – selected security-oriented surveillance technologies. SurPRISE Deliverable 2.3.

F. Trauner (2011): "The internal-external security nexus: more coherence under Lisbon? European Union Institute for Security Studies Occasional paper 89, March 2011

United Nations – UN (1994): New dimensions of Human Security. Human development report 1994, United Nations Development Programme, New York, Oxford University Press.

S. D. Warren and L. D. Braneis (1890): "The Right to Privacy". In: Harvard Law Review 193 (1890) Vol. IV Dec. 15 1890, No. 5 http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm

S. Watson (2011): The 'human' as referent object? Humanitarianism as securitization. In: Security Dialogue 42(1):3-20. DOI:10.1177/0967010610393549 p. 5

World Economic Forum (2014): Global Risks 2014. Geneva, Ninth Edition. http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf

All URLs lately checked on 25 January 2015.

8 List of Figures

9 List of Tables

10 List of Abbreviations

Abbreviation	Definition
AFSJ	Area of Freedom, Security and Justice
CCTV	Closed circuit television
CSDP	The Common Security and Defence Policy
DNA	Deoxyribonucleic acid
DPA	Data protection authority
DPI	Deep Packet Inspection
EC	European Commission
ECHR	European Court of Human Rights
EDRI	European Digital Rights
EDPS	European data protection supervisor
EUCFR	Charter of Fundamental Rights of the European Union
ECHR	European Convention on Human Rights
EGE	European Group on Ethics in Science and New Technologies
EU	European Union
Eurojust	European Union's Judicial Cooperation Unit
Europol	European Union's law enforcement agency
FRA	European Union Agency for Fundamental Rights
ICO	Information Commissioner's Office
IRISS	EU project (Increasing Resilience in Surveillance Societies)
LIBE	Committee for civil liberties, justice, and home affairs
NATO	North Atlantic Treaty Organization
NGO	Non Governmental Organisation
OSCE	Organization for Security and Co-operation in Europe
SLT	Smartphone Location Tracking
SOST	Surveillance-oriented security technology
SWIFT	Society for Worldwide Interbank Financial Telecommunication
UDHR	Universal Declaration of Human Rights
UN	United Nations
UNDP	United Nations Development Program
US	United States
TEU	EU Treaty
WP29	Article 29 Working party