"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 6.1 – Citizen Summits on Privacy, Security and Surveillance: Country report Austria

Lead Beneficiary: ITA/OeAW

Author(s): Stefan Strauß (ITA/OeAW)

Due Date: June 2014

Submission Date: October 2014

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

Executive Summary

SurPRISE re-examines the relationship between security and privacy, commonly positioned as a "trade-off". Where security measures and technologies involve the collection of information about citizens, questions arise as to whether and to what extent their privacy has been infringed. This infringement of individual privacy is sometimes seen as an acceptable cost of enhanced security. Similarly, it is assumed that citizens are willing to trade off their privacy for enhanced personal security in different settings. This common understanding of the security-privacy relationship, both at state and citizen level, has informed policymakers, legislative developments and best practice guidelines concerning security developments across the EU.

However, an emergent body of work questions the validity of the security-privacy "trade-off". This work suggests that it has over-simplified how the impact of security measures on citizens is considered in current security policies and practices. Thus, the more complex issues underlying privacy concerns and public skepticism towards surveillance-oriented security technologies may not be apparent to legal and technological experts.

In response to these developments, the SurPRISE project consulted with citizens from nine[1] EU member and associated states on the question of the security-privacy "trade-off" as they evaluate different security technologies and measures.

This report presents the major results of the Austrian citizen summit as conducted on February 22 2014 in the Austrian capital of Vienna. The analysis grounds on the exploration of the empirical data gathered during the event. In accordance with the special design of the participatory process the methodological approach combines data gathered from a pre-defined survey and the outcome of three thematic group discussion rounds conducted at the summit. The aim of this participatory event was to investigate how Austrian citizens perceive the interplay between privacy, security and surveillance in relation to the employment of surveillance oriented security technology (SOST). The two SOSTs considered at the summit were smart CCTV and Deep Packet Inspection (DPI).

In order to consider potential coherences between the summit results and national peculiarities the report starts with a short review of policy relevant aspects as well as public debates about privacy, security and surveillance in the national context in section 2. This is followed by a description of the process design of the Austrian summit including the structure of the citizen panel. The main section 4 presents the major empirical results and provides deeper insights into the perceptions of citizens on privacy, security and surveillance based on the output of the survey as well as the three thematic discussion rounds conducted at each of the tables (one for each SOST and the final recommendation round). This section also includes an analysis the major suggestions and recommendations of the participants followed by a final section giving summary and conclusions about the main findings of the Austrian citizen summit.

The changing role of privacy and security on a global scale is also visible in Austria where national security policy had been adapted in order to cope with the changed requirements. As in other countries, also in Austria there is some shift in security strategies observable with an increase in pre-emptive surveillance practices and the employment of according technological means. This development amplifies tensions between privacy and security that are visible in several critical debates in the Austrian public and that reflect in the results of the summit.

The citizens expressed high concerns and worries about mass surveillance and privacy intrusion. Although there are several distinctions in the SOST-specific perceptions, concerns were very high in both cases and especially DPI which raised massive fears was strongly rejected by the vast majority. The results reveal that citizens see a number of serious threats to privacy by extensive surveillance practices aided by technology that go beyond SOST-specific concerns: a trade-off between privacy and security is not acceptable to the citizens – neither for the effectiveness of security measures nor for the protection of privacy. On the contrary they clearly demand both: effective security measures that are in accordance with an effective protection of their privacy. Instead of following a delusive line of argumentation such

[1] Austria, Denmark, Germany, Hungary, Italy, Norway, Spain, Switzerland and United Kingdom

as "those who have nothing to hide have nothing to fear", citizens highlighted that they neither want to fear security measures nor lose their privacy. This was underpinned by a number of arguments and suggestions citizens developed during the participation process. The Austrian citizens made a quite strong statement towards a revision of security foci and according measures. Citizens have a strong resistance against untargeted security practices and use of surveillance-oriented security technologies in this regard. While the majority feels quite secure in their daily life, a strikingly high amount of citizens expressed enormous concerns that privacy is heavily threatened and that the already strained relation between privacy and security aggravates further.

Despite of their high fears and concerns citizens do not neglect security measures per se but realize demand for solid approaches without undermining privacy of the general public. This was not merely expressed in a general sense but underpinned by an urgent need to reinforce effective and independent control units to scrutinize security authorities and surveillance practices that have to be in accordance with privacy and other fundamental rights. Basically, the work of police and other security authorities is perceived as very important to the Austrians. However, they observe a gap between security and surveillance competences and their appropriate implementation. In other words: surveillance measures are perceived as being too extensive and untargeted. Citizens are highly concerned about function creep and uncontrolled power due to surveillance practices and technologies. In order to alleviate this situation, citizens identified pressing demand to restrict surveillance to bring it back at an appropriate and acceptable level, i.e. more effective security measures that do not undermine privacy. In this respect, it was expressed that security authorities need to be improved in their capability to deal with contemporary security problems and to understand privacy protection. In the views of citizens this not least also needs more training and qualified security forces instead of extensive use of surveillance technologies. Citizens underlined the crucial role of data protection authorities and wish for revitalization and reinforcement of their competences and capacities.

Citizens discussed a variety of issues and elaborated several recommendations that contain a clear message to policy makers at national and European level**: less surveillance, more transparency, scrutiny of SOST usage and a general demand to foster checks and balances**. The main recommendations of the citizens are:

- Reduce and restrict surveillance technologies and practices
- More transparency of security and surveillance actions and according information
- More investment in humans not in technology
- Strengthen social coherence, civil courage and social responsibility
- Better training and education for security forces/personnel
- Enhance transparency, information and participation
- Awareness raising in the public for privacy and security
- Better integration of civil society and human rights institutions into security policy
- Fostering the role of science and research particularly as regards alternative approaches
- Reinforcement of independent data protection authorities to scrutinize security measures

Altogether the results of the Austrian citizen summit not merely shed light on the complex interplay between privacy, security and surveillance and the perceptions of citizens but provide valuable input for policy and decision making for taking appropriate action to revitalize effective privacy protection and regain the trust of citizens.

1 Introduction

Privacy, security and surveillance are among the most contested and controversial issues in society affected by technological progress. The increasing role and use of surveillance oriented security technology (SOST) for a variety of purposes is a matter of societal concern visible in a number of public discourses. Although citizens are directly affected by the security and surveillance measures employed in their countries, their views and opinions on these issues are widely unknown. To reduce this gap, based on a participatory approach the SurPRISE citizen summits explore the different perceptions of citizens about the relation between privacy, security and surveillance.

Objectives of this report

This report presents the results of the SurPRISE citizen summit conducted in Austria. To grasp the bigger picture of how perceived fears, concerns, demands and prospects are intertwined the methodological approach consists of a mix of quantitative and qualitative elements: to explore the citizens' perceptions quantitatively a survey with a set of predefined questions had been developed that also allows comparison of national differences; to get a deeper understanding of what the citizens think about the treated issues three table discussion rounds have been conducted. This combined approach provides an informed foundation for analysing the citizens' views within the scope of the SurPRISE project. The analysis grounds on an empirical investigation employing a combination of methods: i.e., a statistical evaluation of the survey results, a content analysis of the discussion outcomes as well as a review of policy documents, media and research reports.

In section 2, the report starts with a short description of the Austrian country profile and some of the main national characteristics. It is followed by an overview of the major policy issues of privacy, security and surveillance in the national context to give an impression of public discourses that are related to the topics of the Austrian citizen summit. Section 3 briefly describes the design of the participatory process, the major building blocks of the organisational setting, the basic structure of the citizen panel as recruited in Austria and some information on how the participating citizens assessed their summit. In Section 4, the major results of the large scale participatory event gathered from the quantitative survey data as well as the qualitative outcome of the different thematic group discussions and the citizens' recommendations are presented. The final section summarizes the major findings and provides concluding remarks.

2 Privacy, security and surveillance in the national context

Starting with a brief description of Austria and some general characteristics of its political-administrative system, this section provides an overview of the role and meanings of privacy, security and surveillance in Austria. To get some indications on how the interplay of these issues is shaped, also some aspects of policy and legal regulation are included.

2.1 Country profile of Austria

Austria may be characterised as a small country (population 8.4 million)[2] located in central Europe, with an alternating political history, marked by an imperial past and periods of radical breaks in democratic development. However, based on the foundation of the Second Republic after World War II, over the following decades a stable political system with successful economic development to a modern welfare state took shape. Austria is a democratic republic by constitution with a federal system of government and became an EU member state on January 1st 1995. The system of government and public administration is decentralized and shaped by the principle of federalism based on three tiers made up of federal, provincial and municipal levels (the nine federal provinces called "Länder", and 2,354 municipalities)[3]. Legislative and executive powers are divided between the National Parliament, Federal Government and the nine Provincial Parliaments and Provincial Governments. Jurisdiction is separated from executive entities by constitutional law and emanates from the federation (also provincial courts formally act as federal authorities)[4]. Above all, the public administration has to act according to the constitutional "principle of legality" which says that all actions in the sphere of official duties have to be based on legal regulation. Federal administration is headed by the federal president, governed by the federal Chancellors and organised into departments led by ministers who are monocratic organs. The Federal Chancellor cannot issue instructions to them but is formally a minister of equal rank who is also responsible for a department, the Federal Chancellery. Heading unit of the administration in the provincial states is the respective provincial government. At provincial level there are no provincial ministries or similar units but a joint bureau of the government headed by the governor of the Province. Every province is structured in municipalities.[5] At communal level the municipalities are the administrative bodies that are enabled to act widely autonomous: According to constitutional law, the municipality is a territorial authority with the right to self-government (Art. 116 B-VG)[6]. Thus, in a set of legally determined competences that are mostly or fully in the concern of the municipality (several community services such as maintenance of local infrastructure, environmental issues, etc.) it is not bound by instructions of superior bodies. Among the currently 2,354 municipalities merely 72 cities have more than 10,000 inhabitants. About 80% of the Austrian municipalities have a population below 3,000 people. This benefits a more cooperative culture among communities compared to provincial or federal level.

---

2 According to recent figures of the Statistics Austria http://www.statistik.at/web_de/statistiken/bevoelkerung/

3 http://www.statistik.at/web_de/klassifikationen/regionale_gliederungen/gemeinden/index.html

4 Since January 2014 due to a change of the constitution besides general courts competent for civil and criminal laws also administrative courts exist: one at federal level, one in each of the nine provinces and with the federal finance court a special one for financial matters. These courts can be invoked after decisions of an administrative body. The legal basis for this change is determined in the amending law of the administrative jurisdiction - "Verwaltungsgerichtsbarkeits-Novelle 2012" BGBl.I Nr. 60/2011 http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2012_I_51/BGBLA_2012_I_51.pdf

5 Austrian Federal Chancellery ("Bundeskanzleramt") (2009): Administration in Austria. http://www.bka.gv.at/DocView.axd?CobId=41629 See also H. Stolzlechner (2004): "Einführung in das öffentliche Recht", Vol. 3, Vienna, 2004.

6 Bundes-Verfassungsgesetz (B-VG) BGBl. No. 1/1930 as amended by BGBl. I No. 164/2013 http://www.jusline.at/116_B-VG.html

The Austrian political system is currently governed by a grand coalition between social democrats (SPÖ) and conservatives (ÖVP). This combination has a relatively long tradition in Austria for periods where none of these two parties achieved a majority. Between the year 2000 and 2006 this tradition was interrupted by a mid-right coalition (between conservatives ÖVP and the right-wingers FPÖ) built the government. Austria's political system has long been known to represent an ideal type of "neo-corporatism", characterised by a tradition of consensus democracy with a strong co-operation between major interest groups (Trade Union Federation, Chamber of Commerce, Chamber of Labour, Chamber of Agriculture) and the state. This system of co-operation, commonly referred to as "social partnership", is – although a voluntary arrangement – well-established in Austria's political system and political culture. At its core it is the voluntary and autonomous cooperation between the central associations representing labour and industry. The wider system of interest mediation includes these associations on the one hand, and the representatives of public policy and the political parties on the other. It is precisely the aggregate institutional, personal and functional interlock of actors and bodies in this quasi 'all-channel-network' that is considered as an essential factor for the stability of the economic and social partnership in Austria[7]. However, since the last decade this "institution" appears to lose in political weight.

2.2 Main issues of the Austrian security policy

Security policy and related strategies are somewhat coined by Austrian history and its status as a neutral country can be expected to play an important role in the positioning of Austria in international affairs and in the way security is framed. Based on the principle of perpetual neutrality ("immerwährende Neutralität")[8] grounded in the constitution, Austria does not intervene in military conflicts or participate in military alliances. The national army mainly serves purposes of civil protection and humanitarian support in national and international issues. Since Austria became a member of the European Union in 1995, its status as neutral country is somewhat stressed as Austria is also a part of the Union and thus to some extent involved in EU's foreign affairs and security policy. In this regard, there is a shift from neutrality towards solidarity observable. This shift also entails partially different foci on national security objectives and strategies to fulfill them. This was not least the case in the enactment of the Austrian security- and defense doctrine in 2001[9] that brought several changes in the framing of security. Against the background of a paradigm shift in European security policy after the cold war with increasing complexity of threats the doctrine explicitly highlighted that "the evolution of the EU and of NATO in terms of security policy will specifically be of vital significance"[10] for the future of Europe. Hence, there was a sharpened focus on comprehensive and co-operative security. Instead of defining security and its different conceptualizations, the doctrine claimed that "security in all its dimensions is the basic prerequisite for the existence and the functioning of a democracy under the rule of law as well as for the economic welfare of the community and its citizens"[11]. Although the doctrine underlined the solid an positive security situation of Austria without any concerning development the document argues that as a political task of every state, security policy had to be realized as holistic concept as "risks and dangers replace threat scenarios"[12]. Entailed was an emphasis on pre-emptive measures to already prevent the emergence of threats.

The path entered with the doctrine and its basic security framing had been partially carried forward also in the ensuing new security strategy that the Austrian government presented in 2011 and resolved in 2013. As the conditions for security in Austria have significantly changed further in the last decade according to the federal government, policy makers decided to adapt the security doctrine to the

---

7 E. Tálos, and B. Kittel, (2002): Austria in the 1990s: The Routine of Social Partnership in Question?, in: Berger, S. and Compston, H. (Eds): Policy Concertation and Social Partnership in Western Europe. Lessons for the 21st Century, New York, Oxford: Berghahn Books, pp. 35-50.

8 Neutrality is a core principle of Austrian policy and politics. It was declared on October 26 1955 and is legally defined by Austrian constitutional law.

9 Austrian Parliament (2001): *Security and Defence Doctrine*, Resolution by the Austrian Parliament, December 2001 http://www.bka.gv.at/DocView.axd?CobId=3604

10 Ibid p. 2

11 Ibid p. 1

12 Ibid p. 3

altered requirements and to steer towards a comprehensive, holistic security strategy[13]. General objectives of the strategy inter alia include the comprehensive protection of the Austrian population, ensuring territorial integrity of the republic, protection of the constitutional order and its fundamental rights, strengthening of the common good, preservation of social peace, securing vital resources and the environment, fostering resilience in the public and private sector, extension of civil and military capacities, strengthening the European area of freedom, security and justice, combating terrorism and organized crime, reducing of illegal migration, supporting crisis management, disarmament and prevention of weapons of mass destruction, participation in development cooperation, supporting security awareness, etc. These general objectives are addressed by different internal and external security activities. Strongly linked to a comprehensive security framing is a changing focus of security and law enforcement authorities towards more pre-emptive state mechanisms which is also visible in Austria in a variety of ways: "new preventive measures" is an explicit objective for internal security; The strategy perceives security policy as a "cross-cutting issue which has to be taken into account in almost every sphere of life and policy"[14]. In this regard the Austrian strategy mirrors the global shift in security policy carried forward by securitization towards a holistic framing of security spanning across a variety of different domains to cope with the challenges given by transformations in global security policy and technological progress[15]. A certain role of technology shows inter alia in some parts of the internal security objectives, e.g., an effective tackling of crime with a need for more flexible strategies also to deal with new forms of computer and economic crime; or the objective of "utilising and protecting data"[16] that refers to technical progress and new approaches to use technologies and digital data for fighting crime. Here, also the increasing importance of data protection due to increasing digitization is mentioned. To address the uncertain challenges as regards cybercrime and security of IT systems Austria created a working group for ICT security and developed a specific ICT security strategy[17]. Since 2008, the Federal Chancellery established a Computer Emergency Response Team (CERT). The CERT is responsible for cyber security issues and corresponding efforts such as coordination between public and private sectors[18].

While the former national security strategy inter alia highlighted the role of more narrow cooperation with the NATO (towards a potential joining and away from neutrality) this is somewhat relativized now. The current strategy puts more emphasis on the United Nations and its function for peacekeeping as well as on the OECD and its role as "multidimensional security organization"[19]. Overall, a reinforcement of national and international co-operations plays a prominent role in the strategy: explicitly mentioned is a strengthening of internal security authorities, especially the police, to perform national and international operations as well as co-operations between civil and military forces and agreements for international data exchange. The intended enhancement of internal security authorities also includes "the provision of a sufficient number of suitable, adequately trained police officers, judges, prosecutors and other experts for the purpose of participating in international crisis management operations"[20]. While the reinforcement of cooperative approaches aims to address increasing global security challenges to some extent they also imply a gradual conflation of internal and external security (especially regarding military-police cooperation) which is visible on a European level as well. This mix up and the strong framing of security as a comprehensive concept had been inter alia criticized by the Austrian research center for peace and conflict resolution (ÖSFK): due to the use of different and

[13] Austrian Federal Chancellery (2014): The Austrian security strategy. Security in a new decade – Shaping security http://www.bka.gv.at/DocView.axd?CobId=52251
[14] Ibid p. 4
[15] S. Strauß, J. Čas, (2013): D 2.3 – Major security challenges, responses and their impact on privacy – selected security-oriented surveillance technologies. SurPRISE Deliverable 2.3
[16] Austrian Federal Chancellery (2014) op. cit. p. 11
[17] Austrian Federal Chancellery (2012): National ICT strategy Austria. http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=48411
[18] G. Jandl (2012): The challenges of cyber security – a government's perspective http://www.etc-graz.at/typo3/fileadmin/user_upload/ETC-Hauptseite/human_security/hs-perspectives/pdffiles/issue1_2012/6-HSP12_Jandl__FINAL_.pdf
[19] Austrian Federal Chancellery (2014) op. cit. p. 15
[20] Ibid p. 11

sometimes even conflicting terms and concepts of security (such as a mix up between the concept of human security and state-centered security) the strategy document remained open for political opportunism. The strategy's focus towards a comprehensive/holistic security entails the threat of totalizing security policy resulting in surveillance state. A further point of critique was the lacking incorporation of Austria's neutrality. The ÖSFK also advised that instead of upholding state-military paradigms and framing security as a holistic concept, conflict management with peaceful methods should build the guiding principle for a peace-oriented security policy embracing human security as main concept[21].

General Security concerns of Austrians

In 2011 a special Eurobarometer survey[22] explored some of the most important security challenges in the view of European citizens. The table below shows the results for Austria:

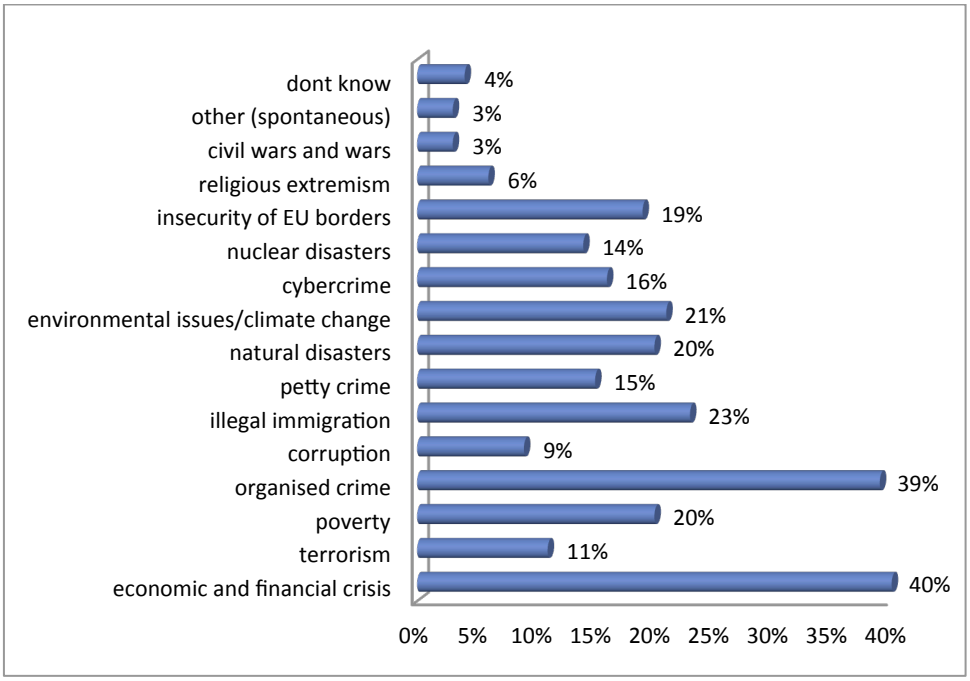


Figure 1: Most important security challenges for Austrians[23]

With 40%, financial and economic crisis is perceived as the highest threat, followed by organized crime (39%). Apart from illegal immigration (23%) Austrian citizens also perceive issues linked to nature and environment (climate change 21%, natural disasters 20%) as very challenging. Terrorism which is extensively used as major argument to foster security plays a minor role with 11%. Furthermore, 63% of the Austrians are convinced that their country does enough to combat terrorism. 59% share the same opinion as regards fighting organized crime[24].

---

21 Austrian research center for peace and conflict resolution (Österreichisches Studienzentrum für Frieden und Konfliktlösung – ÖSFK) (2011): Stellungnahme zum Entwurf „Österreichische Sicherheitsstrategie. Sicherheit in einer neuen Dekade – Sicherheit gestalten". http://www.uni-klu.ac.at/frieden/downloads/Stellungnahme_sicherheitspolitische_Strategie_Bundesregierung.pdf

22 European Commission (2011): Special Eurobarometer 371 on internal security. http://ec.europa.eu/public_opinion/archives/ebs/ebs_371_en.pdf

23 Question: What do you think are the most important challenges to the security of Austrian citizens at the moment?

24 Ibid pp. 66

According to special Eurobarometer on civic protection from 2012[25], the majority of Austrians is not concerned about terrorist attacks (54% say they are not concerned, 32% stated to be fairly concerned). A national survey of 2014 comes to similar results: compared to 2011, the amount of those who are *not concerned at all* about terrorist attacks increased from 28% (in 2011) to 54% (in 2014)[26]. The high importance of economic challenges as shown in the Eurobarometer results of 2011 are also confirmed in this national survey: The Austrian population is most concerned about the increasing gap between the rich and the poor (44% highly worried, 44% somewhat worried).[27]

2.3 Major Privacy issues

Austria was among the first countries that created a discrete legal framework for data protection which exists since more than 30 years as a central part of Austrian legislation. The first privacy law was created in 1978. As in most other European countries, key changes were made during the end of the 1990ies due to the European Data Protection Directive 95/46/EG[28]. Based on these changes, Austria created a new Data Protection Act which is effective since the year 2000. The act also regulates the tasks and competences of the national data protection authority (DPA). The DPA has been reorganized as a consequence of the laws' amendment in 2013. Before this, the data protection commission (DPC) represented the authorities' main body. Formally, the DPC was an independent authority but also a formal part of the Federal Chancellery. This circumstance was heavily debated by legal and privacy experts who doubted the DPCs independence from government and assumed insufficient accordance with European law. As a consequence, the EU-commission initiated a lawsuit against Austria as regards lacking independence of the DPC. In October 2012, the European Court of Justice agreed with the critics and came to the decision that the functional independence of Austria's DPC alone is not sufficient to protect it from external influence. In Reaction to the Court decision, the Austrian privacy law was enacted in 2013 including reorganization of the DPC.

The situation regarding privacy awareness in Austria is ambivalent. Though the country is deemed as being relatively privacy aware compared to other EU countries, experts locate a lack of information in the public for privacy relevant issues and a variety of controversial aspects as regards handling of personal data by public and private authorities. Several years before Edward Snowden uncovered the global mass surveillance activities of NSA and other intelligence agencies, in a representative study the Austrians made clear to perceive privacy as important (over 90% agreed). 68% of the respondents had the impression that public authorities tend to extensively collect data about citizens; 77% assessed themselves as little informed about privacy issues. 76% claimed that Austrians are not sufficiently informed about privacy, risks of abuse and legal aspects[29]. In a ranking of Privacy International in 2007[30], Austria received rank 17 out of (at this time) 27 EU member states in the category "systemic failure to uphold safeguards". Main reasons mentioned were increasing video surveillance and collection and storage of personal data in registers. Particularly mentioned was the leading role of Austria together with Germany regarding data exchange of fingerprint and DNA-databases. Further, also the lawsuit about lacking independence of the Austrian DPA (as mentioned above) was considered in the ranking[31].

A problematic aspect in Austria was and still is the low personal resources of the DPA. Compared to other European countries, the Austrian DPA is considerably understaffed (e.g. Belgium has 37 persons,

---

25 European Commission (2012): Special Eurobarometer 383 on civil protection http://ec.europa.eu/public_opinion/archives/ebs/ebs_383_en.pdf

26 C. Seidl (2014): "Immer weniger Österreicher fürchten Terroranschläge". Der Standard Online Jan 1 2014 http://derstandard.at/1388514309607/Immer-weniger-Oesterreicher-fuerchten-Terroranschlaege

27 C. Seidl (2014): op. cit.

28 European Parliament and the Council of Europe (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 http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

29 K. Allwinger, J. Schillhab, (2008): *Vertrauen der ÖsterreicherInnen in den Datenschutz*, Baden: Oekonsult Communication & Consulting ges.m.b.h. http://www.oekonsult.eu/datensicherheit2008.pdf

30 E. Möchel (2012): "Datenschutz: Österreich stürzt ab", ORF Futurezone, December 30 2012 http://www.fuzo-archiv.at/artikel/246261v2

31 Privacy International (2007): Surveillance Monitor 2007 – International country rankings, https://www.privacyinternational.org/reports/surveillance-monitor-2007-international-country-rankings

Austria 20). In a report of the data protection commission from 2007, Austria was among those countries with the lowest staff - on rank 27 of 31. The lack of personal resources and the need for additional personnel has been criticized by the DPA for many years However, this situation did not improve although the data protection authority repeatedly argued for more resources to be able to fulfill its tasks. Since 2000, the number of six members and six substitute members working for the institution did not change. With the enactment of the data protection law, members were obliged to fulfill their functions only besides their regular occupation. With about 22 permanent employees in total, the DPA's personal resources did not change significantly over the years. In its annual report for the year 2013, the DPA raised this issue again and argued that also technological change as well as stronger focus on legal regulations for security authorities entailed significant extensions to its field of duties. Also the reorganization in 2013 so far did not lead to an improvement of resources[32].

Legal aspects

Privacy in Austria is legally defined in the Data Protection Act ("Datenschutzgesetz – DSG 2000"[33]) as a fundamental right at constitutional status. "Everyone, especially also in respect of safeguarding his private- and family life, is entitled to nondisclosure of personal data (…)" (§ 1 DSG 2000). From this fundamental right, further rights are derived: Besides the right to nondisclosure, everyone has the right to know which personal data is processed by whom for which purpose, the right to rectification and deletion of his/her personal data. The right to privacy can be limited according to a reservation of statutory powers ("Gesetzesvorbehalt") but limitations are only allowed on a legal basis and to protect the general public (§1 (2) DSG 2000). As in other privacy regulations, also the Austrian privacy law determines essential privacy principles such as necessity of data processing, purpose limitation, transparency, data reduction, etc. and the need to consider commensurability in order to avoid privacy infringement. The legal framework explicitly refers to the European Convention on Human Rights (ECHR) in particular Article 8 (2): "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[34]

A peculiarity of the Austrian privacy framework is the distinction between personal, indirectly personal and sensible data (§ 4 DSG 2000): *Personal data* is defined as information relating to data subjects who are identified or identifiable. Data are understood as *indirectly personal*, if the data refer to a person in such a manner that the identity of this person cannot be ascertained by legal means. Sensible data concern information demanding special protection such as racial or ethnic origin, political opinion, trade-union membership, religious or philosophical beliefs, and data concerning health or sex life.

The data protection act defines two main control units: the data protection authority (DPA, formerly the data protection commission - DPC) and the data protection council which is a political advisory board that counsels the DPA. The data protection authority is the major control unit to ensure that personal data is processed in accordance with the legal regulations. The DPA is the focal point for persons concerned of privacy abuse and handles according complaints. Besides dealing with formal complaints the DPA also provides an ombudsman-procedure which aims at mediating between the concerned person and the data controller. In case of justified suspicion of abuse against the provisions of the data protection law, the DPA can also verify data applications.

For electronic processing of data the law uses the term "information network system" ("Informationsverbundsystem") defined as the joint processing of data in an application by several parties as well as usage in a way that every party also has access to data provided by the others (§ 4 N13 DSG 2000). For the examination of the legitimacy of data applications the DPA administrates the so-called data processing register (DPR) which is accessible to the public. In general every person or

[32] Austrian Data Protection Commission (2014): Annual report 2012/2013, Vienna 2014. http://www.dsb.gv.at/DocView.axd?CobId=55304

[33] Federal Act concerning the Protection of Personal Data (DSG 2000) BGBl. No. 165/1999, as amended by BGBl. I No. 135/2009 http://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.pdf

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

institution is obliged to register information systems that process personal data at the DPR before operation. This aims at providing transparency and verifiability regarding lawful operation of institutions that process personal data. Typical data applications that have to be registered in the DPR are information systems, databases and CCTV systems. However, there also some exceptions from this registration defined in the law, e.g. CCTV registration is not mandatory in case of real-time observation without data storage or an analogue storage device (§ 50 DSG 2000). In case of violations against the mandatory registration financial penalties up to Euro 10,000 are designated.

In addition to the federal privacy law there are also laws in the nine different provincial states. For regulating concrete aspects about handling and processing personal data there are several other legal regulations such as national decrees (e.g. Data processing register decree, privacy appropriateness decree, etc.)[35] Several sector-based laws also address privacy relevant issues, e.g. the Telecommunications Act (Telekommunikationsgesetz – TKG)[36] that inter alia includes regulation about the confidentiality of communications and data protection. The law contains several data protection provisions regarding technical communication services. The TKG also played an important role regarding the Austrian implementation of the European Data Retention Directive.

The use of personal data by security authorities is inter alia regulated in the Security Police Act (Sicherheitspolizeigesetz – SPG)[37]; especially in part four, which refers to the data protection act and highlights the principle of commensurability (§ 51 SPG). In line with the DSGs reservation of statutory powers the SPG allows usage of personal data if security authorities need this data to fulfil their tasks under some justified reason. It also regulates data transmission whereby the data protection act does not apply (§ 56 SPG). The SPG partially overlaps with code of criminal procedure (Strafprozessordnung – StPO)[38] which regulates the prosecution of suspicious persons under order of courts or prosecution.

2.4 Public discourse on surveillance-oriented security technologies and related practices

The following section contains a brief overview of selected controversies about SOSTs and related practices in Austria. It briefly describes some legal and applied issues that significantly changed practices of security authorities as regards new (pre-emptive) modes of law enforcement and related support by new technologies.

2.4.1 Changing security practices and regulations

Since 2001, Austria successively expanded the competences of security authorities regarding surveillance and related activity with impact on individual privacy. The Security Police Act plays a crucial role in this regard. It was amended several times and each time extended the competences regarding the deployment of SOSTS in Austria. Since 2005, the use of CCTV was widened to neuralgic areas that can be defined by security authorities. The law also paved the way for the extension of CCTV in public transport such as in metro wagons. During a night meeting in 2007 at the parliament, the two governing parties made a variety of enactments, inter alia also of the SPG, with new regulations allowing police forces the use of IMSI-catchers and other technologies for eavesdropping communication and surveillance without judicial order ("richterlichen Beschluss"). Changes also obliged providers to reveal the identity of internet users to the police if requested. The amendment raised many concerns and constitutional complaints by several companies such as telecom-providers and private individuals.

---

[35] For an overview of Data Protection Decrees ("Verordnungen zum Datenschutzrecht") in Austria see https://www.dsb.gv.at/site/6201/default.aspx

[36] Telecommunications Act 2003 ("Telekommunikationsgesetz") BGBl. I Nr. 70/2003, as amended by BGBl. I No. 44/2014 http://www.jusline.at/Telekommunikationsgesetz_%28TKG%29.html

[37] Security Police Act ("Sicherheitspolizeigesetz") BGBl. No. 566/1991, as amended by BGBl. No. BGBl. I Nr. 44/2014 http://www.jusline.at/Sicherheitspolizeigesetz_%28SPG%29.html

[38] Code of Criminal Procedure ("Strafprozessordnung") BGBl. No. 631/1975, as amended by BGBl. I No. 71/2014 http://www.jusline.at/Strafprozessordnung_%28StPO%29.html

Also the federal data protection law has undergone several amendments that are related to changing security practices. Especially relevant is the 2010 amendment[39] that facilitated the operation of CCTV systems: before the amendment, data gathered by CCTV had to be treated like any other personal data including registration and request for implementation of the camera system at the data protection commission. Since 2010, the requirements for operating CCTV are reduced as information to the DPC is not necessary e.g. if surveillance footage is not recorded or stored on an analogue medium and deleted within 72 hours.

The Data Protection Act also includes the individual right to information about personal data processing which is essential for transparency. However, in Austria there are some barriers for individuals to exercise this right. A recent comparative study about the transparency of data controllers' practices in Europe identified several problems[40]. A precondition for the right to information is to locate the data controller. In 25% of the analysed cases in Austria, this did not succeed. Furthermore, also in successful cases the outcome of the responses given by data controllers was relatively low and sometimes inadequate. This was especially the case as regards companies but to some extent there was also room for improvement among public authorities identified in order to foster the right to information. According to the Austrian study this is a further indicator for an increasing imbalance in power[41]. To improve the right to information and transparency, for already several years a national initiative[42] presses for the creation of a national law for transparency and freedom of information similar to other countries (such as in Canada, Germany, Netherlands, Ireland, Sweden, UK, US, etc.). The long lasting tradition of official secrecy and the according Official Secrecy Act ("Amtsverschwiegenheitsgesetz") is a great burden for fostering freedom of information in Austria.

In 2011, the Security Police Act was enacted again as part of the so-called "anti-terror package" leading to an extension of competences for police forces to apply surveillance activities. Since then, authorities are enabled in the pre-emptive observation of individual suspects ("erweiterte Gefahrenforschung"); and the SPG now also allows the use of tracking devices to detect the location of an individual and in case also of accompanying persons (also without juridical order). Once again, these changes were strongly criticized by legal experts, judges, privacy advocates, journalists and NGOs as a dangerous step towards surveillance state[43].

A further controversial issue is the amendment of the criminal code ("Strafgesetzbuch –StGB"). As a consequence of 9/11, in 2002, new regulations were introduced to fight organized crime and terrorism. The introduction of the so-called "terror-paragraph" (§ 278 StgB) raised a larger public debate. The debate was triggered in 2010, as a group of animal rights activists had been imprisoned for over 2 years on the legal basis of the new section. The charge was initiated by a private company that accused some activists of damaging their property. During investigation, law enforcement conducted eavesdropping operations by wiretapping phone calls, location tracking, video surveillance and online investigation. The prosecution accused the activists to be a terror-organization. After 2 years of investigative custody, the activists were finally acquitted of all charges. In the proclamation of sentence, the judge made a

---

39 Austrian Parliament (2009): Bundesgesetz, mit dem das Datenschutzgesetz 2000 und das Sicherheitspolizeigesetz geändert werden (DSG-Novelle 2010), Bgbl. I N0. 133/2009 http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=BgblAuth&Dokumentnummer=BGBLA_2009_I_133

40 A. Galetta, P. de Hert, X. L'Hoiry, C. Norris (2014): Mapping the Legal and Administrative Frameworks of Access Rights in Europe – A Cross-European Comparative Analysis. D5.1 of the IRISS project http://irissproject.eu/wp-content/uploads/2014/06/IRISS-WP5-Summary-Meta-Analyses-for-Press-Release.pdf

41 J. Sterbik-Lamina, S. Birngruber (2014): Austria Country reports. In: Deliverable D5 of the IRISS project: Exercising democratic rights under surveillance regimes. Increasing resilience in surveillance societies (IRISS).

42 http://www.transparenzgesetz.at/

43 Austrian Parliament (2011): "Begutachtungsverfahren Ministerialentwurf betreffend ein Bundesgesetz, mit dem das Sicherheitspolizeigesetz, das Polizeikooperationsgesetz und das Bundesgesetz über die Einrichtung und Organisation des Bundesamtes zur Korruptionsprävention und Korruptionsbekämpfung geändert werden" http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00313/index.shtml See also APA/Futurezone November 15 2011 http://futurezone.at/netzpolitik/5931-ministerrat-beschliesst-sicherheitspolizeigesetz.php

point about the highly controversial legal foundations of the process and the questionable approach of police forces. Highly controversial was inter alia the installation of an undercover investigator among the animal rights group. The process gained some high medial and political interest. The process as a whole and the controversial legal regulation in particular has been highly criticized by a number of experts as imprecise, excessive and a dangerous weapon which is alarming in a constitutional democracy[44]. After the process ended, members of the National Council urged a re-evaluation of the contested section[45]. Beside the investigation on animal rights activists further cases went public: in 2011 a group of students was observed and suspected of being a criminal organization based on § 278 StgB as they filmed the deportation of an African immigrant by police at the Vienna airport[46]. The students were arrested for several weeks. The case revealed that police investigated a student protest movement.

Both debates exemplify the increase in pre-emptive state mechanisms. Linked to those new legal options is the creation of new possibilities for law enforcement to make use of new technologies and to apply surveillance technologies, e.g. IMSI[47]-catcher to observe and intercept mobile communications. In case of the "terror-paragraph" a variety of SOSTs were used: eavesdropping, location tracking, IMSI-catcher, CCTV and online investigation. Starting in 2007 (and increasing reports in 2010, 2011) initiated by the German situation, there was a public debate about online investigation and the use of government spyware the so-called "Bundestrojaner", i.e. the use of Trojan horses and other hidden SOSTs by security authorities for tracing computer usage, online activity and investigation on personal computers[48]. While in Germany, public awareness was raised by the Chaos Computer Club revealing several flaws of the German software pointing to wider application contexts than legally intended, there were only few media reports in Austria, although similar surveillance activity was already in use. In 2008 it came out that Austrian investigators used key-loggers to observe an Islamic person who was accused of propagating a "threat video" and invoking terror activity. Legal experts were divided over the legal basis for this investigation.[49] This case gained some public attention.

[44] N. Flori (2011): '„Gefährliche Waffe": Paragraph 278a' Wiener Zeitung February 11 2011, http://www.wienerzeitung.at/nachrichten/oesterreich/politik/28903_Gefaehrliche-Waffe-Paragraf-278a.html

[45] https://de.wikipedia.org/wiki/Wiener_Neust%C3%A4dter_Tiersch%C3%BCtzerprozess

[46] E. Linsinger (2011): „Enormes Sicherheitsrisiko", Profil Online February 12 2011 http://www.profil.at/articles/1106/560/288752/enormes-sicherheitsrisiko

[47] International Mobile Subscriber Identity

[48] https://de.wikipedia.org/wiki/Online-Durchsuchung_%28Deutschland%29

[49] Der Standard Online (2011): '"Bundestrojaner" in Österreich nicht erlaubt aber im Einsatz?"', October 10 2011 http://derstandard.at/1317019787787/Bundestrojaner-in-Oesterreich-nicht-erlaubt-aber-im-Einsatz

2.4.2 Digital profiling and surveillance - overview

The NSA scandal caused massive shocks on a global scale. In Austria media uncovered that the NSA operates a surveillance control quarter in Vienna, where according to media reports a so called special collection service monitors the telecommunications traffic in cooperation with the CIA[50]. The US embassy in Vienna declared that this unit is not a secret intercept station but only gathers publicly available data and will be closed within the next years, whereas this decision is not related to the public debate[51]. Shortly afterwards the Snowden files revealed information about countries involved in the surveillance activities of US intelligence rumours started about cooperations between Austrian intelligence services and the NSA. Investigations of the prosecution to examine this case were prematurely cancelled[52]. After a visit from an Austrian government delegation in Washington representatives of the Austrian governing parties declared that cooperation with the NSA is "indeed important" but this should not lead to surveillance in an Orwellian sense[53]. According to the recent report of the federal office for the protection of the constitution ("Verfassungsschutz", Austria's main inner intelligence service) Austria plays a certain role for international intelligence agencies: due to the large amount of international organisations the number of "classical agents" in Vienna is surpassingly higher. The report also detects a paradigm shift in the work of intelligence agencies in which activities intrude the privacy of ordinary people and semi-private or private security companies are involved in data gathering and transfer[54].

Austria has a long tradition in collecting personal data for police work. The number of data collections continuously grew over time with an increasing number of databases, registers and person records. While the different databases are separated, security authorities have options to aggregate data for law enforcement. Also the registration of residents which is mandatory in Austria is inter alia used for law enforcement. Registration exists already since 19th century and in its origins had the primary aim to observe movements of suspicious persons. Over time it had been adapted and now serves a variety of purposes in the public administration. In 2001/02, due to the population census in 2001, national registration became centralized with the creation of the central register of residents (CRR)[55]. The CRR is administrated by a special unit of the Ministry of the Interior and contains data of all persons registered in Austria (citizens as well as foreign visitors). The CRR is also used for purposes of national security. The legal framework for the registration allows data matching between CRR and other databases e.g. for profiling, manhunt and other security purposes[56]. Already in 1997, Austria created a legal basis for dragnet investigation ("Rasterfahndung"), i.e. the aggregation of data and information on suspects. Main reason for the law was the so-called "letter bomb assassinator" Franz Fuchs who sent letters with explosives to politicians and prominent individuals[57]. Since 2001, the number of data collections and databases for security authorities has been further extended and a variety of databases and electronic

---

50 Der Standard Online (2013): '"NSA Villa" - Pilz: USA greifen auf Österreichs Luftraumüberwachung zu', November 15 2013 http://derstandard.at/1381372194814/NSA-Villa---Pilz-USA-greifen-Oesterreichs-Luftraumueberwachung-zu

51 Der Standard Online (2013): '"NSA Villa' in Wien wird geschlossen', September 10 2013 http://derstandard.at/1378248644840/NSA-Villa-in-Wien-wird-geschlossen

52 F. Schmid (2014a): "Staatsanwaltschaft bricht Ermittlungen zur NSA-Affäre ab", Der Standard Online Mai 28 2014 http://derstandard.at/2000001627044/Staatsanwaltschaft-bricht-Ermittlungen-zur-NSA-Affaere-ab

53 F. Schmid (2014b): 'Kooperation mit NSA laut Regierungsparteien „durchaus wichtig"', Der Standard Online Juni 20 2014 http://derstandard.at/2000002176643/Nach-Besuch-in-USA-Kooperation-mit-NSA-laut-Regierungsparteien-durchaus

54 F. Schmid (2014c): 'Verfassungsschutz: "NSA könnte zum Nachteil Österreichs agieren"' Der Standard Online Juni 25 2014 http://derstandard.at/2000002298526/Verfassungsschutz-NSA-koennte-zum-Nachteil-Oesterreichs-agieren

55 Cf. G. Aichholzer, S. Strauß (2010): The Austrian case: multi-card concept and the relationship between citizen ID and social security cards. In: Identity in the Information Society (IDIS) (2010) 3: pp. 65–85.

56 As defined in the registration act („Meldegesetz" - MeldeG), particularily in § 16a MeldeG. "Bundesgesetz über das polizeiliche Meldewesen (Meldegesetz 1991 - MeldeG) BGBl. No. 9/1992, as amended by BGBl. I No. 161/2013 https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10005799

57 Der Standard Online (2007) "Hintergrund: Überwachung in Österreich", December 6 2007 http://derstandard.at/3078169

registers for law enforcement is in use.[58] Although the database-systems are separated and not per se interlinked, law enforcement can access the data. A central tool in this regard is the police database-system EKIS (electronic criminal police information system) - a sort of meta-system that supports police authorities in data mining and profiling activities. EKIS is a powerful instrument as it grants security authorities access to a variety of data collections and registers such as different investigation records on persons, objects and cultural artifacts, person information records, motor vehicle registers, fingerprint- and DNA-databases etc.[59] In 2000 a police scandal went public where EKIS played a key role: the system was illegally accessed to spy on artists and activists that are critical against the right-wing party FPÖ[60]. In 2010, a local politician was sentenced for illegal access to EKIS[61]. Privacy advocates reported other cases of illegal access and demand for several years to sharpen control of EKIS to prevent illegal access and abuse[62]. Also the police labor union had concerns about insufficient protection from unauthorized or unqualified access to the system[63].

Data retention - DR ("Vorratsdatenspeicherung")

Since April 2012, Austrian internet- and telecom providers are obliged to implement the data retention based on the European Directive from 2006[64] and keep records on phone calls and internet connections. The introduction of data retention and the creation of the related legal basis by the amendment of the Telecommunications Act triggered an enormous public debate. The high awareness and relevance of the issue is inter alia visible in the high number of critical statements (over 180) on the parliament's website[65] already before the amendment of the corresponding law. A broad scope of actors and concerned individuals ranging from privacy, legal and technical experts, public and private institutions, civil society actors as well as individual citizens commented on the issue and contributed to the debate to convince the government about the democratic threats of data retention and skip its implementation. Similar to the situation in Germany, NGOs emerged and the so-called "Arbeitskreis Vorratsdatenspeicherung (AK Vorrat)"[66] became the primary civil society actor in organizing actions against the pre-storage of ICT data. Due to the increasing public resistance, Austrian policy-makers stated to be aware of the threats and that government will strive for a solution in accordance with fundamental rights. To underline the point, government involved fundamental rights experts into the legislative process. However, also the involved experts left no doubt about the massive impact on privacy, democratic core values and lacking accordance with fundamental civic rights. A variety of demonstrations in Austrian cities took place several times to take a stand for freedom and against surveillance and citizens intensified their protests against further restrictions to their right to privacy[67]. Despite of the heavy protests, the DR was implemented and executed.

---

58 http://www.facts.biz.ly/Dateien.html

59 Ministry of the Interior: "Informationen zum EKIS" http://www.bmi.gv.at/cms/BMI_Datenschutz/ekis/start.aspx

60 A. Medosch (2000): "Grundrechtlicher Super-GAU in Österreich kontaminiert die EU". Telepolis October 25 2000 http://www.heise.de/tp/artikel/8/8992/1.html
DiePresse.com (2009): "EKIS: Polizeisystem mit Spitzel-Vergangenheit", February 17 2009 http://diepresse.com/home/panorama/oesterreich/453338/EKIS_Polizeisystem-mit-SpitzelVergangenheit

61 DiePresse.com (2010): "Amtsmissbrauch: Steirischer Polizist verurteilt", March 2 2010 http://diepresse.com/home/panorama/oesterreich/543599/Amtsmissbrauch_Steirischer-Polizist-verurteilt

62 ARGE Daten (2005): '"Wer ein Fremder ist, bestimme ich!" - Fremdenrechtspaket im Datenschutzrat' http://www2.argedaten.at/php/cms_monitor.php?question=PUB-TEXT-ARGEDATEN&search=84404ctc

63 Der Standard Online (2009): "Gewerkschaft hat Sicherheitsbedenken", September 6 2009, http://derstandard.at/1252036691580/Postler-zur-Polizei-Gewerkschaft-hat-Sicherheitsbedenken

64 https://en.wikipedia.org/wiki/Data_Retention_Directive

65 Virtuelles Datenschutzbüro (2010): "Österreich: Rekordzahl von Stellungnahmen zur Vorratsdatenspeicherung" http://www.datenschutz.de/news/detail/?nid=4083 ; Austrian Parliament (2011):"Ministerialentwurf betreffend ein Bundesgesetz, mit dem das Telekommunikationsgesetz 2003, das KommAustria-Gesetz sowie das Verbraucherbehörden-Kooperationsgesetz geändert werden" http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00269/index.shtml

66 http://akvorrat.at/

67 B. Wimmer (2012): "Mehr als 80.000 Bürger protestieren", Futurezone March 31 2012 http://futurezone.at/netzpolitik/8271-vorratsdaten-mehr-als-80-000-buerger-protestieren.php

In 2011, a citizen initiative received high attention in the public: over 100,000 concerned individuals signed a petition against data retention[68]. The petition urged the Austrian government to take public concerns seriously by taking a stand on stopping the introduction of the DR not merely in Austria but at EU level and to evaluate existing anti-terror laws to ensure accordance with fundamental rights and citizens' privacy. Parallel to the initiative, NGOs and legal experts brought in a constitutional complaint ("Verfassungsbeschwerde") against the DR in Austria with over 10,000 signatories and a variety of citizens sued the republic for their right to privacy. The Austrian Constitutional Court finally validated the lawsuits in autumn 2012[69]. In reaction to the constitutional complaints at national level the Austrian Constitutional Court (and the High Court of Ireland) asked the European Court of Justice to investigate the Data Retention Directive's validity. In April 2014, the EU Court of Justice finished its examination and declared the Data Retention Directive as invalid as it affects the fundamental rights in a non-appropriate way. In its decision the court underlined the "wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, without that interference being limited to what is strictly necessary"[70]. European countries now have to revise their national implementation of the Directive. Experts in Austria expected the national law to be eliminated. This assessment is fed with recent figures of 2013 revealing that the data gathered by data retention was not used for its original purpose to combat organized crime and terrorism but for theft, drug abuse, stalking and petty crimes[71]. These figures clearly point towards function creep which has been among the main arguments against data retention also in the judgment of the European Court. As a consequence to the Court decision, data retention in Austria was abandoned on June 27 2014[72]. According to assessments of legal experts, data of telephone calls are still available for the duration of three months because providers store the data within this period. Law enforcement can use this data based on judicial order[73].

---

68 http://www.parlament.gv.at/PAKT/VHG/XXIV/BI/BI_00037/index.shtml?forceShow=true#tab-Uebersicht

69 Der Standard Online (2012): "Verfassungsgericht prüft Vorratsdatenspeicherung", September 21 2012 http://derstandard.at/1347493199974/Verfassungsgericht-prueft-Vorratsdatenspeicherung

70 CJEU – Court of Justice of the European Union (2014): "The Court of Justice declares the Data Retention Directive to be invalid", PRESS RELEASE No 54/14, Luxembourg, 8 April 2014. http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

71 B. Wimmer (2014): "Österreichische Vorratsdaten für Diebstahl und Drogen", Futurezone June 11 2014 http://futurezone.at/netzpolitik/oesterreichische-vorratsdaten-fuer-diebstahl-und-drogen/69.898.233

72 F. Schmid, M. Sulzbacher (2014): "VfGH kippt Vorratsdatenspeicherung", Der Standard Online June 27 2014 http://derstandard.at/2000002350932/Verfassungsgerichtshof-kippt-Vorratsdatenspeicherung http://orf.at/stories/2235721/2235722/

73 ORF (2014): "Vorratsdatenspeicherung: Ein Rest bleibt", June 28 2014 http://oe1.orf.at/artikel/380566

3 Process design – the citizen summit in Austria

3.1 Organisational setting

The Austrian citizen summit took place on February 22 2014 in the Austrian capital Vienna in the "Aula der Wissenschaften" (hall of sciences). Located in the city centre, the venue was easy to reach with public transportation and also accessible for people with impairments. The venue was arranged for 240 persons with eight persons at each of the 30 tables. To ensure that the planned capacity meets the factual amount of attendees, pre-registered participants were asked to confirm their participation few days before the event. As incentive for their engagement participants received a reimbursement of travel costs and an allowance. With Prof. Anton Zeilinger, the president of the Austrian Academy of Sciences and Prof. Alexander Van der Bellen, the commissioner for universities and science of the city of Vienna, the event was opened by two eminent speakers. During the whole event, a head facilitator acted as a moderator to guide the citizens through the summit and its different thematic elements in general. In addition, table facilitators were responsible for moderating the discussion rounds as well as for support of participants at their tables.

3.1.1 Recruitment of the citizen panel

The recruitment of the participants was mainly conducted by an external contractor in order to achieve a group of citizens reflecting the national demographics according to the criteria defined in the SurPRISE consortium, i.e.

- **Age:** Citizens from various age groups, which illustrate a representative picture of the Austrian population.
- **Gender:** about equal numbers, (50% women and 50% men, which is almost consistent with the gender distribution in Austria[74])
- **Geographical zone:** In Austria, participants from Vienna and two further surrounding provinces (Burgenland and Lower Austria) were recruited. This choice was made in order to minimize the risk of no-shows and to reduce costs for travel compensation. These areas also provide 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 as far as possible 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.

In addition to the contracted recruitment, the Austrian summit was announced via press releases in the media and on the ITA/OeAW websites. These announcements also included information on participation to provide also open recruitment and raise awareness on the summit. Some journalists also followed the summit on the spot and reported in radio and print media.

[74] Statistics Austria (2014): "Bevölkerung im Jahresdurchschnitt" http://www.statistik.at/web_de/statistiken/bevoelkerung/bevoelkerungsstand_und_veraenderung/bevoelkerung_im_jahresdurchschnitt/index.html

3.1.2 Basic elements of the participation process

In order to ensure a certain level of basic information participants received an information brochure about the SurPRISE project in general and the relevant topics for the citizen summit (i.e. the role of the different surveillance-oriented security technologies regarding privacy and security). The two SOSTs the Austrian summit focused on were smart CCTV and Deep Packet Inspection (DPI). To gain deeper insights into the opinions of participants the SurPRISE forum followed a mixed approach with a combination of 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. In each country, the whole setting was supported 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 to the corresponding SOST. The provided mix between written (the information brochure) and visual (films) information ensured that the information level among the participants was widely similar which enabled discussions on a relatively equal level. For each table, a moderator was assigned to moderate the discussion rounds and support participants if necessary in case of general requests. In preparation of the summit table moderators received guidelines about the process design and were instructed how to perform their tasks. In total, three discussion rounds had been conducted: one for each SOST focussing 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 on the different issues presented. The third and final discussion round aimed at participants developing suggestions and recommendations to policy makers at national as well as European level.

3.2 Structure of the citizen panel

In total, 260 persons had been invited, from which 234 participants were present at the summit. With 0nly 10% percent, the drop-out rate of this sample was relatively low. The participants represented a good mix of the Austrian population with a relatively balanced structure regarding age, gender, education as well as citizens from urban (10%), rural (32%) and metropolitan (49%) areas (see Figure 3 and Figure 4). With 48% (Female) and 49% (male) participants from both genders balance each other. This balance also largely prevailed in the different age categories; a slight majority of participants belong to middle-aged groups (between 40-59), as shown in Figure 2 below.

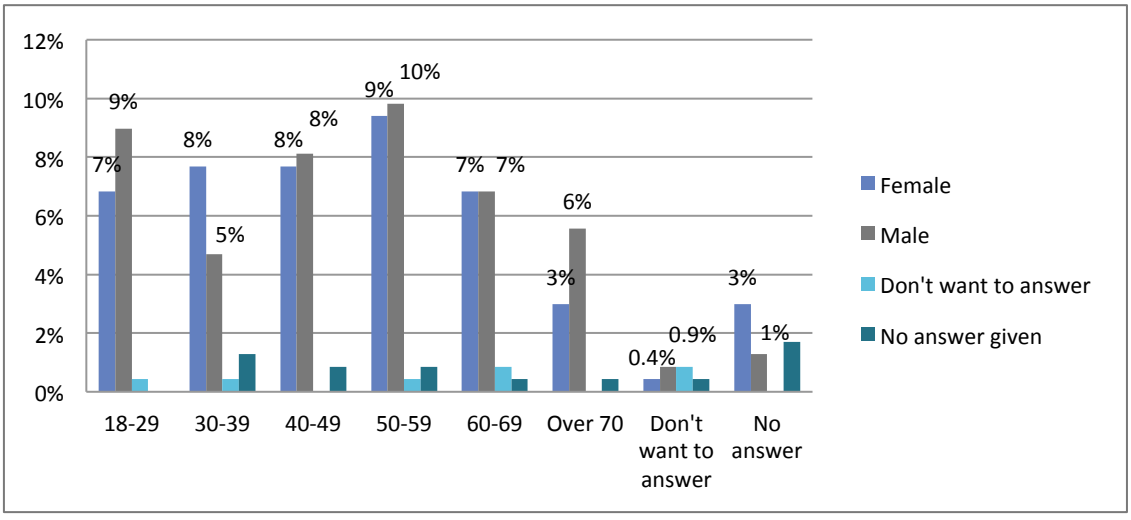


Figure 2: Age/gender structure

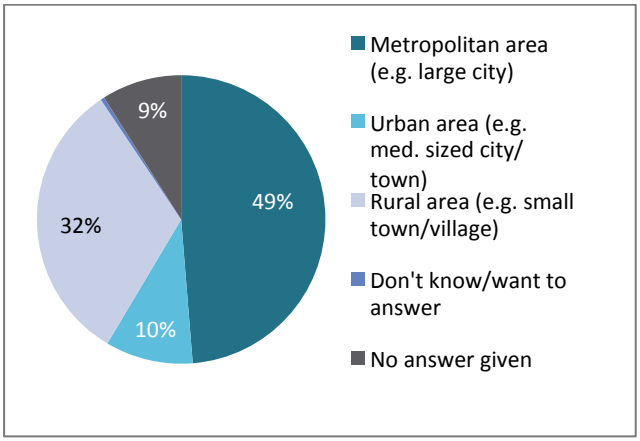


Figure 3: Area of living

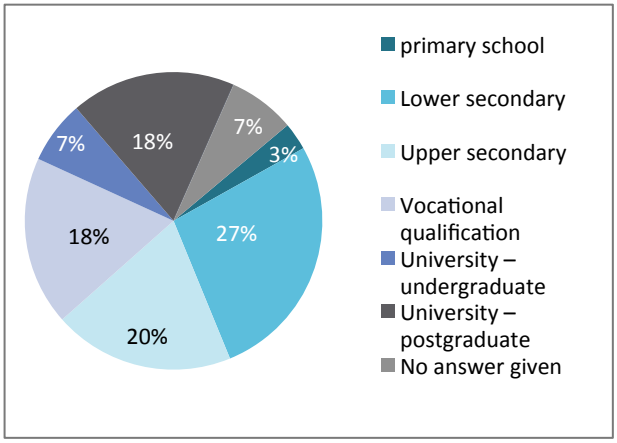


Figure 4: Education

3.3 How citizens assess the summit

In general the feedback of the participants was very positive towards the purpose of and to all components of the event. With 66% the majority stated to have won new perspectives on the main issues of the summit – privacy, security and surveillance. About 54% of the participants agreed or strongly agreed that the meeting had generated valuable knowledge for politicians. 45% of participants did not change their attitude towards SOSTs, while only 3% had a more positive, 45% stated that they had a more critical attitude after participating in the event.

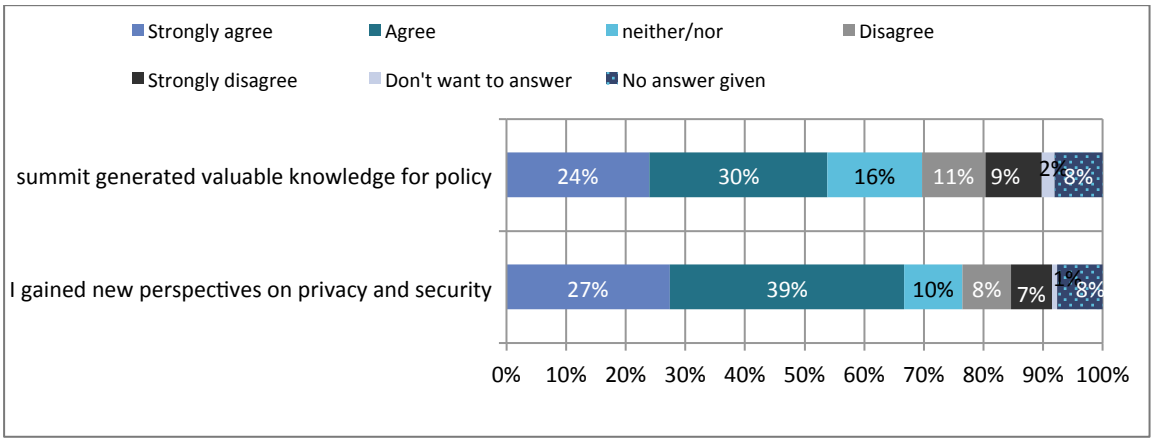


Figure 5: Attitudes on new perspectives and knowledge for policy

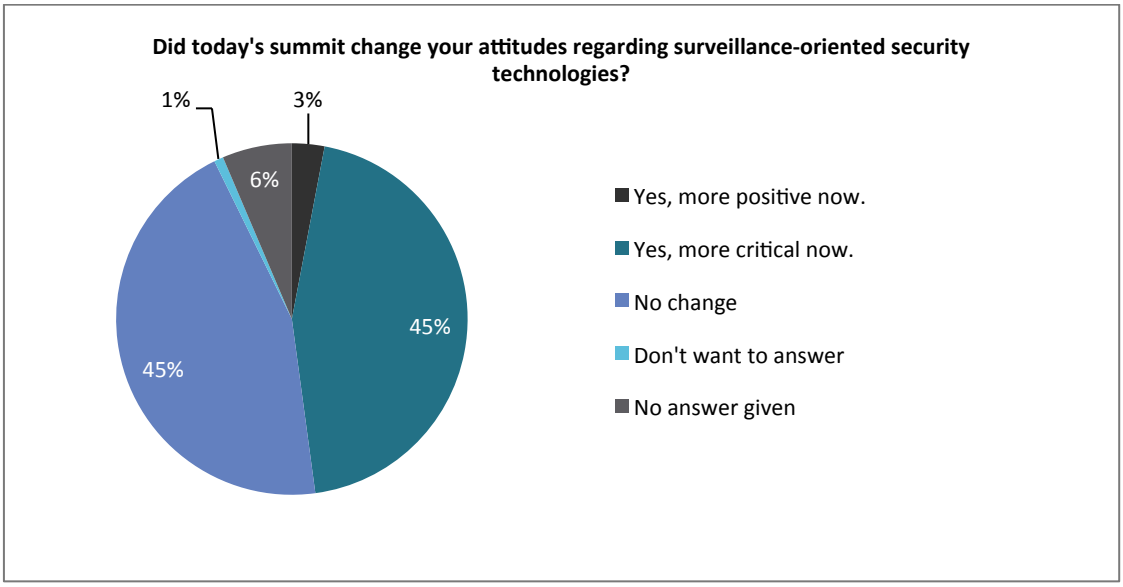


Figure 6: Changing attitudes on SOSTs

The positive atmosphere was also reflected in the vivid debates at the tables which in several cases went on until the head facilitator had to remind to come to finish the discussions by referring to the time schedule. In line with the controversial topic of the summit, discussions dealt with a variety of issues regarding security, privacy and fundamental rights. Although the summit put some emphasis on the two SOSTs and technology in general played an important role, in most discussions the different aspects of surveillance, security and privacy not merely linked to specific technologies received much higher attention. This underlines the high relevance of these issues for the majority of participants and some awareness about the privacy-security discourse in general. The notes and observations during the summit show that the degree of knowledge among participants was quite diverse which had some impact on the quality of discussions. The general quality level of discussions was unexpectedly high for such a diverse group of people with different backgrounds. Several discussions in the recommendation round at the end of the summit were very reflected and profound; several participants gave additional input via the post cards, some also provided their notes to their table facilitators. This supports the impression that the summit raised awareness and interest for the topic also beyond the summit. Some people also gave feedback via email few days after the summit expressing their thanks for the good organization and that they also discuss these issues with their family, friends and acquaintances.

4 Empirical results of the citizen summit[75]

This section presents the main quantitative and qualitative results of the Austrian citizen summit. The analysis provides deeper insights into the perceptions of citizens on privacy, security and surveillance based on the output of the survey as well as the three thematic discussion rounds conducted at each of the tables (one for each SOST and the final recommendation round). To grasp the different views and concerns about the complex interrelations between privacy, security and surveillance the material combines general and technology-focused elements.

4.1 General attitudes on privacy and security

The clear majority of the panelists feels secure in their daily life (78%) and perceives that Austria is a secure country to live (81%). Compared to this relatively distinct assessment, online security is perceived as more controversial: 60% of the respondents are worried about their security online, while 38% do not share this concern. This suggests that privacy and security on the internet plays some particular role in the citizens' view; and, more generally indicate that technology usage might affect the views on 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).

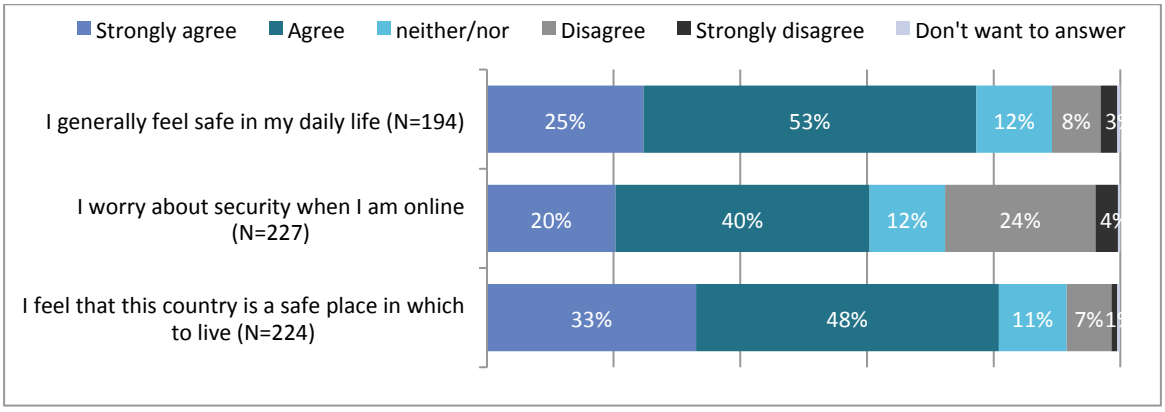


Figure 7: General attitudes on security

Changes in the security attitudes

To explore whether attitudes might have changed during summit due to further input from intensive debates and elaboration of the issues from different angles citizens were asked at the beginning and at the end of the summit to assess the statement whether SOSTs should be routinely implemented to improve public security. A comparison of the answers given at the beginning and the end of the summit reveals that citizens seem to encounter an ambivalence regarding privacy and security in relation to surveillance-oriented security technologies, as illustrated in the figures below:

[75] For better readability, the percentage values in the charts are rounded, which thus in some cases can contain marginal rounding differences.

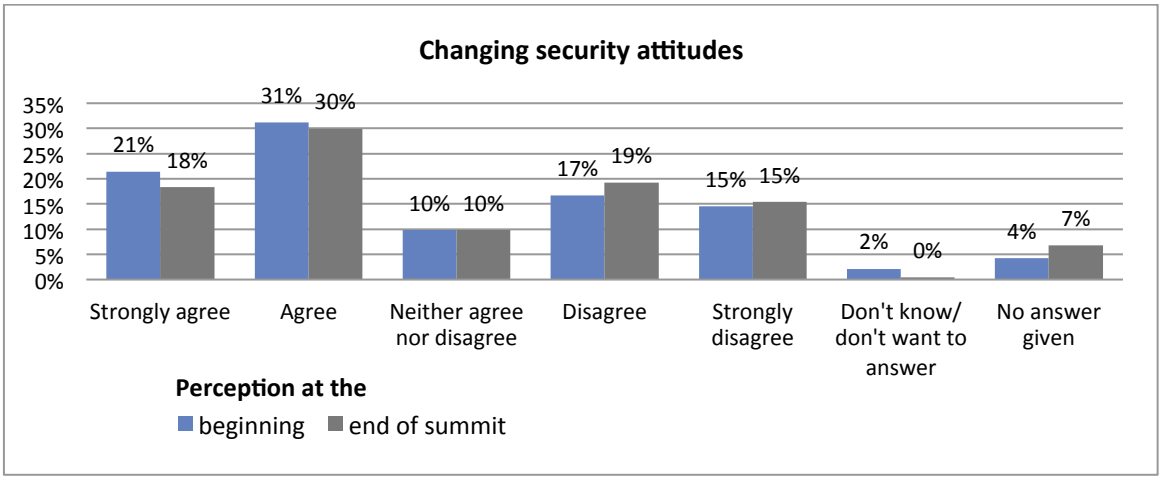


Figure 8: Changing security attitudes[76]

In the beginning of the summit, over 50% shared the opinion that surveillance-oriented security technologies should be routinely used to improve public security while 32% oppose this view. This assessment has slightly changed until the end of the summit, where 48% shared this opinion, while 34% disagreed. Attitudes slightly shifted towards a more critical assessment. Interestingly, the "neither, nor" position remained stable while "no answer given" also increased. One explanation for these changes is that the discussions brought in other views and stimulated the participants to consider different perspectives and reflect more about the different issues on security and privacy.

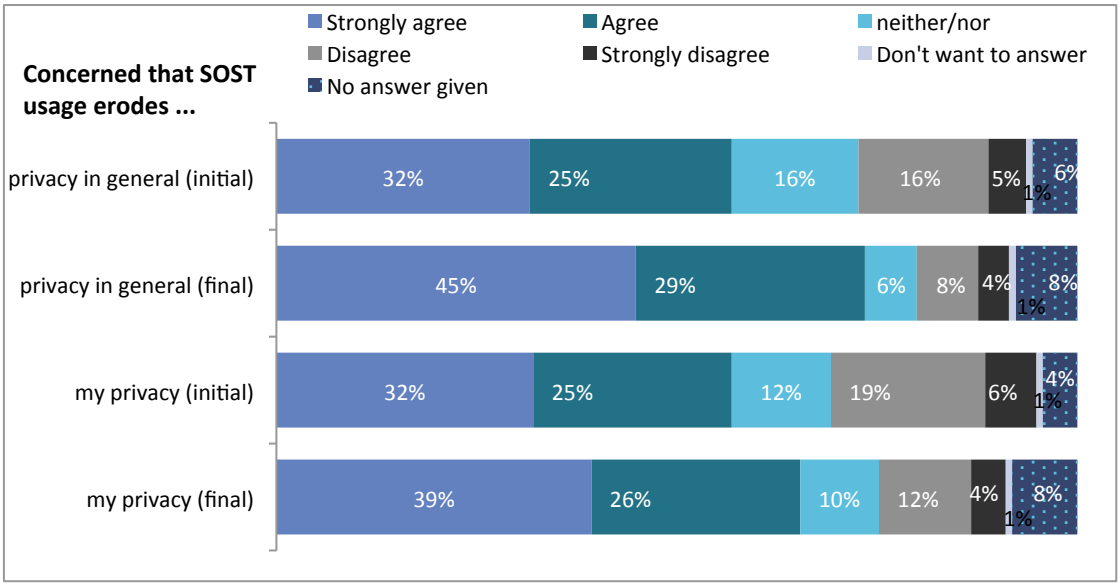


Figure 9: Concerns about privacy erosion due to SOST usage77

[76] Question: Overall I believe surveillance-oriented security technologies should be routinely implemented to improve public security.

[77] Questions: "I am concerned that the use of surveillance-oriented security technologies is eroding privacy in general."; "I am concerned that the use of surveillance-oriented security technologies is eroding my privacy."

Perceptions of individual and collective aspects

Privacy can mean different things to different people. For some it mainly refers to one's individual domains of his or her private life that have to be protected. However, it can also be understood as a societal achievement with high value for the public contributing to a balance between public and private spheres. How is this perceived by the Austrian citizens? Interestingly, participants seem to differentiate quite clearly between their "own" personal privacy and privacy in general for the society, whereas concerns regarding the latter were rated even higher. Hence privacy is not merely perceived as an individual right but also seen as a common societal value. This also reflects in the SOST-specific questions (see next sections). In the citizens' initial opinion at the beginning of the summit, the fear that SOST usage undermines privacy in general was agreed by 57% and disagreed by 21%. This significantly changed to 74% (agree) and 12% (disagree). The corresponding fear that personal privacy is undermined was shared by 57% while 25% disagreed. At the end of the summit respondents also changed their attitudes here to 65% (agree) 16% (disagree). The changing attitudes point towards a more comprehensive view on privacy with a stronger consideration of its value for the individual as well as the society.

At first glance, one might get the impression of a contradiction as the results indicate high privacy concerns about SOSTs as well as some reluctant agreement to use them routinely. The further analysis of the results as shown in the next sections resolves this seeming contradiction. The participants are aware of the importance of security measures, the entailed challenging tasks and accept the employment of SOSTs to some extent for law enforcement. However, in the opinion of the citizens this usage should be restricted, more focused and targeted on evident suspicion and not extensively used. The results underline that citizens wish to have a better balance between privacy and security.

4.2 How do participants perceive the use of surveillance-oriented security technologies?

In the previous section, the citizens' attitudes were examined on a general level. This section now takes a more specific perspective and deals with the different perceptions regarding the two SOSTs – smart CCTV and Deep Packet Inspection (DPI) as example of internet surveillance. These SOSTs represent emerging forms of surveillance-oriented technologies that can be expected to become of wider societal concern. While the former is more well-known the latter is relatively unacquainted to the wider public.

In line with the assumption that due to the differences of these SOSTs (e.g. CCTV is wide-spread, DPI is widely unknown and unregulated) the citizens' perceptions on these technologies are different. While 80% of the respondents stated to understand what smart CCTV is, 60% gave the same answer regarding DPI. The citizens perceived DPI as much more intrusive.

4.2.1 Perceived effectiveness vs. intrusiveness of SOSTs

The perceived effectiveness of the two SOSTs strongly differs. While for 56% smart CCTV is an effective security tool (against 21% disagreeing), only 27% share this opinion regarding DPI, while 53% have an opposed opinion (with 32% strongly disagreeing). In both cases, for 15% these SOSTs are neither effective nor ineffective indicating that for some participants the effectiveness is difficult to assess.

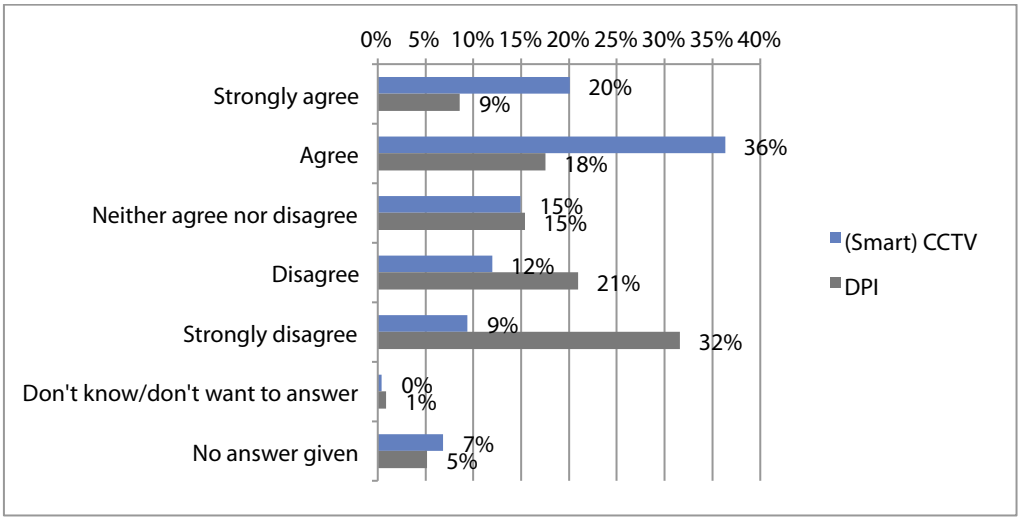


Figure 10: perceived effectiveness of [SOST] [78]

Figure 11 provides some further insights into people's perceptions about the usefulness and intrusiveness of the SOSTs. Regarding smart CCTV about one-third of the respondents perceives the technology as useful but highly intrusive while for 31% share the opinion that this SOST is useful and not very intrusive. For one-fourth smart CCTV is not effective and highly intrusive. As regards DPI the position is much more distinct as for near than the half (48%) this SOST is useless and highly intrusive, while 40% perceive it as useful and only 5% perceive little intrusiveness.

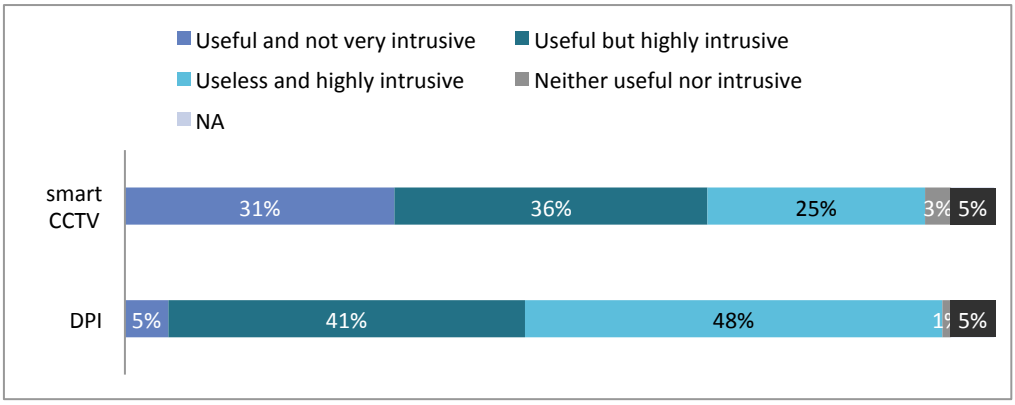
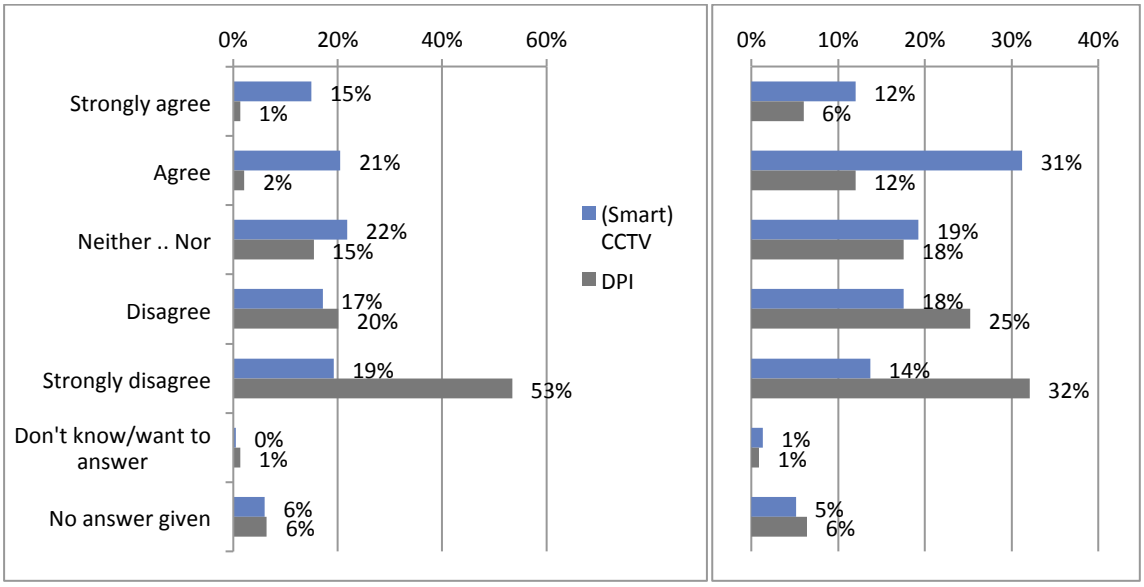


Figure 11: perceived usefulness and intrusiveness of [SOST]

Being asked about whether feeling more secure when the SOSTs are used (see Figure 12 below), respondents are undecided regarding smart CCTV: about one third agrees (36%), another third disagrees (36%) and the rest of 22% stating "neither/nor" directly expressed an ambivalence. Regarding internet surveillance, citizens had a more distinct opinion with over 70% feeling not more secure because of DPI (53% strong-, 20% disagree).

[78] Question: "In my opinion [SOST] is an effective national security tool."



Q: "I feel more secure, when [SOST] is used"

Q: "… is an appropriate means to combat security threats"

Figure 12: Perceived security gain

Relatively similar are the results regarding the perceived appropriateness of these SOSTs (the figure on the right): 43% perceive smart CCTV as appropriate to combat security threats (12% strong, 31% agree), whereas 32% perceive the opposite and 19% neither agree nor disagree. Regarding DPI the objections against this technology are significantly higher as 57% do not perceive this as an appropriate security technology (32% strong, 25% disagree).

In general, citizens seem to feel very uncomfortable with the employment of these surveillance-oriented technologies, whereas DPI (74%) was assessed to be much more threatening than smart CCTV (42%).

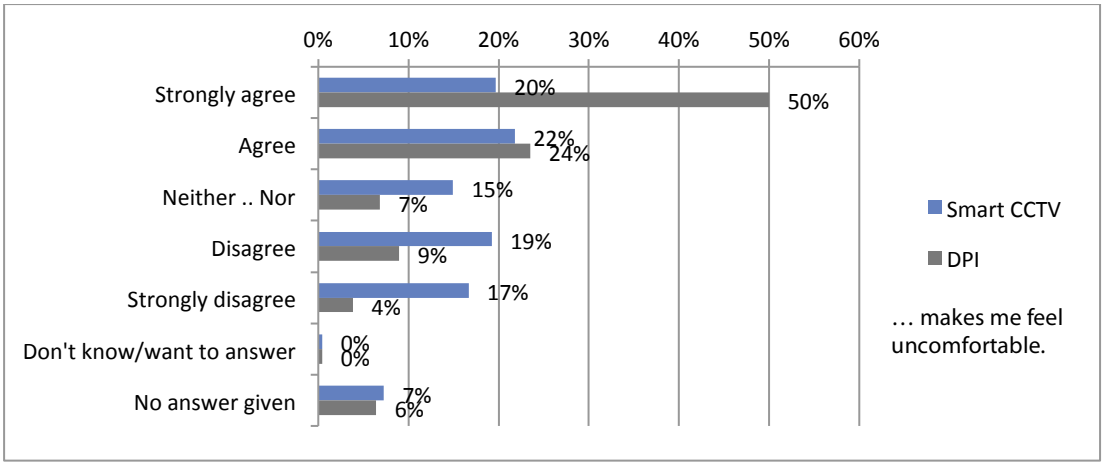


Figure 13: General uneasiness with the two discussed SOSTs[79]

Major concerns about SOST usage

Taking a closer look at the major concerns of citizens reveals quite pronounced worries about privacy infringements and misuse of personal information that may lead to misinterpretations of one's behavior. These concerns were not only related to potential privacy impacts in the participants' personal domains:

[79] Question: "The idea of [SOST] makes me feel uncomfortable."

63% of the citizens disagreed to be only concerned if smart CCTV is used in their living or working areas; in case of DPI, 55% disagreed to be only concerned if it is used to observe their personal online activities. A look at the major concerns reveals some relevant aspects for the citizens' assessment as shown in the figures below:

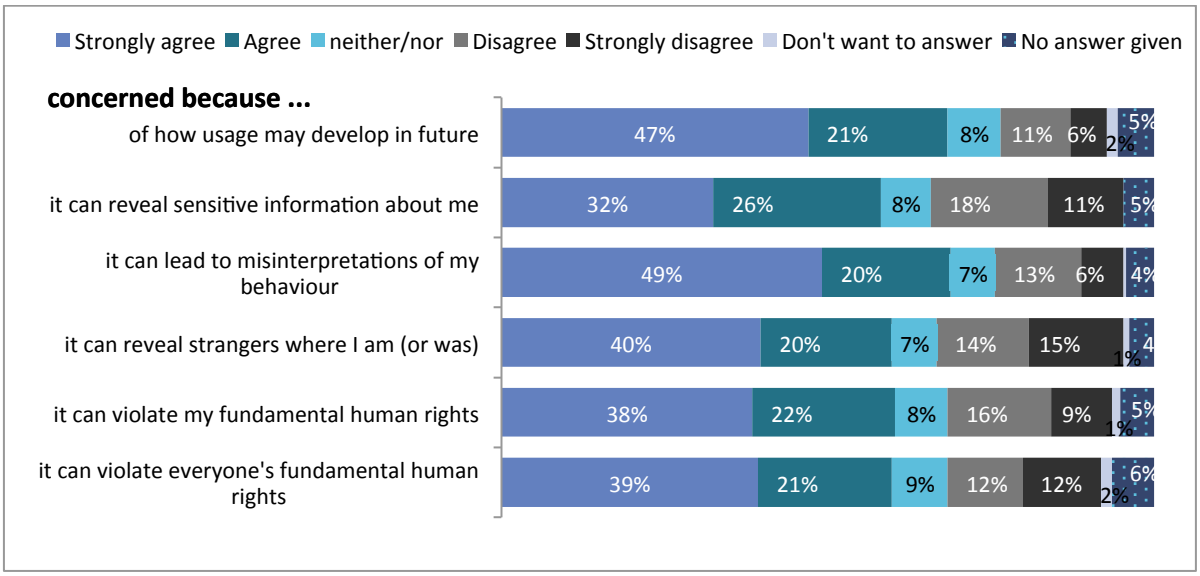


Figure 14: Major concerns regarding smart CCTV

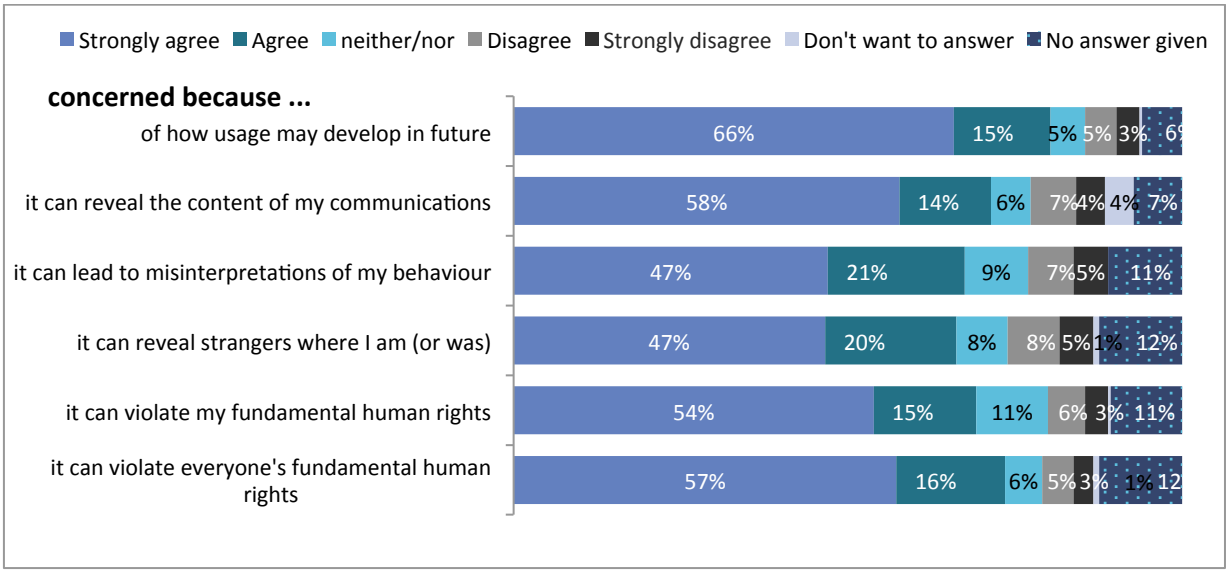


Figure 15: Major concerns regarding DPI

The clear majority expressed high concerns about SOST usage not only because surveillance affects them personally but seem to be highly worried about potential violations of human rights due to SOST usage on a personal as well as on a collective level, i.e. about everyone's human rights being affected (in both cases 0ver 60%). These concerns also reflect in most of the table discussions; often in relation a perceived lack of effectiveness of surveillance-oriented security technologies. At most tables it was controversially debated that untargeted SOST usage can hardly be effective but is highly intrusive. Despite of the peculiarities regarding the specific SOSTs, results mirror these concerns for smart CCTV as well as for DPI.

Conspicuous are the high concerns about how surveillance-oriented technologies might develop in future: Near to 70% of the participants fear about an extension of smart CCTV usage; with over 80%, worries about DPI in this regard are even stronger underlining the extraordinarily high perceived intrusiveness of this SOST. This is further highlighted by differences in the highest category: almost half of the participants strongly agree to be concerned about potentially upcoming smart CCTV usage while in case of DPI this concern is shared by two thirds of the responders. These significantly higher fears about internet surveillance are also visible in the different table discussions.

Different qualities of privacy intrusion and related fears

As already indicated in the answers regarding privacy concerns above, the clear majority perceives the use of both SOSTs as highly intrusive in case of DPI near to 80% of the citizens share this opinion.

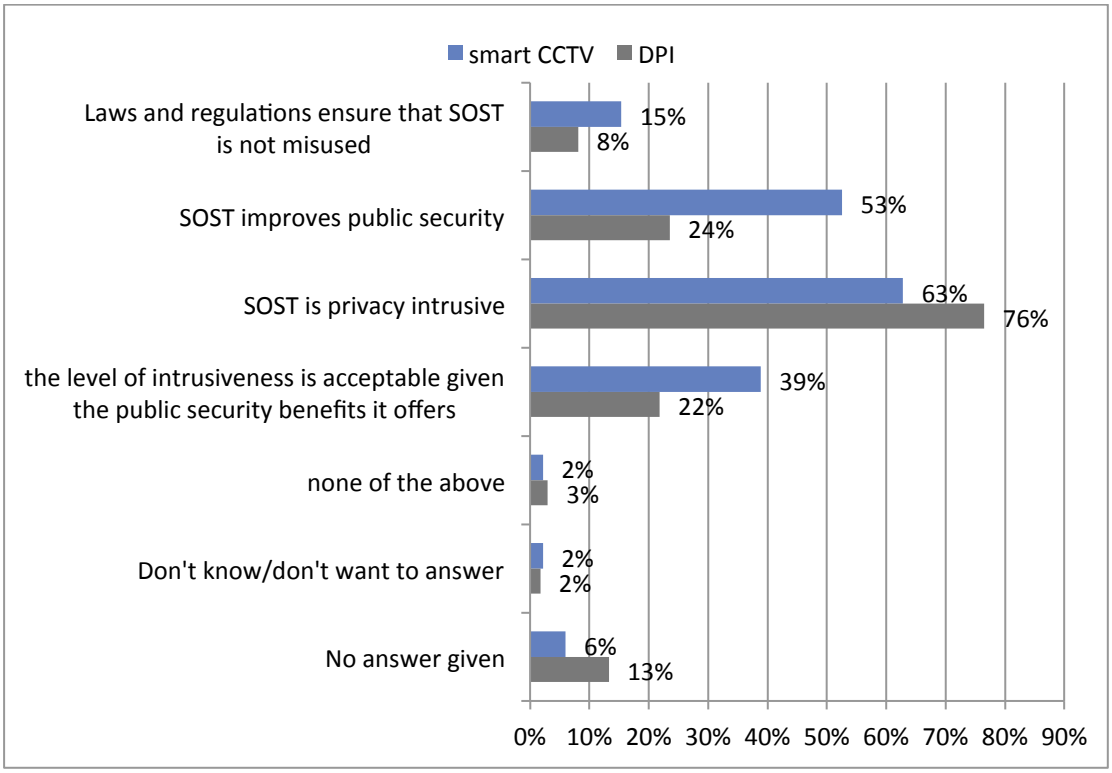


Figure 16: Perceived intrusiveness of SOST[80]

In line with the assumption that the familiarity and higher understandability play some role, regarding CCTV some participants argued with increasing habituation becoming more used to this SOST as in some areas it can hardly be avoided being observed. However, this does not imply that participants are less concerned about visual surveillance but they distinguish between different qualities of privacy intrusion. One of the participants for instance explained why she completely neglects internet surveillance: „CCTV only sees me but DPI knows everything I do and intrudes my privacy completely".

This view widely mirrored in a lot of discussions as DPI was heavily debated with high concerns and enormous fear of abuse. Broad agreement is given among the vast majority that DPI and internet surveillance and the monitoring of private communication has to be rejected. As major reasons for this rejection in most discussions it was found that it is not suitable to combat crime and is highly intrusive. Several discussants argued that this form of surveillance brought enormous potential for abuse which is not controllable, or in the words of a citizen: this "permanent surveillance cannot be stopped". As very critical was seen that everyone is targeted and it cannot be controlled what happens with the data which could also be manipulated. The effectiveness of this very controversial technology was widely questioned: "This does not make sense, because criminals and terrorists surely use a different wording

[80] Multiple choice question where participants could choose max. four of the presented options.

and not any suspicious key words", "there have to be other possibilities". Instead of investing in such technologies one participant made clear that "DPI has to be prevented by all means! Money should be invested in humans and not in technologies!", similar issues were raised by several other participants. Citizens also expressed many fears about future development of such technologies: "If this comes into the wrong hands the consequences are not foreseeable". While a number of the discussed concerns and fears where obviously related to privacy intrusion of online surveillance, several participants also expressed fears of censorship and the end of communication free from observation similar to totalitarian control. Some discussants draw parallels to regimes such as the STASI or regimes in some Arab countries where citizens are controlled and repressed.

Compared to the strict rejection of DPI there is a somewhat higher ambivalence given in case of CCTV. Regarding CCTV in several discussions aspects where raised that it can be useful and acceptable but should be limited to certain neuralgic points in the public: "in some areas, such as at airports, or high security areas, large-scale events, CCTV makes some sense." At a few tables, also the use of CCTV to monitor ATMs was seen as useful. Mainly the use at airports seems to be widely accepted as several participants mentioned that to some extent it seems reasonable to automatically detect luggage and suspicious objects. While the observation of objects was not seen as that problematic, at the same time, concerns were raised when it comes to observation of individuals and their behavior. The tracing of personal movements and behavior was seen as an enormous threat to privacy. A few participants said to feel more secure especially when a camera is present in shady environments and subway stations. One participant argued that it cannot prevent crime: "despite of the cameras a woman was raped during the day in the metro!" Some discussants argued that it can give information to find criminal offenders afterwards. Several participants expressed acceptance regarding the employment of CCTV in some sensitive areas and public spaces with a lot of people such as airports, or at large-scale events such as soccer games. But "monitoring of political events, demonstrations etc. is scandalous!" one participant pointed out. One discussant brought in that CCTV should be used to monitor police work to document proper work and have some evidence in case of violence. Most participants questioned the positive security effects of smart CCTV for several reasons: "Who determines what is abnormal/suspicious behavior?", "who is responsible for controlling the use of smart CCTV?", "who controls what happens with the images?", and similar questions were raised. As a consequence, in most of these discussions participants came to conclusion that smart CCTV should be restricted to sensitive areas and under several conditions. The most important condition mentioned is a strict limitation of usage and storage of the gathered data and footage: some participants elucidated that the information of non-suspects should be deleted quickly and "only footage relevant for justified suspicion of crime should be allowed to be stored - but nothing else!"; whereas also here the storage duration should be limited.

Major attitudes regarding SOST usage in general

To learn more about the citizens' perceptions several questions about the attitudes of SOST usage were asked (see Figure 17 below). Here the results give further insight into the tensions between effectiveness and intrusiveness. The perceived effectiveness of SOSTs for public security is quite controversial. The results in the previous section show this on a SOST-specific level and this is also the case on a cardinal level: 49% in total share the opinion that SOSTs contribute to improve public security. However, this agreement is somewhat hesitant as only 16% strongly agree while the highest share of 33% moderately agrees. At the same time, 25% disagree, 14% neither agree nor disagree and 12% did not answer. This indicates that the slight majority tends not to agree per se to this general statement. For the citizens the security gain seems to depend on the context of a SOST, i.e. for what purposes and under which conditions SOSTs are used. In the discussions a variety of aspects regarding purpose and usage of surveillance had been debated. High concerns were expressed about privacy infringement and overwhelming collection of personal information against the intention of the population. With 80% sharing the opinion that once surveillance technology is available governments make use of it[81] and

[81] Due to language-wise specifics, the German translation of Q87 for all German-speaking citizen summit events differs slightly from the English original, not implying a positive attitude regarding this issue as in the English version (If SOST is available, national governments might as well make use of it). Therefore, this result must be seen cautiously under the preface of being more negatively biased than this is the case in other countries where the summit event took place.

77% assuming that abuse of SOSTs is quite likely the Austrian population is very concerned about the problem of function creep.

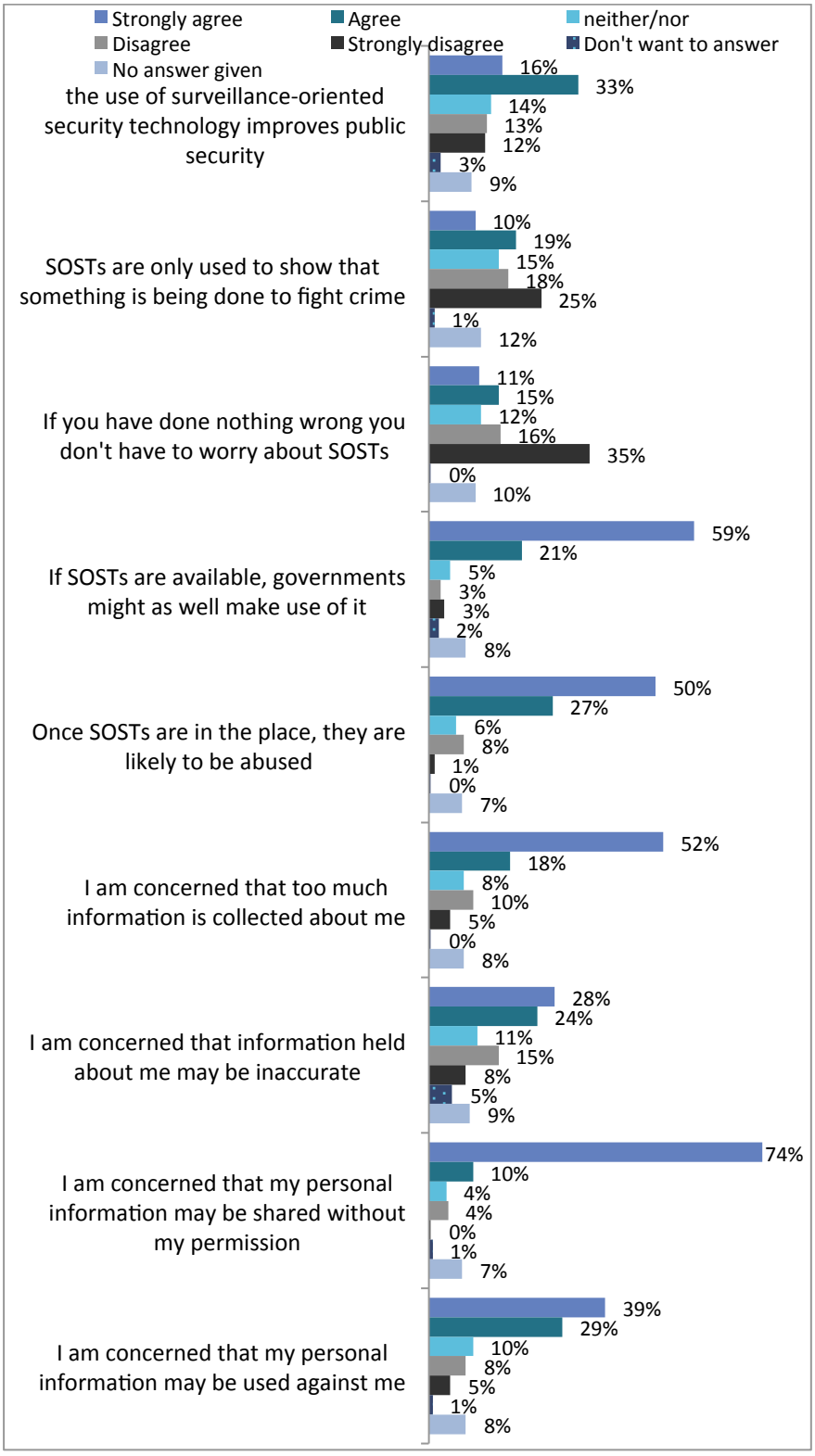


Figure 17: Major attitudes regarding SOST usage in general

Nothing to hide but highly concerned

"Nothing to hide" – as most classical argument to distract privacy concerns is not an option for the clear majority of Austrian citizens: 51% disagree to the statement that "if you have done nothing wrong you don't have to worry about SOSTs" while only 26% tend to agree. Instead, citizens worry precisely because SOSTs can be used against them even though they have done nothing wrong. At the tables the participants discussed intensively about the dangers of misinterpretation of the information collected by surveillance practices. The citizens see it as very critical in this regard that surveillance not just affects real suspects but mostly blameless and innocent persons. The fear was expressed that this can lead to wrong accusations. While real criminals often knew how to avoid being monitored the innocent have little options to avoid privacy infringements. Related discussions were concerned with the proneness to errors and false positives of surveillance technologies. "Who defines what is normal behavior?" "Is it acceptable to accept proneness to errors and wrong accusations in order to pre-detect potentially criminal behavior?" Some discussants complained that citizens did not have many options to do something against this situation. This perception is inter alia underlined by high concerns about extensive information gathering (70%) and 84% of the participants fearing that personal information is shared without their permission. A similar perception is also given regarding SOST usage (see next section).

4.2.2 Avoidance, resistance against surveillance

As shown in the previous section, despite of some differences regarding the two SOSTs, surveillance technologies in general are perceived as highly intrusive. The differences regarding the two technologies are explainable as they also represent somewhat different forms of privacy intrusion. The fact that DPI aims at the essence of online information and communication and thus has deep privacy impacts potentially comprising all types[82] of privacy, especially personal communication, behavior, thoughts and feelings and association is clearly visible in the results. But respondents also left no doubt to be concerned about visual surveillance by smart CCTV. In total, the opinion that these SOSTs are forced upon them without considering their needs is highly developed: in case of internet surveillance 85%, in case of smart CCTV almost 70%.

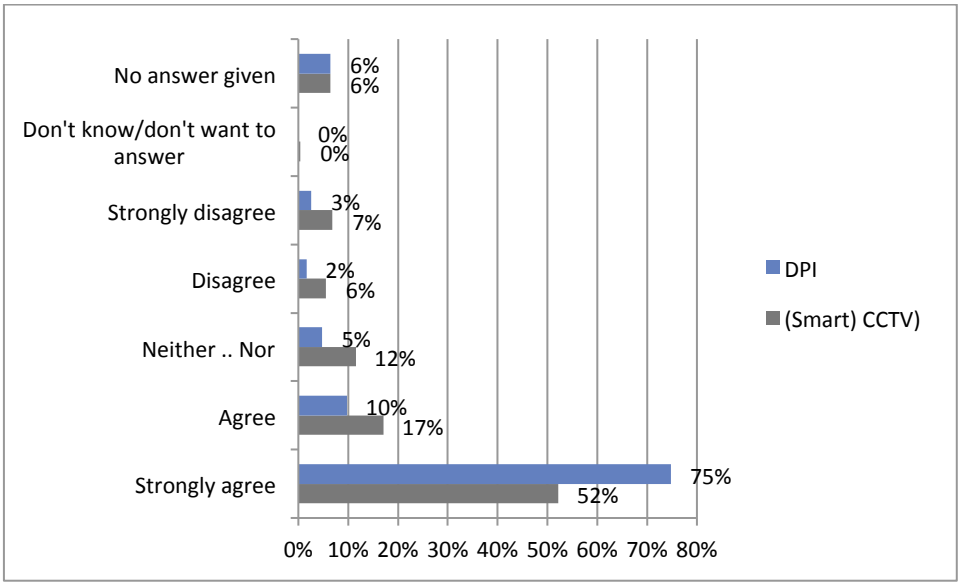


Figure 18: Question "I have the impression that [SOST] is forced upon me without my permission."

[82] S. Strauß, J. Čas, (2013) op. cit.

Security vs. privacy trade-off is not an option

As the results presented in the previous sections indicate, security and privacy does not seem to be a question of either the former or the latter for the participants. Hence, instead of trading one against the other, citizens wish effective security measures that respect their fundamental rights.

From a wider perspective, these results highlight that citizens see themselves confronted with technological surveillance activities beyond their control and without respect to their needs. Closely related to this is a perceived **lack of information** and control about the employment of SOSTs indicating strong demands for more transparency and scrutiny about security and surveillance activities. This is inter alia highlighted by about 50% of the participants in total wanting to know more about privacy protection (as shown in Figure 17). In the view of citizens transparency is one crucial connecting piece in this regard to come towards a better balance between effective security measures and privacy protection.

Power, control and transparency

The importance of transparency is confirmed by further results also in the table discussions, where these and related issues were debated. "A main problem is that the public is not informed enough about surveillance", "also the controllers should be controlled", and similar arguments were brought in. The use of surveillance data as well as information about existing limits and legal restrictions of surveillance in general were seen as very opaque and blurry. "What happens with surveillance data? Who can access it and why? Who analyses the data, who ensures that no innocent person becomes accused? What are the limits? Who decides what is normal and abnormal behavior? What if the political system changes?" These and similar concerns where stated by many participants that expressed fears about security authorities abusing their power. At several tables, the problem of function creep was discussed and that a gap existed between the official reasoning for online surveillance and hidden reasons such as espionage or suppression. Some persons shared their impression that surveillance discussions in the public distract from important topics such as finance scandals, corruption and "the real offenders". "**Control of the controllers**" was an important discussion point at several tables in relation a lack of appropriate mechanisms in this regard. Related to discussions about the lack of transparency and control of surveillance practices some participants also brought in further critical aspects such as "**manipulation of the masses" and the fear of censorship**. Especially as regards DPI and internet surveillance many citizens showed a strong resistance and left no doubt that the intrusion of personal communication is inacceptable to them.

Resisting actions and behavioral changes

In accordance with the perceived high intrusiveness of both surveillance-oriented security technologies there is a strong demand for more information on how to protect privacy (as shown in Figure 19 below). Differences regarding the SOSTs are relatively marginal here except the lack of opposition which, with 18%, is significantly higher regarding smart CCTV. Citizens show stronger resistance and willing to take action to prevent a further extension of internet surveillance. The relatively high value of no answers given might indicate a perceived lack of options for avoiding this more complex form of surveillance.

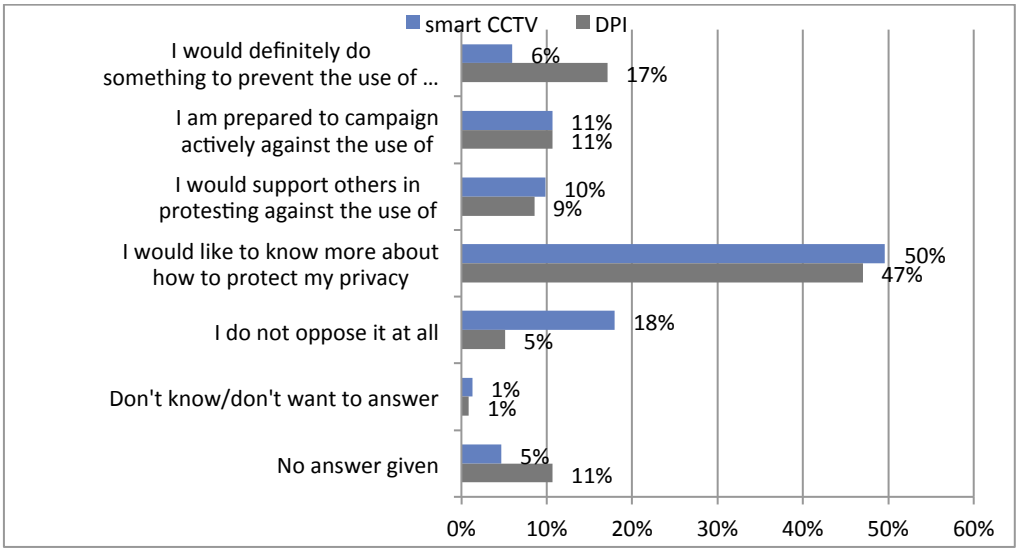


Figure 19: Actively challenging SOST usage

Being asked about what measures the participants would set to avoid being in contact with these SOSTs answers are quite different: while citizens seem to be relatively sure not to alter their behavior because of smart CCTV (definitely not 44%), behavioral changes because of DPI receive significantly higher values as 28% claim that they would change their behavior. However, also the perceptions and beliefs regarding no changes are in the similar range (25% are sure about no behavioral changes, 23% don't think so). This indicates some uncertainty about the extent to which the participants perceive that a SOST could be avoided by behavioral changes. As citizens expressed to want to know more about privacy protection this somewhat suggests that altering behavior might not be an appropriate option for them to deal with SOSTs.

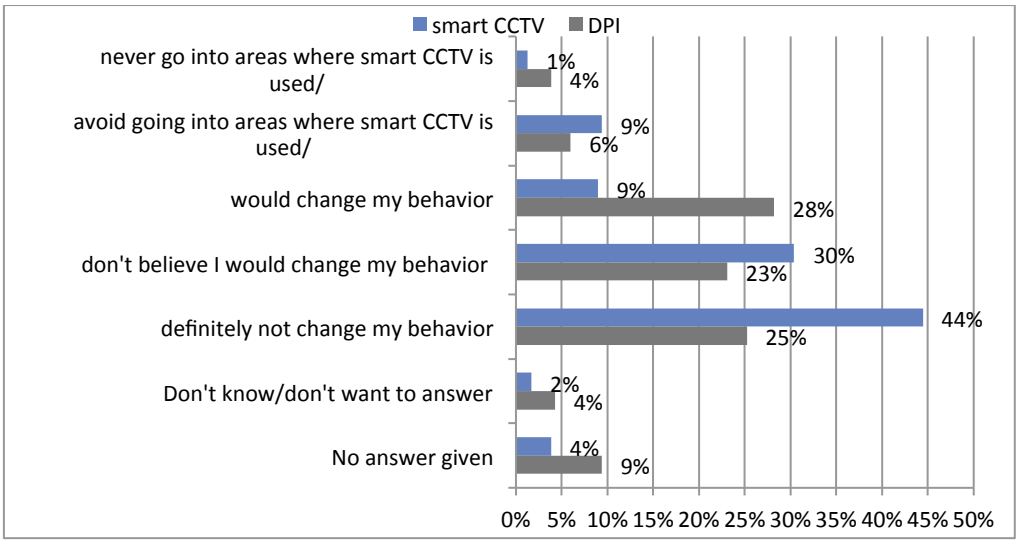


Figure 20: Actively avoid being subject to SOST

Social responsibility vs. lack of ability to act

In some discussions, a feeling of desperation was expressed that citizens cannot do anything against surveillance. Some participants even expressed anger about surveillance being conducted without even considering the citizens' opinions and needs. In several discussions issues were raised regarding self-determination, civil courage, solidarity and social responsibility. One participant mentioned that in his view "more social dialogue and more communication" between security authorities and the public is important as "technologies do not prevent crimes". Also aspects of the chilling effect came up as some citizens shared the opinion that surveillance has negative effects on social cohesion and solidarity as it might become chilled and disturbed. Other participants did not just see low solidarity and lack of civil courage as negatively affected by surveillance. They also argued that people need to be supported and strengthened in being solidary and showing civil courage as something crucial to establish more social capacity to deal with security challenges.

4.3 Trustworthiness of security authorities and the role of alternative security approaches

Trustworthiness of security authorities is among the most controversial issues, which reflects in a number of results:

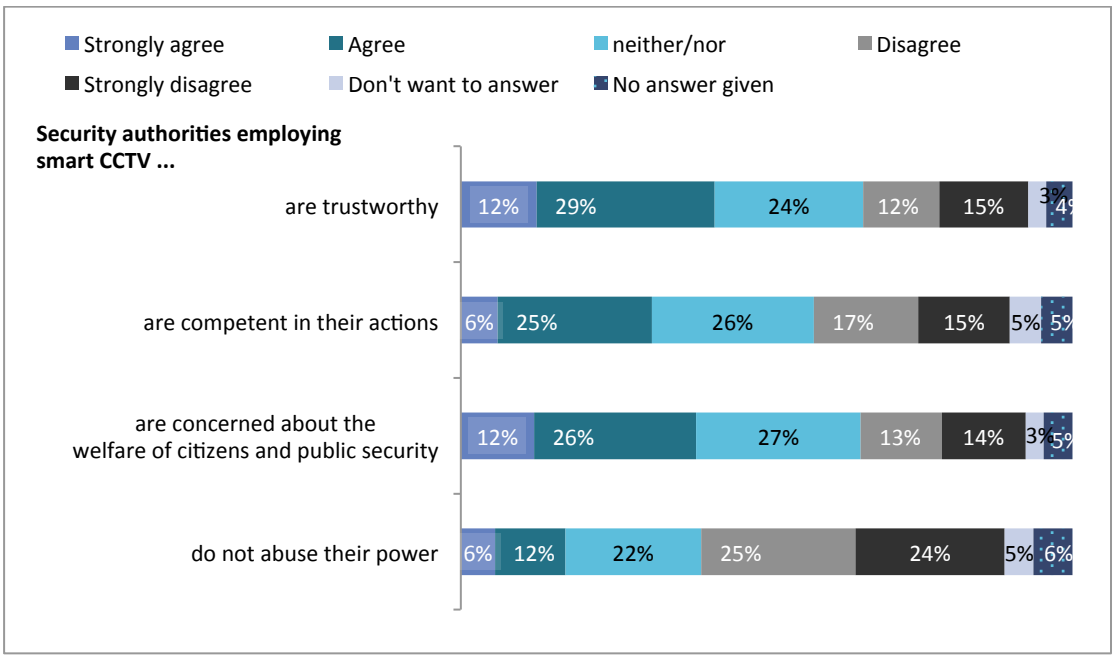


Figure 21: Perceived trustworthiness of security authorities employing smart CCTV

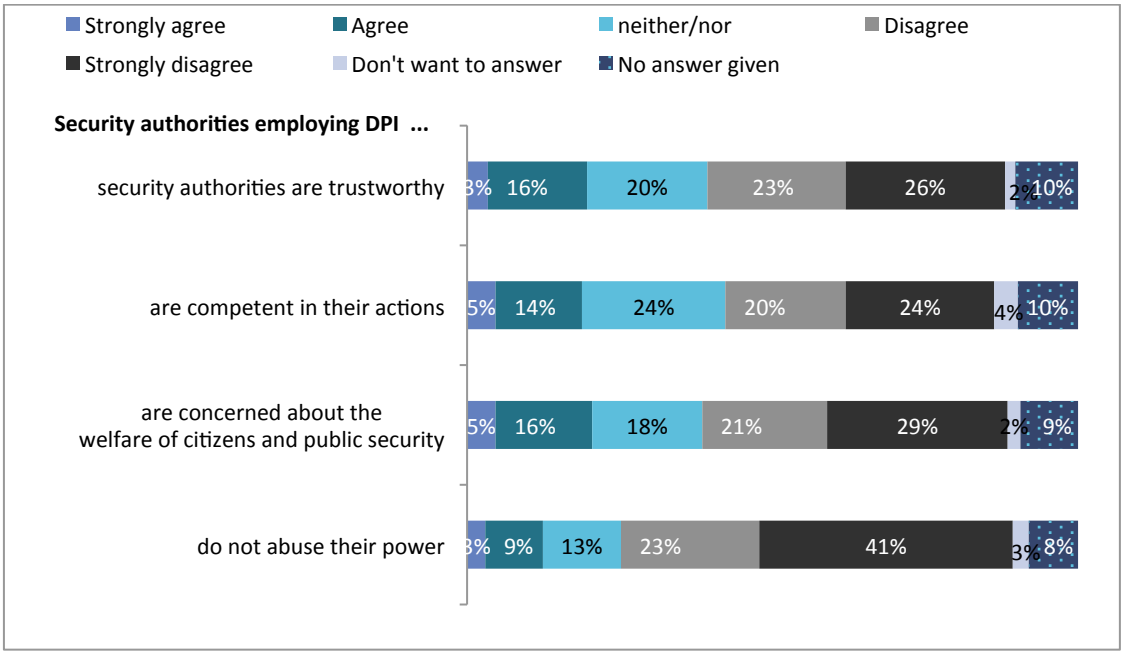


Figure 22: Perceived trustworthiness of security authorities employing DPI

Insecurity, uncertainty and misleading trust

In line with the perceived high intrusiveness of SOSTs and the related worries and fears of citizens about privacy infringement, trust in security authorities employing surveillance-oriented security technologies is relatively complex. Several respondents perceive security authorities as trustworthy: with 41% this is significantly higher in case of smart CCTV, while only 19% perceive this for authorities using DPI, confirming the related fears of citizens. The abuse of power is a major concern in both cases with 49% regarding smart CCTV and 64% regarding DPI. These results indicate some insecurity about the foundations of trust in security authorities. Not least because of the "neither/nor" positions, which are notably high (compared to other results) despite of the SOST-specific rates. This gives the impression, that citizens are quite uncertain regarding trustworthiness of security authorities. On the one hand, this refers to some resistance against the employed measures (as shown in section 4.2). On the other it also indicates a perceived lack of options to build trust.

The discussions provide some explanations for these controversial issues regarding trust: As the overall results reveal, the majority of citizens has a critical perception on the purpose and use of the SOSTs which is widely perceived as intrusive and ineffective. This raised further concerns regarding abuse of power by misusing the information gathered by surveillance technologies. In the table discussions the role of trust was mostly seen in relation **to lack of controllability of security authorities and surveillance practices:** Many participants perceive that the public has insufficient information which reinforces concerns: "A lack of information and transparency triggers fear". With surveillance measures that intrude privacy based on a lack of trust in the observed individuals one can hardly trust in the authorities conducting these measures. Against the background of these results, citizens feel less secure and perceive that their fundamental human rights are in danger because of perceived overwhelming security and surveillance activities. Quantitative as well as qualitative results highlight that citizens are in strong favor of alternative approaches without surveillance technology and demand more transparency of SOST usage in general.

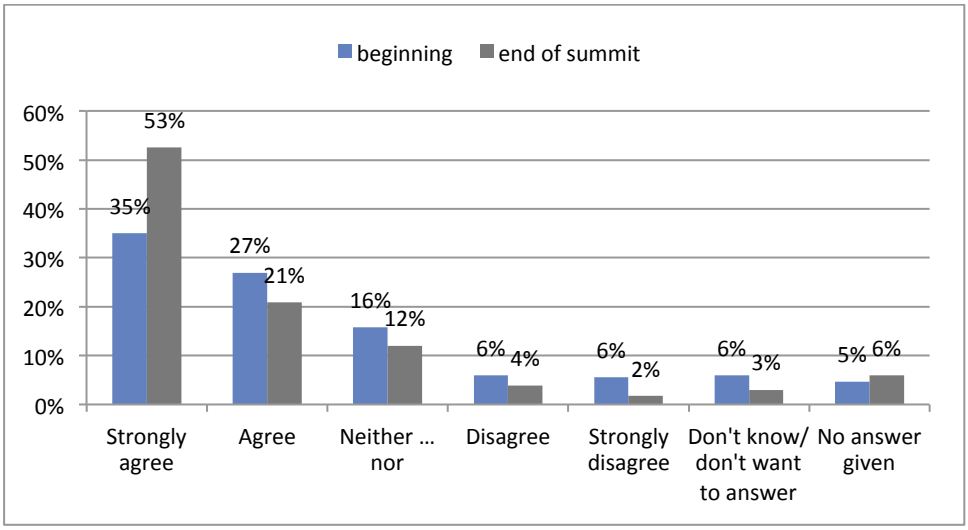


Figure 23: Role of alternative security approaches without technological means[83]

Figure 23 shows that participants wish to have more focus on alternative security concepts without surveillance that are less privacy intrusive. These results indicate a more critical reflection among participants about purpose and usage of SOSTs. This also corresponds with the attitudes on alternatives: Being asked about alternative security concepts without surveillance technologies, the already high values of 62% (agree) vs. 12% (disagree) in the beginning changed to 74% (agreed) vs. 6% (disagree).

Regaining trust with less surveillance and more checks and balances

In the views of the citizens alternatives include actions needed to regain trust in the political system. To improve the current situation a number of issues and suggestions had been discussed. "Laws and regulations lag behind technological surveillance possibilities therefore there is a lack of trust in regulation" stated one discussant and argued for more control of surveillance technologies in accordance with effective legal frameworks. This argument came up at several tables also in relation to a need for certain legal prohibition of general storage and retention of surveillance data. Several participants took a stand for legally restricted storage duration and binding rules for the deletion of personal information. Also regulatory challenges regarding national and international laws were raised: "It is not clear who is in charge and responsible administrative authority for international surveillance. How is this regulated?" Discussants here identified a need for national actions to limit surveillance but also for international regulations in order to reduce disparity between different countries and impact of SOSTs beyond different legal borders.

4.4 Citizens' recommendations to policy makers

The table discussions qualitatively mirrored the results of the quantitative part of the citizen summit. Citizens developed a variety of recommendations for policy makers on national and European level. Despite of the variety of discussions at the tables the vast majority of citizens send a **clear message: less surveillance, more transparency, scrutiny of SOST usage and a general demand to foster checks and balances**. This message grounds on high concerns and fears of privacy abuse that does not result from a resistance against security measures and authorities in general. On the contrary, the citizens recognize the important role of security authorities and their challenging tasks as shown in several discussions. However, citizens are not willing to accept privacy intrusions but on the contrary wish to have effective security measures that do not undermine privacy. Citizens are highly concerned about **function creep and uncontrolled power** due to surveillance technologies. Security authorities are thus advised not to abuse their power and not to act beyond their legal competences. This was underpinned by a variety of recommendations and suggestions aiming at improving measures to **control the work**

[83] Question: "Alternative approaches to security which do not involve surveillance oriented security technologies should be given higher priority."

of security authorities and their actions. Several of the pressing issues for citizens refer to the **presumption of innocence** which is a core principle of justice systems. At many tables the fear was expressed that this principle might erode with increasing mass surveillance as then everybody becomes suspicious without even noticing it. Here a gap between surveillance under known or plausible suspicion and untargeted surveillance of the masses was seen as very critical problem that lead to a situation where the threats of security measures exceed the potential benefits. Several participants argued towards more control of surveillance activities and the demand for justified reasons for surveillance in order to target real suspects and criminals instead of the general public. This was also seen as a great barrier to the effectiveness of SOSTs because untargeted mass surveillance was also perceived as a critical economic factor that causes enormous costs and brings little security benefits. Citizens made clear to want more evaluation (and according information) of purpose, appropriateness, costs, impacts of SOSTs and surveillance practices in accordance with **proportionality**. Some participants mentioned data retention and that surveillance measures are mostly paid by tax payers respectively the citizens themselves. The wider surveillance goes the less it is effective and the more it raises costs as a lot of irrelevant information was processed, as one discussant argued. Hence it was argued that it needs to be clear who is allowed to gather and use which information and why. To reduce the risks of privacy abuse the citizens call for regulatory measures that limit the use of surveillance data and make data access only possible by according court decisions.

As regards security measures the majority is in favor of a stronger focus on the development and use of **alternative concepts** away from the current technology centered security concepts. Both SOSTs were seen as critical whereas DPI was strongly rejected by the majority, argued by its perceived massive intrusiveness and threat to privacy and other human rights. This strong rejection against one particular SOST does not mean that citizens are more in favor of another surveillance technology. Instead, for citizens the problem of surveillance goes deeper and beyond the employment of SOSTs. Similar is the case for alternative concepts which are not merely understood as alternatives to technical means but as alternative foci to reduce the identified high perceived threats triggered by surveillance activities. In line with the citizens' major message to restrict surveillance and foster transparency the clear majority located a lack of information on the employment of SOSTs as well as the reasons behind their use. At the tables several aspects about the lack of control of SOST usage and the according authorities had been discussed. Some tables also developed relatively concrete suggestions to improve accountability and responsibility of security authorities for the employment of SOSTs in order to come towards more scrutiny and controllability of surveillance activities. In this regard, citizens wish to have independent control units that scrutinize the proper use of security technologies and practices to **ensure commensurability and proportionality of security and surveillance**. A number of tables particularly recommended the installation of ethic commissions and the **reinforcement of data protection authorities** in order to reduce privacy intrusion and appropriately support security measures in accordance with legal regulations.

In general, citizens are quite in favor of more focused and justified security measures which was discussed at the majority of tables. Or in the words of a participant "there is a need to differentiate between different potential threats". Prevention was considered as important but with different measures: instead of reinforcing surveillance, citizens highlighted the need **for more investments into social justice and education**. This was not just meant in a general way but also regarding more investment in qualified security personnel and better trained staff for security authorities. In general, citizens consider the work and competence of security authorities as highly important. As problematic in this regard citizens discussed a lack of well-trained staff and limited resources for police units. Besides the highlighted demand for enhancing transparency and control of security authorities also a need for better equipped executive forces and mostly better trained and educated staff was raised. In the view of the citizens this should be improved in order to allow for different security foci in accordance with privacy and the needs of society.

5 Summary and Conclusions

In the last decade, Austria has undergone several changes and faced new challenges in privacy and security policy. Transformations in global and European security policy triggered some action at national level to adapt security strategies to the changing requirements. While on the one hand, this includes reasonable measures to deal with contemporary security challenges, on the other hand, some of the measures have impacts on privacy in a way that amplifies tensions between security and privacy. A major issue in this regard is the shift towards more pre-emptive surveillance practices aided by different kinds of technology. In Austria this shift inter alia led to a successive extension of powers given to security authorities such as police forces (as outlined in section 2). These developments are seen as controversial by the wider public which is visible in several critical debates about privacy and surveillance, and most prominently in the discourse about data retention where many citizens expressed their fears and concerns. To some extent these complex and controversial issues mirror in the Austrian citizen summit.

Instead of following a delusive line of argumentation such as "those who have nothing to hide have nothing to fear", participants highlighted that they neither want to fear security measures nor lose their privacy. Hence, in the view of Austrian citizens the assumed trade-off between privacy and security is not appropriate – neither for the effectiveness of security measures nor the protection of privacy. On the contrary: the vast majority of citizens expressed with a broad variety of concerns and issues that they demand both: effective security measures that are in accordance with an effective protection of their privacy. This demand is clearly visible in the summit results and was underpinned by a number of arguments and suggestions citizens developed during the participation process. The Austrian citizens made a quite strong statement towards a revision of security foci and according measures. They have a strong resistance against untargeted security practices and use of surveillance-oriented security technologies in this regard. While the majority feels quite secure in their daily life, a strikingly high amount of citizens expressed enormous concerns that privacy is heavily threatened. The analysis reveals a distinct fear that the already strained relation between privacy and security aggravates further. This is particularly the case as regards the increasing use of SOSTs which was assessed as highly intrusive. Here some distinctions are given in the assessment of intrusiveness; indicating that, related to the different types of privacy (person, communication, behaviour, etc.), for citizens the intrusive capacity of a SOST also makes a difference in the perception of privacy threats.

Despite of their high concerns citizens are not neglecting security measures per se but stated demand for solid approaches that do not undermine privacy of the general public. The variety of recommendations underpins an urgent need to revitalize checks and balances. The citizens are in strong favour of more effective control units to scrutinize surveillance practices and that security authorities work properly and in accordance with fundamental rights. In relation to the effectiveness of privacy protection citizens expressed the importance of their right to know about security and surveillance and the usage of personal data. Here the role of DPAs is addressed. As outlined in section 2.3, data protection authorities in Austria had to encounter several difficulties, not least the difficult situation of lacking resources which has been criticized for many years. This issue seems to be of wider public concern as the citizens underlined the crucial role of DPAs and wish for revitalization and reinforcement of their competences and capacities.

The work of police and other security authorities in general is perceived as very important to the Austrians. However, they observe a gap between security and surveillance competences and their appropriate implementation. In other words: surveillance measures are perceived as being too extensive and untargeted. In order to alleviate this situation, citizens identified pressing demand to restrict surveillance to bring it back at an appropriate and acceptable level, i.e. more effective security measures that do not undermine privacy. In this respect, it was expressed that security authorities need to be improved in their capability to deal with contemporary security problems. In the views of citizens this not least also needs more training and qualified security forces instead of extensive use of surveillance technologies.

To come toward a setting where both – security and privacy – are "safe and sound" citizens wish the focus to be set away from mass surveillance towards developing alternative approaches without

surveillance technology that are less intrusive. This demand had been repeatedly expressed in different shades in the table discussions. Participants were noticeably motivated by exchanging their thoughts and concerns; they became more confident and open to developing their own ideas and suggestions. Based on the vivid discussion climate citizens developed a set of recommendations that enabled different perspectives on alternatives without a narrow security lens. As most important alternative citizens highlighted the role of effective control mechanisms to scrutinize that security authorities work properly and in accordance with fundamental rights.

The main recommendations of citizens are:

- Reduce and restrict surveillance technologies and practices
- More transparency of security and surveillance actions and according information
- More investment in humans not in technology
- Strengthen social coherence, civil courage and social responsibility
- Better training and education for security forces/personnel
- Enhance transparency, information and participation
- Awareness raising in the public for privacy and security
- Better integration of civil society and human rights institutions into security policy
- Fostering the role of science and research particularly as regards alternative approaches
- Reinforcement of independent data protection authorities to scrutinize security measures

Overall, the Austrian citizen summit revealed and underpinned a certain demand for action to change the modes of security and surveillance in a way that is accordant with the respect of fundamental rights. The citizens made clear that this is a sine qua non for the effectiveness of security measures. If SOSTs and security measures are perceived as menace to societal values and to the well-functioning of society by the wider public they cannot be effective or appropriate means for public security. The identified needs to revitalize and foster the protection of fundamental rights to rebalance the relation between privacy and security are not least crucial to regain and reinforce trust of the citizens in their political-administrative system in Austria as well as in Europe.

6 Bibliography

Aichholzer, G & Strauß, S (2010): "The Austrian case: multi-card concept and the relationship between citizen ID and social security cards", *Identity in the Information Society (IDIS),* 3, pp. 65–85.

Allwinger, K & Schillhab, J (2008): "Vertrauen der ÖsterreicherInnen in den Datenschutz", Baden: Oekonsult Communication & Consulting ges.m.b.h. http://www.oekonsult.eu/datensicherheit2008.pdf

ARGE Daten (2005): '"Wer ein Fremder ist, bestimme ich!" - Fremdenrechtspaket im Datenschutzrat' http://www2.argedaten.at/php/cms_monitor.php?question=PUB-TEXT-ARGEDATEN&search=84404ctc

APA/Futurezone (2011): November 15, http://futurezone.at/netzpolitik/5931-ministerrat-beschliesst-sicherheitspolizeigesetz.php

Austrian Federal Chancellery (2014): The Austrian security strategy. Security in a new decade - Shaping security. http://www.bka.gv.at/DocView.axd?CobId=52251

Austrian Federal Chancellery ("Bundeskanzleramt") (2012): National ICT strategy Austria. http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=48411

Austrian Federal Chancellery ("Bundeskanzleramt") (2009): Administration in Austria. http://www.bka.gv.at/DocView.axd?CobId=41629

Austrian Data Protection Commission (2014): Annual report 2012/2013, Vienna 2014. http://www.dsb.gv.at/DocView.axd?CobId=55304

Austrian Parliament (2001): *Security and Defence Doctrine*, Resolution by the Austrian Parliament, December 2001 http://www.bka.gv.at/DocView.axd?CobId=3604

Austrian research center for peace and conflict resolution ("Österreichisches Studienzentrum für Frieden und Konfliktlösung – ÖSFK") (2011): Stellungnahme zum Entwurf „Österreichische Sicherheitsstrategie. Sicherheit in einer neuen Dekade – Sicherheit gestalten". http://www.uni-klu.ac.at/frieden/downloads/Stellungnahme_sicherheitspolitische_Strategie_Bundesregierung.pdf

CJEU – Court of Justice of the European Union (2014): "The Court of Justice declares the Data Retention Directive to be invalid", PRESS RELEASE No 54/14, Luxembourg, 8 April 2014. http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

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

Data protection commission (2014): annual report for the years 2012/2013. https://www.dsb.gv.at/DocView.axd?CobId=55304

Der Standard Online (2013): '"NSA Villa" - Pilz: USA greifen auf Österreichs Luftraumüberwachung zu', November 15 2013 http://derstandard.at/1381372194814/NSA-Villa---Pilz-USA-greifen-Oesterreichs-Luftraumueberwachung-zu

Der Standard Online (2013): '"NSA Villa' in Wien wird geschlossen', September 10 2013, http://derstandard.at/1378248644840/NSA-Villa-in-Wien-wird-geschlossen

Der Standard Online (2012): "Verfassungsgericht prüft Vorratsdatenspeicherung", September 21 2012, http://derstandard.at/1347493199974/Verfassungsgericht-prueft-Vorratsdatenspeicherung

Der Standard Online (2011): '"Bundestrojaner" in Österreich nicht erlaubt aber im Einsatz?"', October 10 2011, http://derstandard.at/1317019787787/Bundestrojaner-in-Oesterreich-nicht-erlaubt-aber-im-Einsatz

Der Standard Online (2009): "Gewerkschaft hat Sicherheitsbedenken", September 6 2009, http://derstandard.at/1252036691580/Postler-zur-Polizei-Gewerkschaft-hat-Sicherheitsbedenken

Der Standard Online (2007): "Hintergrund: Überwachung in Österreich", December 6 2007, http://derstandard.at/3078169

DiePresse.com (2010): "Amtsmissbrauch: Steirischer Polizist verurteilt", March 2 2010, http://diepresse.com/home/panorama/oesterreich/543599/Amtsmissbrauch_Steirischer-Polizist-verurteilt

DiePresse.com (2009): "EKIS: Polizeisystem mit Spitzel-Vergangenheit", February 17 2009, http://diepresse.com/home/panorama/oesterreich/453338/EKIS_Polizeisystem-mit-SpitzelVergangenheit

European Commission (2012): Special Eurobarometer 383 on civil protection http://ec.europa.eu/public_opinion/archives/ebs/ebs_383_en.pdf

European Commission (2011): Special Eurobarometer 371 on internal security. http://ec.europa.eu/public_opinion/archives/ebs/ebs_371_en.pdf

Flori, N (2011): '„Gefährliche Waffe": Paragraph 278a' Wiener Zeitung February 11 2011, http://www.wienerzeitung.at/nachrichten/oesterreich/politik/28903_Gefaehrliche-Waffe-Paragraf-278a.html

Galetta, A, de Hert, P., L'Hoiry, X. and Norris, C. (2014): Mapping the Legal and Administrative Frameworks of Access Rights in Europe – A Cross-European Comparative Analysis. D5.1 of the IRISS project http://irissproject.eu/wp-content/uploads/2014/06/IRISS-WP5-Summary-Meta-Analyses-for-Press-Release.pdf

Jandl, G (2012): The challenges of cyber security – a government's perspective http://www.etc-graz.at/typo3/fileadmin/user_upload/ETC-Hauptseite/human_security/hs-perspectives/pdffiles/issue1_2012/6-HSP12_Jandl__FINAL_.pdf

Linsinger, E (2011): „Enormes Sicherheitsrisiko", Profil Online, February 12 2011 http://www.profil.at/articles/1106/560/288752/enormes-sicherheitsrisiko

Ministry of the Interior: "Informationen zum EKIS" http://www.bmi.gv.at/cms/BMI_Datenschutz/ekis/start.aspx

Medosch, A (2000): "Grundrechtlicher Super-GAU in Österreich kontaminiert die EU", Telepolis, October 25 2000 http://www.heise.de/tp/artikel/8/8992/1.html

Möchel, E (2012): "Datenschutz: Österreich stürzt ab", ORF Futurezone, December 30 2012 http://www.fuzo-archiv.at/artikel/246261v2

ORF (2014): "Vorratsdatenspeicherung: Ein Rest bleibt", June 28 2014 http://oe1.orf.at/artikel/380566

Privacy International (2007): Surveillance Monitor 2007 – International country rankings, https://www.privacyinternational.org/reports/surveillance-monitor-2007-international-country-rankings

Schmid, F (2014a): "Staatsanwaltschaft bricht Ermittlungen zur NSA-Affäre ab", Der Standard Online, Mai 28 2014 http://derstandard.at/2000001627044/Staatsanwaltschaft-bricht-Ermittlungen-zur-NSA-Affaere-ab

Schmid, F (2014b): 'Kooperation mit NSA laut Regierungsparteien „durchaus wichtig"', Der Standard Online, Juni 20 2014 http://derstandard.at/2000002176643/Nach-Besuch-in-USA-Kooperation-mit-NSA-laut-Regierungsparteien-durchaus

Schmid, F (2014c): 'Verfassungsschutz: "NSA könnte zum Nachteil Österreichs agieren"' Der Standard Online, Juni 25 2014 http://derstandard.at/2000002298526/Verfassungsschutz-NSA-koennte-zum-Nachteil-Oesterreichs-agieren

Schmid, F, & Sulzbacher, M (2014): "VfGH kippt Vorratsdatenspeicherung", Der Standard Online, June 27 2014 http://derstandard.at/2000002350932/Verfassungsgerichtshof-kippt-Vorratsdatenspeicherung http://orf.at/stories/2235721/2235722/

Seidl, C 2014, *Immer weniger Österreicher fürchten Terroranschläge*, Der Standard Online, viewed 18 Jan 2014 http://derstandard.at/1388514309607/Immer-weniger-Oesterreicher-fuerchten-Terroranschlaege

Statistics Austria, http://www.statistik.at/web_de/statistiken/bevoelkerung/

Statistics Austria (2014): "Bevölkerung im Jahresdurchschnitt" http://www.statistik.at/web_de/statistiken/bevoelkerung/bevoelkerungsstand_und_veraenderung/bevoelkerung_im_jahresdurchschnitt/index.html

Sterbik-Lamina, J & Birngruber, S (2014): Austria Country reports. In: Deliverable D5 of the IRISS project: Exercising democratic rights under surveillance regimes. Increasing resilience in surveillance societies (IRISS).

Stolzlechner, H (2004): "Einführung in das öffentliche Recht", Vol. 3, Vienna, 2004.

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.

Tálos, E & Kittel, B (2002): Austria in the 1990s: The Routine of Social Partnership in Question?, in: Berger, S. and Compston, H. (Eds): Policy Concertation and Social Partnership in Western Europe. Lessons for the 21st Century, New York, Oxford: Berghahn Books, pp. 35-50.

Virtual Data Protection Office („Virtuelles Datenschutzbüro") (2010): "Österreich: Rekordzahl von Stellungnahmen zur Vorratsdatenspeicherung" http://www.datenschutz.de/news/detail/?nid=4083 ;

WIKIPEDIA, "Wiener Neustädter Tierschützerprozess" https://de.wikipedia.org/wiki/Wiener_Neust%C3%A4dter_Tiersch%C3%BCtzerprozess

WIKIPEDIA, "Online-Durchsuchung Deutschland" https://de.wikipedia.org/wiki/Online-Durchsuchung_%28Deutschland%29

WIKIPEDIA, Data Retention Directive https://en.wikipedia.org/wiki/Data_Retention_Directive

Wimmer, B (2014): "Österreichische Vorratsdaten für Diebstahl und Drogen", Futurezone, June 11 2014 http://futurezone.at/netzpolitik/oesterreichische-vorratsdaten-fuer-diebstahl-und-drogen/69.898.233

Wimmer, B (2012): "Mehr als 80.000 Bürger protestieren", Futurezone, March 31 2012 http://futurezone.at/netzpolitik/8271-vorratsdaten-mehr-als-80-000-buerger-protestieren.php

Legal sources

Administrative Jurisdiction Amendment "Verwaltungsgerichtsbarkeits-Novelle (2012)" BGBl.I Nr. 60/2011 http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2012_I_51/BGBLA_2012_I_51.pdf

Austrian Parliament (2012): citizens' initiative to abolish the EU Directive 2006/24 / EC and to evaluate all terrorism laws http://www.parlament.gv.at/PAKT/VHG/XXIV/BI/BI_00037/index.shtml?forceShow=true#tab-Uebersicht

Austrian Parliament (2011):"Ministerialentwurf betreffend ein Bundesgesetz, mit dem das Telekommunikationsgesetz 2003, das KommAustria-Gesetz sowie das Verbraucherbehörden-Kooperationsgesetz geändert werden" http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00269/index.shtml

Austrian Parliament (2011): "Begutachtungsverfahren Ministerialentwurf betreffend ein Bundesgesetz, mit dem das Sicherheitspolizeigesetz, das Polizeikooperationsgesetz und das Bundesgesetz über die Einrichtung und Organisation des Bundesamtes zur Korruptionsprävention und Korruptionsbekämpfung geändert werden"

Austrian Parliament (2011): "Begutachtungsverfahren Ministerialentwurf" concerning a federal law with which the Security Police Act, the Police Cooperation Act and the Federal Law on the Establishment and Organization of the Federal Office for Prevention of Corruption and anti-corruption are changed http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00313/index.shtml

Austrian Parliament (2009): Bundesgesetz, mit dem das Datenschutzgesetz 2000 und das Sicherheitspolizeigesetz geändert werden (DSG-Novelle 2010), Bgbl. I N0. 133/2009 http://www.ris.bka.gv.at/Dokument.wxe?Abfrage=BgblAuth&Dokumentnummer=BGBLA_2009_I_133

Code of Criminal Procedure ("Strafprozessordnung") BGBl. No. 631/1975, as amended by BGBl. I No. 71/2014 http://www.jusline.at/Strafprozessordnung_%28StPO%29.html

European Parliament and the Council of Europe (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; http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Federal Act concerning the Protection of Personal Data (DSG 2000) BGBl. No. 165/1999, as amended by BGBl. I No. 135/2009 http://www.ris.bka.gv.at/Dokumente/Erv/ERV_1999_1_165/ERV_1999_1_165.pdf

Federal Constitutional Law („Bundes-Verfassungsgesetz" (B-VG)) BGBl. Nr. 1/1930 idF. BGBl. I Nr. 164/2013 http://www.jusline.at/116_B-VG.html

Registration Act - "Bundesgesetz über das polizeiliche Meldewesen (Meldegesetz 1991 - MeldeG) BGBl. No. 9/1992, as amended by BGBl. I No. 161/2013 https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10005799

Security Police Act ("Sicherheitspolizeigesetz") BGBl. No. 566/1991, as amended by BGBl. No. BGBl. I Nr. 44/2014 http://www.jusline.at/Sicherheitspolizeigesetz_%28SPG%29.html

Telecommunications Act 2003 ("Telekommunikationsgesetz") BGBl. I Nr. 70/2003, as amended by BGBl. I No. 44/2014 http://www.jusline.at/Telekommunikationsgesetz_%28TKG%29.html

All URLs lately checked on August 26 2014.

7 List of Figures

8 List of Abbreviations

Abbreviation	Definition
AK Vorrat	Arbeitskreis Vorratsdatenspeicherung ("Working Group on Data Retention")
CCTV	Closed circuit television
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CJEU	Court of Justice of the European Union
CRR	Central register of residents
DPA	Data protection authority
DPC	Data protection commission
DPI	Deep Packet Inspection
DPR	Data processing register
DSG	Datenschutzgesetz ("Data Protection Act")
EC	European Commission
EKIS	Elektronischen Kriminalpolizeilichen Informationssystem ("Electronic criminal police information system")
EU	European Union
FPÖ	Freiheitliche Partei Österreich ("Freedom party Austria")
ICT	Information and communication technology
IMSI	International Mobile Subscriber Identity
NATO	North Atlantic Treaty Organization
NGO	Non Governmental Organisation
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development
ÖSFK	Österreichisches Studienzentrum für Frieden und Konfliktlösung ("Austrian Study Centre for Peace and Conflict Resolution")
ÖVP	Österreichische Volkspartei ("People's party Austria")
SOST	Surveillance-oriented security technology
SPG	Sicherheitspolizeigesetz ("Security Police Act")
SPÖ	Sozialdemogratische Partei Österreich ("Social democratic party Austria ")
StGB	Strafgesetzbuch ("The criminal code")
StPO	Strafprozessordnung ("Code of criminal procedure")
TKG	Telekommunikationsgesetz ("Telecommunications Act")

9 Annex

9.1 Table recommendations

Template[84]

Recommendations – content[85]

What is the core statement of the table's recommendation?	What is the background of the recommendation?/what is the problem?	The recommendation in detail/What should be done/how to address the problem?
More investments in alternatives (non-technological)	Proportionality of resources/cost-benefit calculation (more harm than benefit)	More social balance
		Improving police work, involve citizens
		Support of social coherence/solidarity
		Analysis of the causes of crime
Creation of national agencies to scrutinize use of surveillance-oriented technologies and compliance with legal regulations	Use of SOSTs is opaque, responsible authorities are not known to the public	Public institution, with independent staff, publicly finances, public interface for requests, duty of disclosure with clear time limits
More focus on humans than on technology	Humans are social beings, security is inter alia perceived security, has to be in social context	Fostering police work, not merely penal force but as partner in security questions. Person in charge for local requests. Police has to develop according offers

[84] This recommendation sheet was filled in by each table. The translation of the template's questions, as well as the translations of the submitted recommendations, can be found bellow.

[85] Translated from German

Ongoing public debate on security technologies	Unclear definition of private sphere, no clear distinction between public and private. Privacy and security ethics is academic and lags behind technology	Creation of an ethical commission for surveillance technologies independent from security authorities, loyal to citizens, with public participation (citizens have to be involved in this commission)
Financial resources also for alternative concepts e.g. more police on the streets	Lack of information about privacy and security, already necessary in schools	DPI has to be dismissed absolutely and without any compromise
		More information and transparency,
		Education is the most important prevention against crime
Transparency for the citizens	Unrestricted data access	Mutual control of control units which have to be created
Control of surveillance institutions	Dependency from authorities that gather data	Access to one's own data
		Limitation of data surveillance
		Legal regulations, who is allowed to observe what and how
Transparency (What happens with our data?)	Mistrust to politics (and economy)	More honesty of politics
		More information to the citizens
		Awareness-raising for threats
		Sincere elucidation/information about all (gathered) data
Further developments should be liable to legal regulations and corresponding transparency	Lack of information	It is the job of elected representatives to implement this on behalf of the citizens (more liability and transparency)
Lack of information and reporting about planning and implementation of security measures	Anxiety about maldevelopment	More open to citizens' concerns
	Security technology must not become security hazard	Ensuring independency of controlling bodies for checks and balances
		Creating corresponding legal regulations
Politics should create legal framework to regulate SOSTs	Lack of information + lack of citizen inclusion	Citizens should be informed about security technologies in a comprehensive + objective way, which threats and benefits these technologies bring along; also for the youth (education in school)
Usage and "rules of the game" for SOSTs should be regulated	Today's decisions on usage of the technologies has unpredictable consequence for the future	Alternative security measures such as extension of police offices and strengthening of civil courage should be supported
For the elaboration of these laws, citizens should be involved		Usage of technologies should be dependent on the approbation of affected persons

in general we put the freedom of an individual above collective security if the danger exists that the latter will lead to a totalitarian surveillance state	the fear of a manipulative and illegitimate utilisation of collected and saved data	no implementation of DPI, only with legal limitations
		reinforce civil courage, peace policy, prevention of crime instead of surveillance
		guarantee of privacy for every citizen
		country specific security strategies and analysis
As legal regulations are considered rather ineffective, it is suggested to raise awareness and education of individuals	Individuals are left alone	Update of the EDV curriculum, e.g. benefit and risk of Facebook
contact point, board of trustees for internet security"	value of the individual is not respected	motivation of economy to protect privacy via reward and funding
inform the public in a transparent and understandable way about utilised data and its collection	Insecurity/obscurity about the usage and dissemination of one's personal data	participation of citizens for the purpose of transparency and retrieval of trust in politics
implement independent regulatory body, such as a parliamentary committee	fear of abuse malpractice	regulatory body should either be direct democratic via decision of the citizens through polling about the utilisation of surveillance information or a representative democracy with parliamentary committees/ministries for data
		independence of politics from economic interests
it is pointless using a sledgehammer to crack a nut (German idiom: pointless to shoot with cannons on sparrows)	privacy should not be subordinated to security	education, open/honest communication of the responsible parties - transparency
	it is pointless using a sledgehammer to crack a nut	Supervision by an independent European institution
		EU wide rules and standards + transnational
		differentiation of choice of technology and utilisation of alternative security concepts
		Participation of the people
Concrete information about technologies	Lacking trust in the public security apparatus	
Transparency for the people	division of the society - poverty endangerment	
Long-term investments into education programmes (preventive)	Misuse of data	
sustainable legislation processes for the formation of laws and investments (no quick shots)		

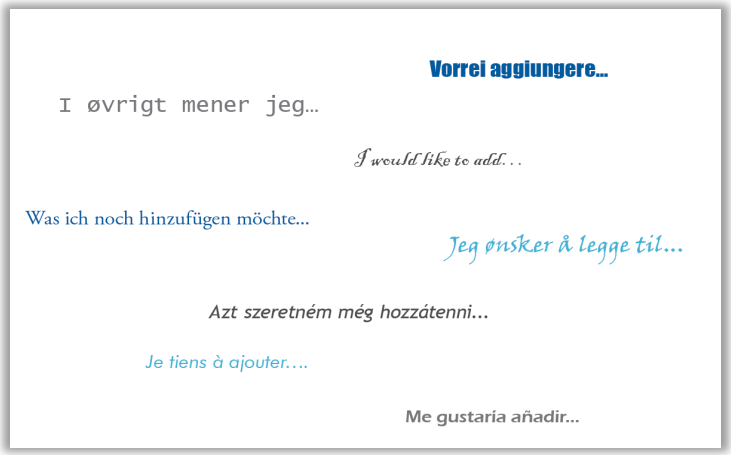
Improve, not extend existing surveillance	improve quality	Of security, police, supervisory, ethics commission
personal responsibility, encourage civil courage		regulations, that protect from misuse of surveillance technologies - EU wide, better worldwide
introduce a "day of data security", on which the topic is discussed and the citizens receive information	problem = strong interference of the surveillance technology into privacy	obligation of the authorities to transparency concerning the form and the intensity of surveillance + state of surveillance technologies
please surveillance only in sensitive areas and the decision makers should in general only have those areas surveilled, in which they would want to be surveilled themselves	big risk of misuse of data	prohibition of multiple use of surveillance data
complete information of the people - national referendum	little concrete benefit of constant surveillance	neutral commission to monitor the surveilling bodies
	too little political participation in type, form and intensity of surveillance	
privacy - secure - internet not possible	my home is my castle	surveillance technology part of national jurisdiction
		the misuse should be part of criminal law
		video surveillance should be restricted to public places
information and education about the used SOSTs	Clarification of the current state: What happens with the data? Who can use them? Where, who and how long are they stored?	information through the media: election campaign topics for the European elections in May 2014, objective Information from the EU commission, TV
		transparency about the users of the data
		stricter monitoring of the surveillance system by NGOs
detailed information to the public about the utilisation of already existing and future surveillance based technologies	legal regulation	regulatory body: administration + expert committees
	Monitoring and transparency regarding the utilisation of data as well as sanctions for misuse	
Laws and clear guidelines for data security have to be established	utilisation of data - respectively abuse of power	independent supervisory bodies are allowed to have insight into the data, they monitor each other respectively
		transparency for the citizens has to be factually given

"establish security" cannot be a contradiction to the respect for human rights	don't establish quantitative surveillance systems, but qualitative - not against citizens, but within the interest of society	education (especially for youth) about the risks of the monitoring system on the internet, e.g. in shape of documentaries on TV and in the media
information of the people	clarification and transparency have to be a precondition for the utilisation of surveillance systems	detailed clarification about the "authorities" that use the security systems and how they use it
increase transparency		regulation of the phrasing of the general terms and conditions on the internet (clarity), free virus scanner for everyone - develop tools for consumers and citizens for self-protection
		investments in research and technology for more targeted, not extensive surveillance/monitoring to protect against crime
		establish stronger monitoring systems for security authorities (against corruption and malpractice)
Principal departure from the tendency toward a surveillance state		protection of privacy
		improvement of privacy, reinforcement of the privacy lobby
		inclusion of the citizens
		protection of the privacy of correspondence (physical and digital)
		common EU wide performance (solidary)
		rejection of automatism
The law has to be transparent and complete (no gaps, no loopholes)	insecurity as regards the law (at the moment) lack of trust	more monitoring rights for a data protection authority
		publish reports
		enlighten people
better education for security staff and authorities, IT technicians and youth	too little sensitivity, e.g. youth, security staff is paid and trained poorly, IT technicians and authorities do not cooperate enough	better collaboration between the authorities
		education takes place in schools, but it is not taken seriously
		more presence of the security personal (should be paid better) on the spot instead of cameras - serve as deterrent
		quality control during training
We want more and regular info campaigns by the government during the implementation of SOSTs	too little information from the government	regular info campaign by the government

more transparency	too little transparency at the moment	more education and approaches towards transparency
a regulatory body/council in the surveillance institutions	unclear, who has access to the data and for which period of time	reinforcement of alternative surveillance methods without technology
strengthen judicial power no further restrictions in the domain of human rights for example	no current qualified politicians that can change something, "old values" of the current politicians don't exist	new, good, trustworthy politicians, that "guide the population accordingly" and address all the relevant problems (e.g. among others topics like CCTV, security,…) step by step
transparency	First-hand control/scrutiny of surveillance	duty of disclosure of the authorities to inform the citizens. monitoring with a supervisory authority
training of experts	especially officials for implementation and raising awareness in schools	training as well as brochures with information material and further training obligations for teachers
alternatives with democratic control	conflict between privacy and security	more incorporation through science
		more support for civil courage and personal responsibility
		reinforcement of social points of contact (new e.g.: caretakers/janitors, meetings of residents, etc.)
more transparency for the population	insecurity about the transfer and usage of personal data	objectivity, illustration of advantages and disadvantages
	too little information	set an example of the European idea
	misinformation, fear	professionals should devote themselves to the topic "creation of transparency"
		put the European idea before national interests of the member countries, serving it and the citizens
establishment of a legal framework, so that information, transparency and supervision are possible for the users	insufficient legal regulations	national and international laws, coherent regulations for the better protection of privacy and the utilisation of data
	no transparency	information about data storage and utilisation
	No possibility for internet users to control	legally binding disclosure to inform users about data processing (also about demanded deletion of data)
	Lack of sincerity of politicians	deletion of data after a certain time frame
		possibilities for encryption

9.2 Postcards

Template



Postcards - content[86]

What I would like to add…to the European politicians
Use of surveillance technologies essentially only for concrete suspicion against organisations as well as private persons
No haphazard use of surveillance technologies
No dubious support without control
Criminality from the east
uncontrolled finance transactions
Appropriate combat
Let national states their national laws
Citizens as chance – transparency and participation instead of surveillance
Hopefully politics will finally become more open, informative and honest!
More citizen participation in advance!

[86] Translated from German

More human resources, less technology!
Please do not take citizens for a fool! The discontent in the population is already big enough!
Lack of information about surveillance systems – more transparency is required!
Listen to your voters, look at your people
More police respectively security guards for protection in public buildings/areas
Only improve and not extend camera systems
More focus on non technological alternatives
Setup of an own/European internet infrastructure!
Do something
signs on public smart CCTV cameras – who operates them and who can access the data
Please involve the citizens more
Create more transparency
Create explicit information
more severe punishments for sexual offenders, child abusers and criminals
Ban of child porn webpages and nude pictures of children (no border zones!) EU wide! Monitoring of access on other providers - very harsh punishments (imprisonment)
develop other options than total surveillance for the safety of the citizens and the fight against crime
in general children need to be far more protected by more severe and harsh punishments for indecent assaults against them
reopen the borders
More supervision
no shutting down of police stations
The state politicians have to make use of all possible measurements to protect and increase the privacy of each individual, which implies giving priority to people not to the economic benefit.
No further increase of surveillance technologies
competent, trained and moral staff
Less money should be spent on security technologies. Money for unemployment, for the economy, youth, environment
Before money is spent on big projects, the consideration period for grants (EUR) within the parliament should be prolonged in order to make reasonable decisions. Furthermore there should be more attention for alternatives and not only those, that are formulated/provided
A safety problem arises from totalitarian groups trying to win over followers with heavenly seeming promises. We should not forget that Hitler seized power in a democratic way and what the consequences were. There is an urgent need for increased vigilance from the state on this topic. The freedom of religion is often misused by those groups to suppress human rights.
If Austrians use social networks, e.g. Facebook, the data protection laws of Austria have to be effective!
More police men on the streets, also non-uniformed
Cameras can't prevent crime the crime only relocates somewhere else!
I don't want to be a transparent human being!
permission of car cameras
more transparency and information for EU citizens

Reinforcement of alternative safety measurements with consideration of costs
creation of a regulatory authority that is trustworthy for citizens
already among pupils, personal responsibility should be fostered - information material
transparency at disclosure for me about my personal data and how it is used by others
“Fonds Soziales”, social responsibility as alternative
Reclose the borders!
More police supervision!
Establishment of one or several regulatory bodies with mutual control - see checks and balances
for the inspection of the data - access to it is apparently not verifiable
access of the "citizens" to their own data or to the files about them
Communicate safety issues about smartphone internet usage more! Inter alia restrict the access of apps respectively enable people to determine by themselves
Possible data transfer and information about one’s whereabouts (or other) threatens the safety of the individual. Even if such data is not passed on at the moment, we don't know what will happen in future generations.
We need clear guidelines respectively regulations, so that the citizens keep their rights (EU fundamental rights).
We shouldn't model ourselves on the United States.
We are against the "transparent” (“gläsernen”) human beings
Explicitly higher minimum sentences for consumers of child pornography!
No data retention!
More police presence, also on the internet, instead of complete electronic surveillance.
Protection of civil rights and privacy
less data misuse
Protection of citizen data
Stemming and stopping lobbyism!
develop alternative concepts instead of technological surveillance
More involvement of science
strengthen the judiciary - introduce a data protection council independent, something like a public ombudsman that the citizens can contact
that security technologies are used for combating crime and not for surveillance of the "little” respectable civilian
humanity - back to handshake quality
no data retention
A recommendation to the policy is very difficult at the moment, as in my opinion there are currently no thoroughbred politicians that have assertiveness.
No longer restricting fundamental rights towards technology
strengthen justice
High demand of honesty!
Informing and disclosure about collected data!
Put more focus on the positive side of humans, don't fuel fear and polarities.

More closeness to citizens, transparency, positive informing.
Encourage more personal responsibility, competence, autonomy than knowledge that is barely used in schools.
Invest less in technological progress and more in the people
Human kindness, solidarity, awareness!
Protect the environment, sustainability, love in everyday life
Stronger integration of NGOs and interest groups into decision making processes (as experts)
Establish civic bodies that consist of security authorities, computer specialists, ordinary citizens, … (participatory democracy)
Ethics committee
Establish a commission with e.g. 20% citizens
Poll on video surveillance (where?)
More information, labelling of (who supervises what?) of video surveillance!
Who has access to which data?
Make the topics part of general knowledge e.g. integrate them in ethics classes in schools
More transparency - population should be informed - clear exposition
DPI should be better structured in who is responsible for it and up to which point it is monitored
More information
Regular referendums (approx. 20-30 years) if and how the technologies should be used
See the citizens as dignified and not as tax payers!
Truth!
Under all circumstances guard the border (or close them altogether) to reduce crime. That would be more important than internet and video surveillance or position all videos at the borders.
Burglary and mugging are increasing and not bearable anymore. Urgent!
Not the technologies are the problematic thing about surveillance systems, but the supervisors.
The heads of surveillance systems are often psychiatric and criminal people. Here lies the problem - can only be solved by politics – watch the watchers!
The possibilities of technology cannot be stopped and not be foreseen in their further development. Someone will use them for some purpose. Governments will not be able to escape using them.
Politicians should ensure satisfaction among the population; that also implies a better education system!
Please use the money that is invested into surveillance technologies for other things! Orphanages, green areas, social events, look after homeless people
The legal framework should be changed in that regard that cybercrime is also punished with more severe sentences. I think that we can hardly take control of technology in that regard, the clever will always find ways to outsmart the technologies.
Information should already be disseminated in schools because the youth already ends up in the clutches of technology companies without realising it.
Alternative options, as existed before the technologies should be used again.
EU wide funding and research, development of technology
Create a legal framework Consequences in case of misuse!
Act in the interest of society (not in personal economic interest!)

Education for the population about the dangers and possibilities of the internet
Differentiate/create borders between surveillance and privacy!
Reduce bureaucracy!
Prevent corruption!
Create better "frameworks" for internet users to prevent cybercrime.
European protection of children and youth from "evil websites"
It is by no means the right way to rely on total surveillance
Alternatives such as e.g. more police on the streets and especially in areas, where a certain high crime is prevalent instead of putting cameras into every corner, it would be smarter and the population would probably feel more at ease too
Protect humans (not only the economy!)
Information about the advantages and disadvantages of security surveillance in public space (media)
Information about the disadvantages regarding security on the internet, especially youth who are very careless (school, media)
Better protection of personal data! Embedded in laws Stemming abuse
In order to inform the population, show the movies about it repeatedly on ORF at an airtime, where most people are still awake!
A lot of people don't know what is technically possible nowadays!
Establish legal frameworks that protect us from the misuse of our data!
Politicians should have the public good of the population at heart and not the good of big corporations! Don't let the corporations blackmail e.g. with job loss, loss of taxes etc.
These systems undermine our natural trust but expect that we have trust in their suspicious activities
Please establish a new regulatory body for new technologies.
There have to be experts that deal with the opinions of the population and provide more safety.
In case of violations there have to be consequences.
Ignorance causes fear!
It will be very difficult but inevitable to try everything to inform broad segments of the population about the functioning and the operating range of surveillance technology. With positive and negative examples - also in order to be credible
The most severe national + international tracing of malpractice!
I strongly wish for more, better, regular info campaigns that unveil the different points of view - also already in school
If used at all, SOSTs should be used very carefully
Data should not be stored at all or only for 24 hours and especially surveillance institutions should be supervised by independent, elected panels of experts
In general I reject Smart CCTV or DPI and would advocate the reinforcement of alternative surveillance methods without technology e.g.: neighbourhood organisations or incognito security guards, that don't record/store data
Funding also for farmer with small stretches of Land (300 m2) e.g.: to maintain little environmental meadows with scattered fruit trees. Fostering of bees through afforestation of suitable tree species (Maple, linden, locust, blackthorn, Cornelian cherry, apple (old species = take out from the authorization of the species)
Providers have to guarantee internet security (product liability)