*"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 6.3 – Citizen Summits on Privacy, Security and Surveillance: Country report Germany

Lead Beneficiary: ULD

Author(s): Eva Schlehahn (ULD)

Due Date: June 2014

Submission Date: September 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 /<br>Österreichische Akademie der Wissenschaften<br>Coordinator, Austria | ITA/OEAW |
| Agencia de Protección de Datos de la Comunidad de Madrid*, Spain | APDCM |
| Instituto de Politicas y Bienes Publicos/<br>Agencia Estatal Consejo Superior de Investigaciones Científicas, Spain | CSIC |
| Teknologirådet -<br>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 -<br>The Norwegian Board of Technology, Norway | NBT |
| The Open University, United Kingdom | OU |
| TA-SWISS /<br>Akademien der Wissenschaften Schweiz, Switzerland | TA-SWISS |
| Unabhängiges Landeszentrum für Datenschutz, Germany | ULD |

This document may be freely used and distributed, provided that the document itself is not modified or shortened, that full authorship credit is given, and that these terms of use are not removed but included with every copy. The SurPRISE partners shall all take no liability for the completeness, correctness or fitness for use. This document may be subject to updates, amendments and additions by the SurPRISE consortium. Please, address questions and comments to: feedback@surprise-project.eu

*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 deliverable presents the results of the SurPRISE citizen summit on privacy, security and surveillance conducted in March 2014 in Kiel, North Germany. During this event, the views and opinions of the participating citizens regarding privacy, security, and specifically pre-selected, exemplary surveillance-oriented security technologies (hereinafter: SOSTs) were explored.

The purpose of this citizen summit was to gain insight the participant's opinions about these topics to examine impact and concerns relating to security policies and practices within the EU from European citizen's perspective. The goal is to create valuable research information for stakeholders entrusted with shaping the future security strategy in Europe and its correlating policies. Together with other work of the SurPRISE-project, the summit results can enlighten European policy makers which issues must indispensably be taken into account. In particular, this concerns the preconditions under which the use of SOSTs is accepted by citizens including the most significant obstacles connected to fundamental human rights and democratic principles in Europe.

Oftentimes, the relationship between privacy and security is seen as a necessary trade-off in order to achieve enhanced security. This perspective has influenced legislative and best practice activities strongly over the last years. Nevertheless, public discussion, especially triggered by the NSA revelations recently, implies that the classical trade-off model falls short as an overly simplified view on the relationship between privacy and security. It became apparent that despite proposed security achievements, privacy and more general human rights concerns play an important role in security-policy related public discourse across Europe. These concerns suggest that the issue at hand is more complex than the simple assumption of European citizens agreeing to unconditional exchange of their own privacy with security benefits.

The SurPRISE-project addressed these concerns in response to the aforementioned development by conducting citizen summits in nine different countries from the EU and associated states. With averagely 200 citizens participating per country, the citizen summits were aimed at investigating the view of citizens on the security-privacy trade-off while they are evaluating pre-selected SOSTs. At the German citizen summit, the citizens had the chance to express their opinion about the two selected SOSTs Smart CCTV and Smartphone Location Tracking (hereinafter: SLT). This deliverable presents the results for the citizen summit in Germany on national level.

In this document, the results are at first set into the national context in Germany in chapter 2. Thereby, the current situation as developed from the country's historic background is explored. Nowadays, the German state is a parliamentarian democracy. But still, the country is sustainably influenced by events of

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

the past under the repressive regimes of the national-socialists under Hitler and the German Democratic Republic (GDR) which formed after the division of the German territory by the occupation powers in the wake of World War II. The experience of these oppressive states and the societal decomposition caused by intensive spying activities of the Nazi secret police and the GDR "Staatssicherheitsdienst" (Stasi, translated: State Security) has left a deep mistrust in German citizens towards governmental surveillance for security purposes. This mistrust has diminished after the 9/11 terrorist attack and follow-up events. But it noticeably returned to the attention of the public and seeped into controversial media discourse after the revelations of whistle-blower Edward Snowden about the spying activities of the U.S. National Security Agency (NSA). This is the situation providing the setting for the following sections describing Germany's major security policies and strategies as well as correlating privacy issues, the public discourse on SOSTs and the related practices.

With this contextual information as background, the German citizen summit was conducted in March 2014 in Kiel in northern Germany. The event organization is described in detail under chapter 3 (Process design – the citizen summit in Germany) including the organizational setting, the structure of the citizen panel, and the perception of citizens regarding the summit in which they participated.

Chapter 4 provides the factual empirical results of the citizen summit. Its structure provides at first the citizen's general attitudes on privacy and security, followed by the more SOST-related opinions of the summit participants. Overall, the citizens took a very critical stance towards SOSTs. Citizens expressed strong concerns about surveillance-focused technologies being used to improve national security. The main reason given for these concerns is that SOSTs are generally perceived as invading the privacy of individuals as well as eroding the concept of privacy as such. Thereby, it became clear that citizens have strong doubts about the effectiveness of surveillance-oriented security technologies for purposes of improving national security. Citizens criticized the lack of reliable and objective evaluation of SOST deployment and said they do not automatically feel more secure when these technologies are employed. For surveillance-oriented security technologies in general, citizens said that they feel exposed to these surveillance tools while the broadness of such surveillance-focused measures was criticized strongly. The citizens think many SOSTs may under circumstances reveal sensible, even intimate information about innocent individuals on a broad scale. Throughout the whole day, citizens expressed severe worry about the perceived ever-increasing surveillance in all aspects of their lives and complained about the subtle progression of modern society into a panopticon setting. Many citizens admitted that once they are aware of surveillance conducted upon them, they feel a chilling effect on their own behaviour. However, citizens also showed a very multi-layered view at the summit event, acknowledging SOSTs as such as in principle being neutral tools which could beneficial for security issues. Still, citizens perceive these technologies as being quite prone to misuse by deploying security authorities as well as by unauthorized third parties.

As a result to this risk perception, a fairly large number of participants said they would actively resist SOSTs because they feel very uncomfortable with the feeling of being surveilled in general. Moreover, in the group discussions, Citizens admitted additional insecurity caused not only by governmental surveillance, but also due to widespread data collection by private companies for profit purposes. This seems to have a significant impact especially on elderly citizens who feel overburdened by the complexity of modern technologies. Owing to these insecurities, some citizens at the summit said that they avoid using such technologies, like mobile phones, computers, etc. completely.

With regard to collective or personal aspects, participants explicitly said the German government is obliged to protect the privacy and democratic freedoms of the country's citizens besides guaranteeing public security, too. Citizens complained that from their point of view, oftentimes security goals would be given too much priority from the governmental institution. They criticized that this would be a too one-sided focus going along with a very strong faith in technology as solution to security issues. As a consequence, citizens feel some uneasiness on personal level when it comes to governmental surveillance. However, this uneasiness does not entirely seem to be restricted to mere personal concernedness. Rather, the broader societal impact of SOST usage by governments causes significant concerns too, especially regarding potential negative effects on human rights and democratic principles. Aspects mentioned by the citizens were the fear of governmental blanket suspicion towards citizens and resulting big-brother-like mission creep for security purposes. Regarding technology-specific aspects, citizens pointed out the misuse risks which ultimately may lead to factual discrimination of certain groups within the population, especially minorities. Also, the abuse of surveillance technologies for political purposes was mentioned several times, repeatedly with references made to the Arab Spring. Citizens pointed out that while Germany nowadays has a democratic state order, this might not always be the condition to live under for German citizens. Based on the historic experiences of the German population with repressive regimes, the participants of the summit highlighted this issue as being a severe risk of SOSTs. Even without a direct and intentional abuse of surveillance information, citizens highlighted the risk of an increasing, but yet subtle undermining of the constitutionally guaranteed presumption of innocence. Ultimately, it can be said that the citizen's opinions emphasized that the gradual erosion of privacy on both levels, personal as societal, creates and fosters deep mistrust in the governmental use of SOSTs.

This mistrust in current governmental security policies and activities also became apparent once citizens had a chance to voice their opinions regarding the trustworthiness of security authorities in general. This trustworthiness linked to the benevolence and the competence of governmental security authorities was doubted by the majority of citizens present at the summit event. Focusing on the addressed SOSTs, the trust in government in percentages was slightly higher regarding the use of Smart CCTV compared to the use of SLT. But still, the percentages indicating trust in the use of these SOSTs was not very high overall. Again, citizens emphasized the intrusiveness of these SOSTs and their misuse potential while during the group discussions, they argued that the low level of trust is mainly rooted in a strongly perceived and sorely felt lack of transparency from governmental side. This insufficient transparency would lead to insecurity about the legal and factual conditions of SOST usage as well as about the purposes. The mentions of the NSA revelations and the misuse of surveillance during the Arab Spring show that citizens feel this insecurity even stronger once foreign security agency are involved. Therefore, the majority of citizens said they would support a shift further away from technology-reliant security solutions involving more human factor and giving room to alternative approaches which in their opinion deserve higher priority. Regarding still necessary technological security solutions, they demanded a clearer and more universal legal framework with efficient means of enforcement.

At the end of the citizen summit, the participants had the opportunity to formulate recommendations to address security policy makers on European as well as national level. With these recommendations, citizens in principle acknowledge that SOSTS could be necessary under specific circumstances to investigate or even prevent crime. Still, the recommendations also reflect the citizen's strong concerns regarding the broadness of currently deployed and foreseeably planned measures going along with vast data collections and negative effects on privacy as well as other human rights. Therefore, the majority of the citizens took the chance to make concrete suggestions with their recommendations. These suggestions cover a wide range of possibilities how the aforementioned critical issues could be addressed in their opinion. These are:

- Increased transparency about SOST usage, purposes and treatment of data collected
- Appropriate and meaningful evaluation of SOSTs on the basis of objective research
- Oversight and control of SOST-deploying security authorities
- Privacy by Design approaches for the specific SOSTs where possible to reduce misuse risks
- Transparency, oversight and control should be realized with suitable, necessary, and effective measures on organizational, technical and legal level

Especially with regard to the involvement of foreign security agencies, the recommendations entailed a demand for a universal and supra-national legal framework at least on European level which is easily enforceable for the average European citizen. The recommendation texts made clear that this counts not only for the governmental deployment of technology, but also for the private sector to ensure a better protection of citizen's privacy while strengthening citizen rights in general. Citizens also supported the idea of less surveillance in general, with a stronger focus on alternative approaches. Examples mentioned for such alternative approaches were:

- Investment in more police staff
- Political and factual solutions to reduce poverty and other types of social inequality
- Non-technological crime prevention approaches like social programs
- More education
- Further possibilities suitable to resolve security issues which could be researched/investigated

In the end, it can be said that while the summit event had a clearly critical group of participating citizens, they strived for a quite multi-layered view on the topics discussed. Thereby, they examined arguments pro and contra SOSTs in earnest, taking into account the need of a free and democratic state to guarantee its inhabitants a suitable degree of security. However, the perceived negative effects of surveillance on individual as well as societal level worry German citizens to a great deal. So it can be said that the often cited security-privacy trade-off simplifies the issues at hand since surveillance for security purposes is also a factor of insecurity to many citizens. Moreover, this model fails to do the complex realities evolving around security matters and measures justice. Consequently a balance between privacy and security has to be struck instead of simply choosing between two excluding options. This finding correlates with the views the citizens expressed throughout this summit and their voiced expectation of German and European security policy makers taking action to balance out security and privacy. In their opinion, this effort is crucial to effectively preserve the achievements of the modern European society with regard to democratic freedoms and human rights of European citizens.

# 1 Introduction

This document is the output of the results deriving from the German citizen summit conducted for the EU-funded research project SurPRISE in Kiel in March 2014. This citizen summit was meant to investigate the opinions of citizens regarding privacy and security, involving specifically surveillance-oriented security technologies (SOSTs) as tangible examples. Citizen summits were conducted in nine different countries with averagely 200 citizens participating per country. Thereby, the overall realisation of the actual events followed a pre-defined and standardized schema to guarantee the international comparability of the results. Those results are analysed and presented in the nine individual reports per country as well as in one follow-up synthesis report on European level.

The analysis entails qualitative as well as quantitative elements on the basis of the opinions given by the citizens who participated in the summit. The goal of the analysis is to create an overview of citizen's stance regarding the topics addressed and to extract useful information for future policy papers and manuals. These documents are meant to ultimately provide European stakeholders entrusted with security policy making a source of sound research information. The empirical research done in the project is intended to complement the theoretical considerations and may provide European policy makers some valuable input to better understand the relations between privacy, security and surveillance. Factors of non-acceptability of SOSTs and the according security policy do not least depend on which crucial issues to take into account with regard to fundamental human rights and democratic core principles in Europe.

# 2 Privacy, security and surveillance in the national context

## 2.1 Country profile of Germany

Germany is a country consisting of 16 federated states located in central Europe. With a population of approximately 80 million inhabitants, it has nine neighbour countries and direct connection to the North Sea and the Baltic Sea. The initial foundations of its democratic state form were developed during the Weimar Republic from 1919 on, when the imperial government form was superseded by a new federal republic and semi presidential representative democracy. However, this first form of democratic community was not stable throughout its history, but rather transformed itself into dictatorship after the seizure of state power by the national-socialists in 1933. This episode was marked by the oppression of regime adversaries as well as the intentionally systematic annihilation of Jews, now called the Holocaust. Furthermore, Germany's aggressive expansion politics towards other countries was an element leading up to the start of the World War II.

After the unconditional capitulation of the Wehrmacht on May 8th 1945, the four victorious powers USA, Great Britain, France and the Soviet Union divided the German territory into one eastern and three western occupation zones. During the post-war area, the three western zones were transformed into what is known as the Federal Republic of Germany within the borders before 1986, while the eastern part of the country and part of Berlin in the Soviet occupation zone were declared as German Democratic Republic (GDR; German: Deutsche Demokratische Republik, DDR). However, the latter developed as a factual dictatorship dominated by the Socialist Unity Party (German: Sozialistische Einheitspartei, SED). The division of the country was manifested through military power of the Soviet Union and since 1961 with the construction of the so-called Berlin Wall. After the peaceful revolution in the GDR, the SED dictatorship was ended, leading up to the German re-union in October 1990.

Today in Germany, the state is a parliamentarian democracy consisting of federal, provincial and municipal entities. The representative head of the state on federal level is the Federal President (German: Bundespräsident), while the head of the government as central executive authority is the Federal Chancellor (German: Bundeskanzler). The state institutions follow the principle of the divided state powers of executive, judicative, and legislative whereas the legislative entities consist of the Bundestag, a constitutional parliament body whose members are elected directly by the citizens, and of the Bundesrat, which represents the 16 federal states of Germany at the national level which partakes in legislative acts of the Bundestag. The governmental administration is the Federal government (Bundesregierung), consisting of the chancellor and the ministers assigned in different areas. The 16 federal states ("Länder") have partial sovereignty with their own legitimacy and competences in specified areas and with own elections from parties on Länder level. In these areas, the Länder also have their own constitutions and their own correlating political institutions deriving from the principle of the divided separated state powers. The judicial power on federal level is represented by the German Federal Constitutional Court (Bundesverfassungsgericht), which has formed and interpreted the German Constitution, particularly the fundamental rights through a large number of decisions. Besides the Bundesverfassungsgericht, the judicial system in general has different branches with diverging subject areas. Five different areas are to be distinguished: Jurisdiction on ordinary civil and criminal matters, administrative jurisdiction, labour jurisdiction, social jurisdiction, and finally, the financial jurisdiction. Furthermore, the jurisdiction is separated on federal as on Länder level. As for the hierarchy of the courts, the legal process may lead through maximal three court instances: The first instance, the court of appeal, and the revision instance. Against the final instance decisions, a constitutional complaint before the Bundesverfassungsgericht is possible. However, the German Federal Constitutional Court is not to be understood as kind of a super revision instance. Rather, a complaint can only be successful if a court decision of a former instance violates constitutionally guaranteed and fundamental rights of the citizen.

From the beginning of the European integration process in 1951, Germany was one of the founding nations of the European Union. The political culture is lively, involving various political parties with a broad range from right to left, economic stakeholders from labour and industry, and with a strong influence of trade and labour unions. Other interest groups partake in public policy discussions as well, such as consumer protection associations and other non-profit organisations.

## 2.2 Major security policy and strategies

The security structure in Germany is generally determined by a strict separation of police and intelligence agencies. This perspective was over times inherently shaped by Germany's historic experience of the aforementioned repressive regimes during national-socialist and post-war GDR eras. To avoid the experienced dangers of centralised governmental power, the separation of governmental authorities was developed in hope to ensure a better protection of citizen's constitutionally guaranteed rights and freedoms. Thereby, governmental intelligence services are restricted within the scope of certain principles, such as only existential state security being allowed as main ground for pre-emptive measures and without being equipped with police powers. As for the law enforcement institutions, these have an obligation to focus more on individual targeting of criminals instead of dragnet activity. This shall be done with a primary focus on the maintenance of public security. Public security as the main focus is thereby defined as *"the inviolability of the legal system, the subjective rights and legal assets of the individual as well as the institutions and events of the state or other inhabitants of public governance"*.[2] While being limited to these principles, governmental entities are also bound to the specific laws applicable and the requirement of proportionality. Furthermore the jurisprudence of the German Federal Constitutional Court oversees the legislative grounds to which the governmental institutions are bound.

Due to Germany's experience with significant security matters, such as terroristic activities coming from all areas of the political spectrum[3], the competences of investigation and law enforcement bodies have been expanded more and more over the years while in principle, still the division of intelligence and police is existent. This development even intensified after the terrorist attacks of 9/11 and Madrid, leading to an extension of intelligence activity in various areas. Germany has three federal intelligence agencies. The first is the Bundesnachrichtendienst (BND, translated Federal Intelligence Service). The BND is the only intelligence agency concerned with foreign intelligence activities to obtain relevant insight to security and international affairs matters. Second, the Militärischer Abschirmdienst (MAD, translated Military Counter-Intelligence Agency), is the intelligence agency of the German armed forces, tasked with constitution protection in this context and the support of the military intelligence. Third, the Bundesamt für Verfassungsschutz (BfV, translated Federal Domestic Intelligence Service for the protection of the constitution) is a country-internal intelligence service mainly concerned with intelligence activities to investigate aspirations against Germany's free and democratic basic order. In this context, the BfV is obliged to take care of left- and right-wing extremism, counter-espionage, foreign extremism, Islamic terror and the observation of sects like Scientology. The intelligence agencies have no police powers. The executive law enforcement structures in Germany are to a large extent a task of the Länder, which have their own police laws. However, there are some police institutions on federal level, such as the Federal Criminal Police Office (German: Bundeskriminalamt, BKA) which is tasked with the national severe crime investigation, the coordination of information together with the police institutions of the Länder, and crime investigations with relations to foreign nations. While in general, the aforementioned intelligence services have duties for pre-emptive intelligence for national security, only the police forces have executive powers like for arrests or searches and may take action for general risk prevention. In principle, there is a division in power and separation of data bases between the police institutions of federal and national level, there is an on-going trend towards greater exchange and cooperation, nonetheless due to the events of 9/11. The expansion of the international European market has brought free movement of citizens and free traffic of goods, capital and services. But these freedoms come along with risks to the inner state security having an influence on the current security policies and strategies in Germany. Focal points of these security policies and strategies are mainly counter-terrorism

[2] So in the local law of several federal states like the Bremen police law, § 2 Nr. 2 BremPolG (original in German): "...die Unverletzlichkeit der Rechtsordnung, der subjektive Rechte und Rechtsgüter des Einzelnen sowie der Einrichtungen und Veranstaltungen des Staates oder sonstiger Träger der Hoheitsgewalt".

[3] For example, those of the left-wing extremist group RAF (Rote Armee Fraktion, translated: Red Army Faction) and the right-wing extremist group NSU (Nationalsozialistischer Untergrund, translated: National socialistic Underground).

and right-wing extremism and illegal immigration. Furthermore, the fight against organized crime is a crucial responsibility for German security agencies. This entails security foci like human trafficking, drug trading, money laundering, counterfeiting, and cybercrime.[4] Due to the terrorist attacks of 9/11 and follow-ups, an emphasis developed on pre-emptive measures specifically at high-risk events like demonstrations, larger sports, or cultural happenings. Several specific data bases and centres for defence in the fields of counter-terrorism and right-wing extremism were created as well.[5] Thereby, the counter-terrorism data base can be accessed by 38 German security bodies and was subject of a lawsuit brought before the German Federal Constitutional Court with claim of the division principle relating to police and intelligence being violated. In April 2013, the court in general accepted the existence of such a data base, but objected to parts of the rules laid down for it. The ruling tasked the German government with the amendment of the criticised parts until 2015.[6]

Beyond this ruling, the cooperation and operation structures of law enforcement and intelligence bodies within the German government was and still is subject of political processes in the context of the investigation around the right-wing extremist group NSU (Nationalsozialistischer Untergrund, translated: National-Socialistic Underground). This group is accused of murder series during the year 2000-2006 and other deadly crimes targeting citizens of different ethnic origin.[7] However, questionable activities of the police, several Domestic Intelligence Services for the Protection of the Constitution (German: Verfassungsschutzämter), and the authority for the military counter-espionage (German: Militärischer Abschirmdienst, MAD), led to severe disruptions on political level, resulting in the resignation of diverse chief executives in the Offices for the Protection of the Constitution on national and federal level. As a consequence of repeated failures during the governmental activities and the interlaced cooperation of police and intelligence in contrast to the general rule of division, a specifically assigned committee of inquiry of the German Bundestag was tasked with the investigation of the events in January 2012 and provided a concluding report in August 2013.[8] Also, due to the failures and eventual involvement of confidential informants (German: V-Leute), fundamental reforms of the Offices for the Protection of the Constitution were demanded, including a stronger connection between the governmental bodies and the sharing of investigation data.[9] The political discourse about these reforms is still an on-going process.

Moreover, cyber security threats were addressed by the establishment of a National Cyber Defence Centre in 2011.[10] The institution Bundeskriminalamt (translated: Federal Criminal Police Office), functions as a central information collection point, and the local police authorities on federal level execute the factual crime prevention and investigation powers.

As for surveillance-related technologies in Germany, their deployment is strictly bound to purposes as pre-defined by the law. Especially regarding pre-emptive measures for hazard aversion may only occur once a specific danger situation must be assumed to avoid the surveillance of citizens without tangible suspicion. Technical security measures deployed by German security bodies are for example cell tower records, Silent SMS (aka Stealth Ping), body scanners at airports, CCTV in public spaces and the usage of social networks in different ways. Also in the digital sphere, governmental institutions made use of the so called "Federal Trojan" (German: Staatstrojaner), which is a Trojan horse application excelling remote control or backdoor functionalities on an infected target device. In 2011, the German Chaos Computer

[4] Bundeszentrale für politische Bildung (Federal Centre for political education), article by Thorsten Müller published June 14th 2012, "Innere Sicherheit in der Europäischen Union"; Zeit Online article published January 14th 2014, " De Maizière sieht Deutschland gleich mehrfach bedroht".

[5] Spiegel Online, September 5th 2006, "Germany Agrees on Anti-Terror Database"; Searchlight magazine blog article by Key-Alexander Scholz, July 7th 2012, "Germany to tackle neo-Nazis with database".

[6] Decision of the German Federal Constitutional Court of April 24th 2013, (Az.: 1 BvR 1215/07).

[7] Die Welt, article of November 13th, "Friedrich spricht erstmals von "Rechtsterrorismus".

[8] For further information, see the decision recommendation and report of the 2nd NSU committee of inquiry to be found on the website of the German Bundestag (PDF-file). Printing matter 17/14600 August 22nd 2013, "Beschlussempfehlung und Bericht des 2. Untersuchungsausschuss es nach Artikel 44 des Grundgesetzes": http://dipbt.bundestag.de/dip21/btd/17/146/1714600.pdf .

[9] Spiegel Online article by Annett Meiritz, Yassin Musharbash and Severin Weiland of November 21st 2011, "Ermittlungspannen bei Neonazi-Mordserie: die Schuld der Behörden".

[10] For an overview, see the English blog article of the Privacy and Information Security Law Blog by Hunton & Williams LLP., published July 7th 2011, "Germany Launches National Cyber Defense Center".

Club (CCC) revealed disproportional capabilities, function creep, security flaws and inherent legality issues regarding this technology. As a consequence, governmental institutions renounced its use and initiated a process for programming and deploying a version of this software being compliant with the German constitution, which is still an on-going process.[11] Another security measure used by the Bundesnachrichtendienst, the German foreign intelligence service, is the key-word based strategic surveillance of email messages and data communications in the internet under involvement of internet service providers.[12] In general, the national security strategy increasingly relies on surveillance, thereby, surveillance-oriented security technologies becoming more and more important. So for example, the German Police Trade Union (German: Gewerkschaft der Polizei, GdP) demanded stronger investment in preventive measures like CCTV of high-risk public spaces.[13]

## 2.3 Major Privacy issues

Due to the historic experiences of vast surveillance and spying in the national socialist and GDR regimes, Germany has one of the most restrictive data protection and privacy laws in the European Union, which is the *Bundesdatenschutzgesetz* (BDSG, Eng.: Federal Data Protection Act), based on the European Data Protection Directive 95/46/EC. Due to the increasing processing of personal data by electronic devices in the country's administration, politicians in the German federal state of Hessen passed the first local data protection law world-wide already in 1970. At this time, the minister president of Hessen, Albert Osswald, stated: "The Orwellian vision of the all-knowing state, which investigates the most intimate corners of the human living sphere, will not become reality in our country" (quote translated from German).[14] The first federal data protection law came into force in 1979. On the basis of Germany's Federal Data Protection Act, each processing of personal data must have a specific and valid legal ground or the explicit, informed and valid consent of the concerned individual. The law always requires a specific purpose for the collection and processing of personal data. The German Federal Data Protection Act also foresees more specific regulations, specifying the requirements as manifested in the European Data Protection Directive 95/46 EC. Furthermore, it is foreseen that the compliance of personal data processing with the law is subject to oversight executed by specifically assigned and independent governmental data protection authorities. On national level, the Federal commissioner for Data Protection and Freedom of Information (German: Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, BfDI) is tasked to monitor the compliance with the Federal Data Protection Act and other data protection provisions. Article 24 BDSG stipulates the scope of competences, which primarily extends over the activities of the public bodies of the government and the activities of private entities in the telecommunication sector and for postal services. Additionally, in each German state, a specifically assigned data protection commissioner is tasked with matters evolving around personal data processing conducted by public bodies in this state and from private entities located there. The data protection supervisory authorities both on national and local level check and inspect the processing of personal data, either on own initiative or on the occasion of complaints from data subjects. They also advise and support data processors and data subjects. Furthermore, on their respective level of competence, these public bodies offer legislative recommendations for the federal and local parliaments and governmental institutions. All data protection authorities publish regular activity reports (yearly or biannual). The workload is in general quite high. For example, the Federal commissioner for Data Protection and Freedom of Information had 86 people on staff in 2012, while approximately 408 complaints from citizens had to be handled per month, additionally to self-induced investigations, participation in relevant data protection committees, consultation of the governments

[11] Spiegel Online article by Philipp Alvares de Souza Soares of March 5th 2014, "Amtliche Spähsoftware: Staatstrojaner-Fiasko verbittert Polizisten".

[12] Heise online, February 25th 2012, "Geheimdienste überwachten 37 Millionen Netzverbindungen".

[13] Cf. the position paper of the German Association of Towns and Municipalities together with the German Police Trade Union of January 27th 2014: " Sicherheit in Städten und Gemeinden – Positionspapier des Deutschen Städte- und Gemeindebundes (DStGB) und der Gewerkschaft der Polizei (GdP)", p. 4.

[14] Spiegel Online article, first published in print "Der Spiegel", 20/1971, May 10th 1971, "EDV im Odenwald", page 88.

regarding legislative undertakings, and research projects.[15] In general, the concept of privacy is differed from the concept of information control, taking into account a broader view on the protection of personal information. In Germany, the principle of informational self-determination (German: Informationelle Selbstbestimmung) was developed by the Federal Constitutional Court in its 1983 census landmark decision as a constitutional right in itself.[16] Regarding security measures, the German Federal Constitutional Court issues several rulings extending the protection of core areas of the citizen's lives. Examples are the 2004 ruling declaring a law enabling governmental eavesdropping in central parts unconstitutional as well as the 2008 ruling also declaring a law broadly enabling online searches as being unconstitutional.[17] In the latter ruling, the court even developed the principle of citizens having a basic right of full integrity and confidentiality of his or her information technology systems ("*Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme*") which the state is assigned to protect and thus sets strict preconditions for online searches on citizens' devices.[18]

In other areas, measures initiated with the premise of safeguarding against severe threats could not be held up since they were challenged due to their intrusiveness of citizens' lives. For example, the German data retention legislation issued under the umbrella of the European Data Retention Directive was declared unconstitutional and invalid by the German Federal Constitutional Court in March 2010 due to the law's violation of the constitutionally guaranteed telecommunication secrecy (Art. 10 (1) Grundgesetz). Additionally, the European Data Retention Directive was declared invalid by the European Court of Justice due to its legislative content not being proportional and entailing a too wide ranging and serious interference on the fundamental rights of European citizens with respect to private life and the protection of personal data.[19]

Beyond such solely security related issues, other legislative actions having an impact on privacy matters were subject of political and public discourse like the Motorway Toll Act for Heavy Commercial Trucks (Autobahnmautgesetz) aimed at enabling the collection of movement and traffic data of heavy commercial trucks. Since this data collection entails the exact toll amount, the correlating payment information, and the license plate number as well as the route of the lorry, it has the potential for being used as means of dragnet surveillance. Therefore, the intensive media attention shows the balance between security and privacy increasingly coming into the focus not only of politicians, but also of the broader civil society.

In the wake of the NSA revelations based on the documents taken away by whistle-blower Edward Snowden, press publications have shed some light on the cooperation between the German intelligence agencies and the US National Security Agency. According to the newspaper "Der Spiegel", the German foreign intelligence service (German: Bundesnachrichtendienst, BND) shared large amounts of meta data from their own communications intelligence with the NSA. Thereby, the BND issued a statement that personal data of German citizens were cleared, and e-mail addressed with the suffix .de as well as all telephone numbers with the country code +49 were filtered out.[20] Further cooperation was declared in a "Memorandum of Agreement" foreseeing the deployment of a common Signals Intelligence (SIGINT) station in Bad Aibling, whereas the exact content of this agreement is subject to secrecy. However, this document is the legal basis for the cooperation, being stated in the context of German legislative acts for counter-terrorism.[21] Moreover, the Federal Domestic Intelligence service for the Protection of the Constitution (German: Bundesamt für Verfassungsschutz) transmitted confidential

[15] Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, BfDI), Tätigkeitsbericht (Bi-Annual Report) for the years 2011-2012, pages 174 et seqq.

[16] Census decision of the German Federal Constitutional Court (in German: Volkszählungsurteil Bundesverfassungsgericht) of 15th December 1983 (Az.: 1 BvR 209, 269, 362, 420, 440, 484/83)

[17] Cf. the decisions of the German Federal Constitutional Court of 3rd March 2004, (Az.: 1 BvR 2378/98) and of 27th February 2008, (Az.: 1 BvR 370/07).

[18] Decision of the German Federal Constitutional Court of 27th February 2008, (Az.: 1 BvR 370/07).

[19] Judgement in joined cases C-293/12 and C-594/12Digital Rights Ireland and Seitlinger and Others by the Court of Justice of the European Union.

[20] Spiegel Online article of August 3rd 2013, "Überwachung: BND leitet massenhaft Metadaten an die NSA weiter".

[21] Tagesschau report of August 7th 2013, "BND-NSA-Kooperation: Streit über Steinmeiers Rolle".

data to the NSA and cooperates with eight further US intelligence services on a regularly basis.[22] Even though the NSA revelation caused a big uproar in German media, they sparked little activity on political level until this day. So far, several parliamentarian inquiries trying to shed light on the accusations were initiated, but brought only few results. Moreover, the Federal Prosecutor of the Federal Court of Justice in Karlsruhe initiated a judicial supervision process in June 2013 which led to first investigations in August 2013.[23] Furthermore, the German government entered negotiations with the US regarding a so-called No-Spy Agreement with the goal of achieving a bilateral renunciation of espionage. Nevertheless, due to the US being quite reserved in that regard the negotiations could not provide the desired agreement.[24]

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

The public discourse on surveillance-oriented security technologies covers a broad variety of different deployment fields and techniques. When the use of body scanners at airports hit media attention, the test runs of such devices at the Hamburg airport in September 2010 came into focus. The public debate showed that body scanners are often perceived as an intense intrusion of bodily privacy, especially for women, children and the disabled or elderly. In the end, the test run was terminated in July 2011 because the efficiency of the technology could not be proven unambiguously.[25] Another security technology focused on surveillance was and still is CCTV in Germany. A good example would be the judicial case of CCTV cameras in the red light district Reeperbahn in Hamburg in 2006, whereas a local resident demanded the termination of the surveillance due to her home being captured by the camera vision. After several instances of judicial proceedings, the highest court instance, the German Bundesverwaltungsgericht (Federal Administrative Court) issued a decision in January 2012, declaring the public space surveillance for public security in principle as a legitimate purpose, but that the cameras were not allowed to capture window, door and balcony images of the plaintiff's house through their panning, tilting and zooming capabilities. Due to the court, such undertakings violated the plaintiff's fundamental right to informational self-determination and the inviolability of the home.[26]

CCTV also plays a role in the context of public security at demonstrations and other large scale events, thereby often being criticized as having a chilling effect on citizens’ freedom of expression and freedom of association. In Germany, CCTV surveillance at demonstrations is only allowed under strict preconditions such as reasonable indication of public security and public order threats, which was also confirmed by several court decisions ruling over such matters.[27]

Moreover, the obtainment of cell phone data by law enforcement agencies (LEA's) is another surveillance-focused approach to achieve public security. These data always contain information about the location of cell phone users, as the ID of the cell tower is recorded. Cell tower data can either be obtained for specified mobile devices in order to reveal location and movement of a mobile device owner, often in combination with Stealth Ping (Silent SMS).[28] It can also be obtained to get the complete set of devices registered with a certain cell tower at a certain point of time in order to investigate which cell phones (and therefore users) were present at a certain location at a certain time period. Such

[22] Süddeutsche.de article by Christian Fuchs, John Goetz and Frederik Obermaier of September 13th 2013, "Verfassungsschutz beliefert NSA".

[23] Mitteldeutsche Zeitung, August 3rd 2013, "Bundesanwaltschaft prüft Ermittlungen zur NSA-Affäre".

[24] Zeit Online, February 28th 2014, "Steinmeier rückt von Anti-Spionage- Abkommen ab".

[25] Spiegel Online, August 31st 2011, „Flugsicherheit: Nacktscanner versagen im Praxistest“.

[26] Decision of the German Federal Administrative Court of January 25th 2012 (Az. BVerwG 6 C 9.11).

[27] Cf. the following exemplary decisions of the Berlin Administrative Court of July 5th 2010, „Beobachtung einer Versammlung durch die Polizei mittels Kameras und die Übertragung der Bilder in die Einsatzleitstelle“, (Az. 1 K 905.09) and of April 26th 2012, (Az. Az. VG 1 K 818.09), a ruling over the CCTV surveillance by the police at the Freedom Not Fear demonstrations.

[28] Cf. article of 1st February 2012 on the EDRI (European Digital Rights) website about the German police increasingly using Silent SMS to locate suspects;Netzpolitik.org article (in German) by Markus Beckedahl, published February 7th 2012, “Zwischenstand: 12 Millionen Funkzellenabfragen in Berlin”;another Netzpolitik.org article (in German) by Linus Neumann, published June 20th , 2011, "Dresden: Demoüberwachung mittels Mobilfunknetz".

procedures are highly controversial, and there have been cases where the use of such techniques was declared un-proportional and unconstitutional.[29]

In the digital world, several technologies focused on the surveillance of citizens are used for security purposes. Prominent examples being in the focus of media and public debate are measures of the strategic telecommunication network surveillance conducted by the Bundesnachrichtendienst. This could encompass the surveillance of email messages and data communications on the basis of certain key words, the governmental use (not only by the BND) of malware targeting individual devices (the so-called Bundestrojaner, Eng.: Federal Trojan or State Trojan), and investigation as well as other security activity in telecommunication networks. The network communication surveillance was conducted through the help of the private network providers deploying a fairly broad screening of emails and other communication outlets running over their servers. Public discussion related to this approach was sparked in 2012 when it was revealed that German intelligence agencies undertook a monitoring of over 37 million emails in Germany. In this context, the screening of communication with key word lists containing over 16.400 different terms was discussed. This kind of security measure was heavily criticized as dragnet surveillance not taking into account tangible suspicion factors.[30] Even more controversial was the discourse about the German State Trojan, of which the German Chaos Computer Club (CCC) discovered in 2011 that it entails overly intrusive surveillance functionalities on citizen's personal computers. This included remote control or backdoor functionalities as well as generally exposing the target device to other external malicious attacks due to weakened security. Several variants of this malware exist, whereas all of them have inherent and severe legality issues in respect to the German constitution.[31] Also, since the private company DigiTask which provided the software, would not provide insight to the software's source code, an internal review by German officials was not possible.[32] Ultimately, the use of the State Trojan provided by this private company was terminated and since then German LEAs have tried to internally develop a legally compliant version of the Trojan on their own, so far without tangible results.[33] Moreover, under specific circumstances, other security institutions in Germany could eventually conduct social network surveillance. Therefore, investigations and searches made through social networks and chat forums by law enforcement and intelligence bodies were also a topic in public discussion and media. This entailed a multitude of ethical and legal questions around different methods, such as passive investigation in the sphere of social networks, or the active use of LEA-set up Facebook fan pages (thereby delivering personal data of suspects and past criminals to private social network vendors located in other countries such as the U.S.) and the proactive request of personal data in the context of illegal content source tracking like copyright infringements or child pornography available online.[34] Thereby, the role of private companies acting as providers for chat and email services sparked controversy due to their own proactive screening of user content and the resulting conflicts with the German data protection law as well as telecommunication secrecy legislation.[35]

In general, the retention of personal data originally collected by service providers was and still is topic of discussion in Germany. After the adoption of the EU Data Retention Directive in March 2006, it became implemented into German national law through amendments made in the German Telecommunications Act which came into force in January 2008. These amendments sparked controversy in the German media and among the citizenship, leading to a strong movement against data retention. A German association of civil rights activists, the "Arbeitskreis Vorratsdatenspeicherung (Working Group on Data Retention)", played a central role in coordinating a quite successful campaign

[29] Berlin Data Protection and Freedom of Information Commissioner, report of September 3rd 2012, „Abschlussbericht zur rechtlichen Überprüfung von Funkzellenabfragen"; also, the Saxony Data Protection Commissioner had similar findings expressed in his report over non-individualised cell tower inquiries and other means of telecommunication surveillance through police and prosecutors in Dresden in February 2011.

[30] Heise online, February 25th 2012, "Geheimdienste überwachten 37 Millionen Netzverbindungen".

[31] The H Security blog article published October 10th 2011, "CCC cracks government Trojan"; The H Security blog, October 26th 2011, "CCC criticises new version of government Trojan".

[32] The H Security blog, September 11th 2012, "Federal Commissioner unable to audit Federal Trojan source".

[33] Cf. footnote 9.

[34] See the overview in the Zeit Online article by Hellmuth Vensky, published July 9th 2012, "Die Fallstricke der Facebook-Fahndung".

[35] Cf. Der Tagesspiegel news article by Markus Ehrenberg, published July 18th 2012, "Sinnvoll skandalös".

to mobilize citizens against the legislative act of the German government. Thousands of citizens demonstrated against the data retention legislation, and a complaint before the Federal Constitutional Court was supported by over 34,000 persons.[36] The court issued a decision on March 11th 2008, thereby declaring the relevant parts in the Telecommunications Act concerning the German legislative implementation of the Data Retention Directive as unconstitutional. The court's decision did not rule out the possibility of a constitutional realization of the Directive, but preconditioned that only indirect retention by private companies and not by the state itself occurs, including appropriate provisions for usage preconditions, data security, transparency and efficient enforcement of these rules.[37] After that ruling, data had to be deleted without delay and in the German security debate, politicians disputed for quite some time about a new implementation and how it would have to look like to fulfil the requirements of the Federal Constitutional Court. In the meanwhile, the public discussion continued as well and was significantly influenced by the action of the German politician Malte Spitz, member of the green party, who initiated a visualization of his mobile phone data for a specified time period. This visualization shows how call data records together with location data collected by providers of mobile phone networks can lead to conclusions about detailed situations in the life of an individual, including social interactions.[38] In June 2011, former federal justice minister Leutheusser-Schnarrenberger provided a new draft for a national implementation of the Directive which went into political discussion.[39] In the meanwhile, the European Union had initiated an infringement proceeding in May 2011 against the German government due to the missing implementation of the EU Data Retention Directive.[40] However, this proceeding was dropped after the judgement of the Court of Justice of the European Union on April 8th 2014 declaring the EU Data Retention Directive invalid.[41] Since then, no new initiative on national level was started to implement data retention in Germany. Also an intense discussion on the value of privacy and data protection was triggered since the revelations about the secret activities of the U.S. National Security Agency (NSA) on the basis of the whistle-blower Edward Snowden in June 2013. Snowden retrieved this trove of information during his work as technician for the company Booz Allen Hamilton, contracted by the NSA, and handed it over to selected journalists who have gradually and selectively published parts of it so far, whereas further revelations are to be expected. In Germany, the factual proof of diverse spying programs caused noticeable public attention which is still on-going. It entails debate over the proportionality of security measures in relation to the dangers of all-encompassing surveillance of citizens as well as of economic espionage targeting the companies of other countries. Thereby, it was shown and confirmed that Germany is seen by the U.S. as cooperating partner in intelligence activities, yet also as a target country.

While on political level, the factual consequences are sparse so far, media has been speculating about the involvement of German intelligence services like the BND.[42] In the public discussion several aspects of the NSA surveillance play a role, for example the dangers of private companies being forced to comply with U.S. government demands of handing over data of German citizens.[43]

Despite of the stated original purpose of such activities, i.e. the persecution of terrorism, also the surveillance of democratically elected German politicians, economic stakeholders and EU institutions caused some irritation on political level. So the public debate and media echo significantly intensified after the revelation that the German chancellor's mobile phone has been wiretapped, exposing the futile work of Germany's security agencies in protecting a single device against the spying of a foreign intelligence entity. The spying on the communication of a foreign, yet allied country's leader has left a

[36] See the website information entry about the Federal Constitution Court complaint coordinated and set up by the Arbeitskreis Vorratsdatenspeicherung, http://www.vorratsdatenspeicherung.de/content/view/51/1/lang,de/%3E.

[37] Cf. The judgement of the German Federal Constitution Court of March 11th 2008, case number 1 BvR 256/07.

[38] Zeit Online article by Kai Biermann, published March 26th 2006, "Betrayed by our own data".

[39] Website entry of the Bundesministerium der Justiz (Federal Ministry of Justice) of June 10th 2011, "Quick-Freeze: Bundesjustizministerin legt Gesetzentwurf vor".

[40] Die Welt article published June 22nd 2011, "EU leitet Verfahren gegen Deutschland ein".

[41] Court of Justice of the European Union, judgment in joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others.

[42] Cf. footnote 16.

[43] Sueddeutsche.de article by Bastian Brinkmann,Oliver Hollenstein und Antonius Kempmann of November 16th 2013, "Was Spionagefirmen in Deutschland für die USA treiben".

mark of mistrust on the relationship between Germany and the USA, fuelling still on-going intense debates of the public about illegal spying on individuals in general. In German media, the whole scandal caused citizens participating in demonstrations against the surveillance as well as drafting several petitions and open letters which demand more action from the German government, wishing for a better protection of German citizens to prevent this extensive intrusion into their personal lives.[44] Furthermore, the digital surveillance revealed led to a significantly stronger awareness regarding the protection of personal communication. One indicator for this is a noticeable stronger effort of citizens using technical means for circumventing or hindering surveillance since summer 2013.[45]

Such governmental surveillance is in general perceived strongly critical within the German civil society, which still has quite strong negative emotions and memories of secretive and oppressive police state institutions like the Gestapo, SS, SD and Security Police. These at their time of the national-socialist regime took actively part in the systematic persecution and extermination of not only regime dissidents, but also individuals of other nations and religious and societal views. Moreover, the later SED-dictatorship in the GDR maintained an official intelligence agency, called the Ministry for State Security (German: Ministerium für Staatssicherheit, commonly known as the Stasi, which is an abbreviation of Staatsicherheit). This organisation is still remembered as an oppressive intelligence body spying on large parts of the population, using covert and open methods of decomposition within the societal structures. Due to these historic experiences, part of the German citizenship has developed some mistrust in governmental intrusion on citizens' lives. This is less so the case for police institutions than it is for intelligence agencies. Therefore, surveillance is often seen as critically and inherently dangerous for the civil liberties of individuals. After the terrorist attacks of September 2001, this stance diminished towards a heightened acceptance of surveillance as means of enabling public security. However, this swing of public opinion proved only temporary, since over time the impact of surveillance technologies on privacy matters once again became increasingly subject of public discussion and political discourse. This includes questions raised in the public discourse on the effectiveness of SOSTs, transparency regarding the rules of their deployment, and limitations aligned to the democratic principles of the German state, like premises bound to single-case operations and effective judicial oversight.

[44] Cf. the overview in the German Wikipedia entry for the NSA scandal; subtitle "Basisdemokratische Initiativen" (Eng. Basic democratic initiatives).

[45] One expression of such changing behavior is the rise of the Crypto-Party-movement, which got a fair amount of media attention in 2013 and 2014, e.g. in the TV show rbb-Kultursendung “Stilbruch” of August 15th 2013, titled "Freiheit im Internet".

# 3 Process design – the citizen summit in Germany

The SurPRISE citizen summit in Germany addressed the opinions of citizens on privacy, security and surveillance-oriented security technologies (hereinafter: SOSTs). The event took place on March 29th, organized by the ULD in the Atlantic hotel in Kiel, northern Germany. Even though this city is located rather far in the North of the country it provided sufficient transport connections for the execution of such a citizen summit. Various means of public transport (via train, ship, buses etc.) and direct access to the motorway made it easy for interested persons to get to the premises of the citizen summit. Kiel itself is the capital and most populous city of Schleswig-Holstein (the northernmost federal state in Germany), located within reasonable distance to Hamburg. Hamburg itself is the second largest city of Germany, which made it possible to recruit participants from urban areas as well as from rural areas in the in direct vicinity of Kiel.

At the event, the citizens were seated at 25 tables, each guided by a table moderator. At 3 tables, additional minute takers have been placed. Nine of the table moderators and all three minute takers were employees of ULD, the other table moderators were current or former trainees as well as students from Kiel University. All table moderators had been trained in advance of this day. A head facilitator led through the event the whole day, explaining the program and the to-dos for the citizens. The planned time schedule was kept and the event went smoothly. The opinions gathered were obtained through various ways based on the citizen summit user manual and the consortium training in accordance with the other project partners.

Regarding the above mentioned topics, the event provided two main foci: One focus was laid on specific, pre-selected SOSTs as tangible examples to discuss about, while the second focus was on the citizen's general stance regarding privacy, security and surveillance – independently from any specific technology. The two SOSTs addressed at the German citizen summit were smart CCTV and smartphone (and general mobile phone) location tracking (hereinafter: SLT). Citizens were provided with different possibilities to express their opinions. At the beginning of the event, the participants received so-called clickers, electronic devices which could in the following be used to vote on answers in a digital questionnaire. These questions addressed different thematic parts, thereby covering quantitative as well as qualitative elements. Citizens could use these clickers as a polling system to either vote their agreement/disagreement on given statements or to answer open questions. Besides the questionnaire, citizens could also express their opinions in discussion rounds. The whole day presented overall three different discussion rounds. The first two rounds were focused on the benefits and drawbacks of the SOSTs mentioned above. These SOSTS-related discussion rounds were started directly after the presentation of a short introductory film giving some background information on the individual SOSTs. The purpose of these two little films was to ensure each citizen would have the same minimum level of knowledge about the technology and to start off the discussion at the tables. The third and last round was focused on creating one recommendation per table on security and privacy aimed at policy makers mainly on European, but also on national level. During the group discussions, the main controversies and arguments debated on were captured through notes of the table facilitators and more in-depth at three tables by additional minute takers. Beyond the table recommendations, citizens were encouraged to write additional thoughts and recommendations related to the topics of the day on smaller postcards, which were collected at the end of the day. After the citizen summit, the table facilitators and minute takers were also asked specific questions about their own impressions on the citizen summit to enable a better evaluation of the event. The participants received a reimbursement of 25 or 50 Euro, depending on their travel distance to the location of the summit.

## 3.1 Organisational setting

Based on the incoming registrations, ULD chose a group which presented the utmost possible mixture regarding the following criteria: gender, age, education, occupation and type of settlement. Out of 250 registered citizens, 221 citizens were invited. The citizens selected received an official invitation/confirmation letter, including the consent form as well as additional material including an information brochure giving basis knowledge about the SOSTs to be discussed, as well as information about the day program and the logistics of the event (date & time, venue address, public transport, parking, etc.). The citizens not selected received a notice explaining why they had not been chosen.

As for the targeting of the citizens, obtaining address data from public authorities would have been one lawful possibility. But in Germany, a central register is neither on federal level, nor on the level of the German Länder existent. Obtaining address data from private companies was not chosen as a way of recruitment since additional consent given by citizens for the further purpose of this summit would have become necessary, causing additional administrative effort. Therefore, ULD decided for an open recruitment approach. Thereby, the challenge was to avoid attracting mainly citizens who are interested in the work of ULD, whereas it could be assumed that those people are already very aware of data protection issues. Therefore, ULD paid particular attention to address citizens not belonging to special interest groups. This was conducted mainly by the following measures:

- Public relations work, using various media outlets,
- Advertisements in local and regional newspapers,
- Involvement of multipliers, such as public authorities (municipalities), companies, non-governmental organizations, associations etc.,
- Distribution of flyers and posters at various locations in the urban and rural areas of Hamburg, Kiel, and direct vicinity like e. g. in cafés, sports groups, libraries, public buildings, university etc.,
- Short information spot in the local TV,
- Direct distribution of information material.

These measures were accompanied by information about the citizen summit on the website of ULD. Furthermore, ULD provided direct contact information by telephone and e-mail as well as the possibility to either register for the event via an online form on the website, or offline via post mail.

## 3.2 Structure of the citizen panel

This section elaborates on the demographic structure of the whole group of citizens who participated in the event. To provide an easy overview of the questionnaire results, tables will show in order the percentage results of the questions. The individual questions will in the following always labelled as Q + their number to allow a better allocation to the complete set of questionnaire pieces developed in the project (e.g. Q3, Q4, etc.). Overall, 221 citizens were selected and invited to the summit. In the end, 190 citizens showed up and participated in the event. Of those citizens who were there and voted with their clickers (in the following always the number N – here: N = 188), a majority of 28.2% came from the age group of 40-49 years old individuals. The smallest age group was those of over 70 years old with only 1.6% (see table below).

**Q01 - Age (total of valid answers: N= 188)**

| | |
|---|---:|
| 18-29 years old | 23.4 % |
| 30-39 years old | 11.7% |
| 40-49 years old | 28.2% |
| 50-59 years old | 23.9% |
| 60-69 years old | 11.2% |
| Over 70 years old | 1.6% |

Table 1: Overview of the different age groups

Of the whole group of participants, about 35.8% were female, while a majority of 62.6% was male. Only 1.6% refused to provide information on their gender.

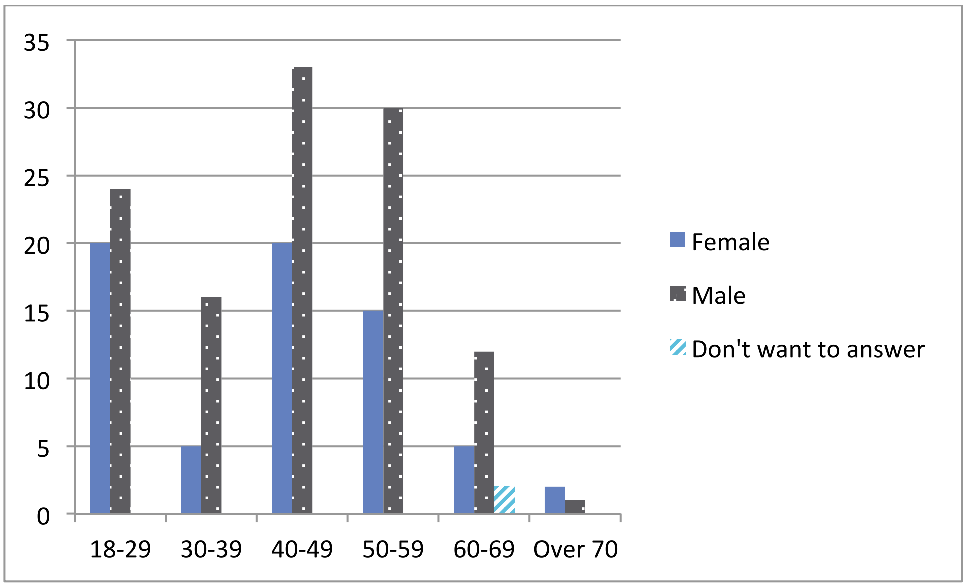


Figure 1: Gender and age ratio of participants

Furthermore, 17.0% of the citizens have children at home aged 16 or under, while 78.6% do not and 4.4% chose the "Don't know/do not want to answer" option (in the following: N/A). The majority of citizens said they come from an urban area (64.8%) and still 28.6% stated they come from a rural area. This result roughly matches the region of Kiel as a medium-sized city with quite large rural vicinity. About 5.5% of the participants said they come from a metropolitan area. The questionnaire results show that the level of education was overall rather high among the participants. A large majority of 27.9% said they have a postgraduate university education, while still 36.6% of the citizens stated to have either an undergraduate university or at least vocational qualification (see table below).

**Q100 – Highest level of formal education (N= 183)**

| | |
|---|---:|
| Primary school | 1.6% |
| Lower secondary | 12.0% |
| Upper secondary | 18.6% |
| Vocational qualification | 16.4% |
| University – undergraduate | 20.2% |
| University – postgraduate | 27.9% |
| Don't know/do not want to answer | 3.3% |

Table 2: Level of education

The majority of citizens stated they were employed (42.9%). Moreover, the group of participants had a considerable number of students (17.6%) and self-employed (13.2%) individuals. Thereby, most of the citizens said they come from a rural area while it is noticeable that no students came from a metropolitan area but rather from an urban one, indicating that most of the students are ones from the University of Kiel nearby (see figure below).

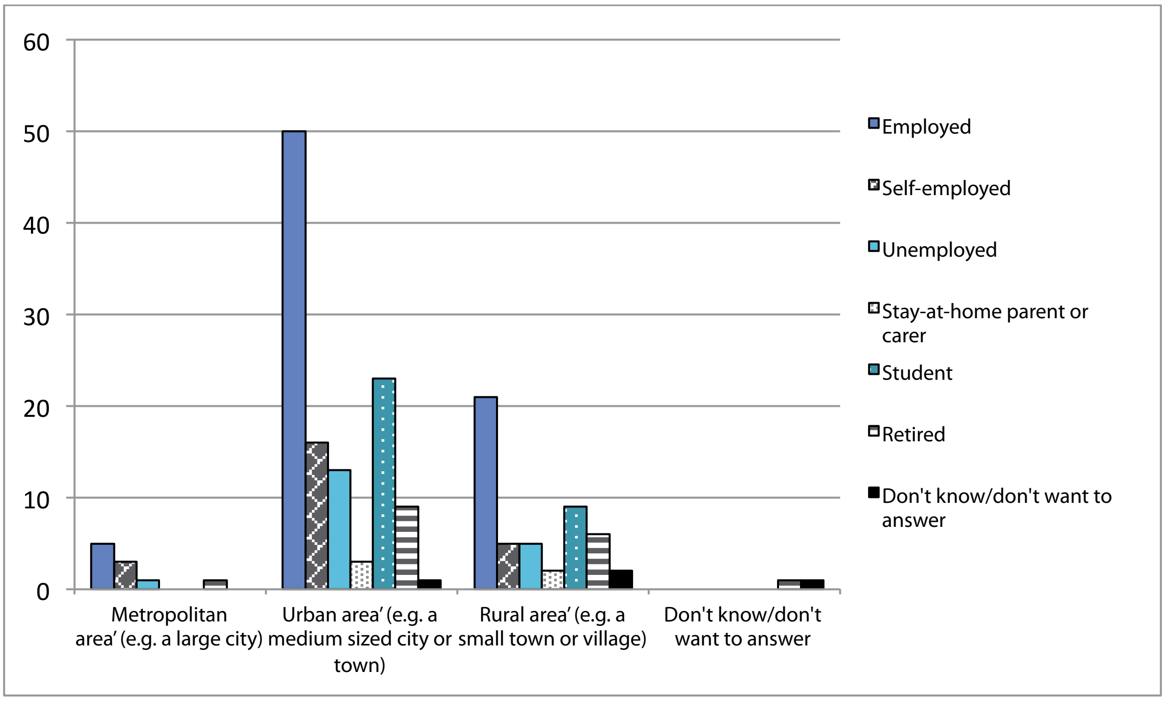


Figure 2: Employment status of citizens per area of living

Of those citizens who voted with their clickers (N = 181), the majority of 30.4% stated being of professional education (expert in a specific field). The next largest percentage of participants (21.0%) said they were manager, legislator, or senior official while only a small group stated being occupied in some kind of craftwork (1.7 %). The related income compared to the average of the German country was stated by the majority of citizens as less than average (43.0% less or even a lot less) while 33.5% said they earn more or even a lot more than the average. A fairly high number of 17.9% chose the "don't know/ do not want to answer option".

Of the complete group of participants, the largest part of 91.1% stated being a citizen of the country, while the rest of the group had various other constellations of citizenship, thereby 2.8% with dual citizenship of two European countries and 2.2% with dual citizenship of two non-European countries. In this context, the citizens were also asked if they would consider themselves belonging to some kind of minority group. The majority of them (69.9%) did not agree to this while 19.7 % consider themselves so and 10.4% chose the "don't know/do not want to answer option".

Overall, it can be said that the majority of citizens belong to a middle-ages group while males were more present than females. Generally, the education level was quite high, and together with the results from the citizenship, minority and occupation questions, it can be assumed that for the largest part, the group of the participants belong to the standard German, educated middle class of national citizenship. Despite ULD's efforts of widespread recruitment, this was to be expected, taking into account the complexity of the topics addressed in this citizen summit.

## 3.3 How citizen assessed the summit

Throughout the day and afterwards, feedback was that the summit was an enjoyable and quite educative event. This impression reflects in the related questionnaire statements given by the citizens present. 53.7% of the citizens agreed or even strongly agreed that they had gained new insight into the topics addressed by participating while 22.6% were undecided and 23.7% disagreed or strongly disagreed with that statement. A majority of 57.8% believe that this event has generated valuable knowledge for politicians (see table below).

| | | | Strongly agree | Agree | Neither agree nor disagree | Disagree | Strongly disagree | N/A |
|---|---|---|---|---|---|---|---|---|
| | | **N** | **Percentages** | | | | | |
| I have gained new insight by participating in the citizen summit | Q106 | 186 | 29.0% | 24.7% | 22.6% | 11.3% | 12.4% | 0.0% |
| I believe the citizen summit has generated valuable knowledge for the politicians | Q107 | 185 | 36.2% | 21.6% | 27.0% | 8.1% | 4.9% | 2.2% |

Table 3: Perception of gained insight and achieved outcome

In general, citizens seem to have perceived this event as useful to stimulate discourse. However, despite the gained information, e.g. through the distributed information material, the films, and the communication with others in the group discussions, did not change their attitudes on SOSTs for a large majority of 66.5% of the participants. Still, a slightly smaller group of 26.5% perceive SOSTs more critical now, which could be interpreted as heightened awareness of the problematic issues linked to the deployment of such measures.

**Q108 – Has this experience changed your attitudes regarding surveillance-oriented security technologies? (N= 185)**

| | |
|---|---|
| They are now more positive | 4.9% |
| They are now more negative | 26.5% |
| The same as before | 66.5% |
| Don't know/do not want to answer | 2.1% |

Table 4: Changes in attitude after the citizen summit

In general, citizens thoroughly enjoyed the opportunity to share their thoughts and opinions with others. Some even explicitly expressed their relief that they were "not alone with their opinion", but were also acknowledging different views as an enriching experience broadening their perspective on the topics discussed.

# 4 Empirical results of the citizen summit

In this chapter, the empirical results of the German citizen summit are presented and interpreted, thereby, giving an impression of the different perceptions of citizens on privacy, security and surveillance. The material used to generate these results consists of the questionnaire conducted during the event, the notes and impressions in the group discussions of the table facilitators and note takers present and the table recommendations and smaller postcards the citizens created. Also in this context, tables and figures will give an overview on the empirical results gained.

The material was collected with the goal to inquire citizen's stance on the relationship between privacy and security, within the classical trade-off model as well as beyond it. Thereby, the factors relevant for the acceptance and acceptability of SOSTs as well as the substantive privacy concerns of citizens form a main objective for the evaluation of the results.

## 4.1 General attitudes on privacy and security

Of the nine citizen summits in the diverse countries conducted, the German summit revealed a significantly stronger critical stance of German citizens towards surveillance-oriented security technologies. In general, the participants assessed their own knowledge on such technologies as being quite well-founded or at least average already before the citizen summit. While 44.9% rated themselves as very or well knowledgeable, still 36.0% said they already had some knowledge on the topic (see table below). This shows that citizens seemed to already have had some awareness of SOSTs before the event.

**Q6 – Before reading the SurPRISE information booklet, how would you rate your knowledge of surveillance-oriented security technologies? (Total of valid answers: N= 178)**

| | |
|---|---:|
| I was very knowledgeable | 8.4% |
| I knew a good amount | 36.5% |
| I had some knowledge | 36.0% |
| I knew little to nothing | 18.0% |
| Don't know/don't want to answer | 1.1% |

Table 5: Knowledge on surveillance technologies before the citizen summit

However, at the end of the day citizens were asked to assess their knowledge after they had read the information booklet distributed in advance of the summit as well as having discussed with other citizens and seeing the introductory films. In response to this question, 79.0% said they are now very or at least well knowledgeable while still 17.7% said they would have some knowledge after the experience at the summit.

**Q93 – After watching the SurPRISE films, discussing with fellow participants and reading the information booklet, how would you rate your knowledge of surveillance-oriented security technologies? (Total of valid answers: N= 181)**

| | |
|---|---:|
| I am very knowledgeable | 22.1% |
| I know a good amount | 56.9% |
| I have some knowledge | 17.7% |
| I know little to nothing | 2.8% |
| Don't know/don't want to answer | 0.6% |

Table 6: Knowledge on surveillance technologies after the citizen summit

Therefore, while citizens assessed their level of knowledge as already high prior to the event, the knowledge and confidence about SOSTs seem to have increased significantly throughout the day. With regard to gain some insight to the general attitudes on privacy and security, questions were asked related to citizen's subjective feelings of personal and general security as well as privacy. Thereby, the level of concerns related to both aspects was explored.

| | | | Strongly agree | Agree | Neither agree nor disagree | Disagree | Strongly disagree | N/A |
|---|---|---|---|---|---|---|---|---|
| | | **N** | **Percentages** | | | | | |
| I feel safe in my daily life | Q3 | 188 | 21.3% | 45.2% | 29.3% | 3.7% | 0.5% | 0.0% |
| I'm worried about security when online | Q4 | 187 | 31.6% | 25.1% | 26.7% | 12.8% | 3.2% | 0.5% |
| I feel I can live securely in this country | Q5 | 186 | 26.3% | 47.3% | 21.5% | 1.6% | 2.7% | 0.5% |
| Security technologies should be used to improve national security | Q7 | 181 | 9.4% | 14.4% | 23.8% | 21.0% | 30.9% | 0.6% |
| Concerned of surveillance oriented security technologies eroding privacy in general | Q8 | 188 | 47.9% | 25.0% | 19.1% | 5.9% | 1.6% | 0.5% |
| Concerned of surveillance oriented security technologies eroding my privacy | Q9 | 186 | 42.5% | 25.3% | 17.2% | 11.3% | 3.2% | 0.5% |
| Alternative approaches to security which do not involve surveillance-oriented security technologies should be given higher priority | Q10 | 186 | 47.8% | 23.1% | 19.9% | 4.8% | 2.2% | 2.2% |

Table 7: General attitudes on security

The results as shown in the table above show that most of the participating citizens feel quite secure in their daily life. However, a higher percentage is worrying about security when they are active online. There are several reasons imaginable for this outcome. One reason might be that citizens have greater difficulty in assessing risks related to complex technological matters in the digital sphere. Another reason that could play a role is that some of the participants already had negative, security related experiences online, e.g. with malware, identity theft, or the like. Inquiring on the citizens general attitudes on privacy and security, quite considerable objections were raised regarding surveillance oriented security technologies being used to improve national security (about 51.9% overall from the disagree/strongly disagree range). This critical stance became even stronger during the day of the citizen summit, thereby resulting in 60.1% either disagreeing or strongly disagreeing at the end of the day to the statement that SOSTs should be routinely used for security purposes (see the results to Q94 in table no. 16 in chapter 4.2.3). Moreover, SOSTs are generally and personally perceived as a threat to privacy, whereas the differences between the results of questions 8 and 9 suggest that the perceived general societal impact has a slightly stronger emphasis than the personal one. This impression was confirmed by the correlating questions Q95 and Q96 asked at the end of the citizen summit which address the question whether the citizens feel concerned regarding SOSTs eroding privacy in general and personally (see the results shown in table no. 17 under chapter 4.2.3). When these later questions were asked, citizens had developed an even stronger opinion of SOSTs endangering privacy on a personal, but even more on a general level.

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

In the previous section, the general stance of citizens on privacy and security was examined. In contrast to this, the current section focuses on important aspects regarding the acceptance and acceptability of specific SOSTs. Moreover, the level of perceived security improvement with regard to the impact and proportionality of technology deployment is being scrutinized, taking into account the perceived effectiveness on the one hand and the perceived intrusiveness of the security measure on the other. Thereby, the main privacy concerns of citizens as well as their stance of avoidance or even resistance against surveillance are evaluated, including perceptions of individual as well as collective aspects in the context of personal experiences in contrast to the citizen's outlook on general societal values.

To prepare the ground for the more in-depth questions related to the specific SOSTs addressed at the German citizen summit, introductory questions delve into the matters of SOSTs awareness and general knowledge about it. So regarding Smart CCTV, Q11 aimed at learning if and how often citizens are aware of CCTV observation within the local area they are living in (see table below). The results show with 58.0%, the majority of citizens are not or only rarely aware of CCTV cameras being used to observe the public space around their living area, while 20.2% said they notice them only sometimes. Still, a considerable number of citizens (20.2%) stated that they had awareness (often or even all the time) about the visual surveillance around their home space.

*Smart CCTV*

| | | | Never | Rarely | Some-times | Often | All of the time | N/A |
|---|---|---|---|---|---|---|---|---|
| | | **N** | **Percentages** | | | | | |
| In the area where you live, how often do you see CCTV cameras | Q11 | 188 | 23.4% | 34.6% | 20.2% | 12.2% | 8.0% | 1.6% |

Table 8: Awareness of Smart CCTV

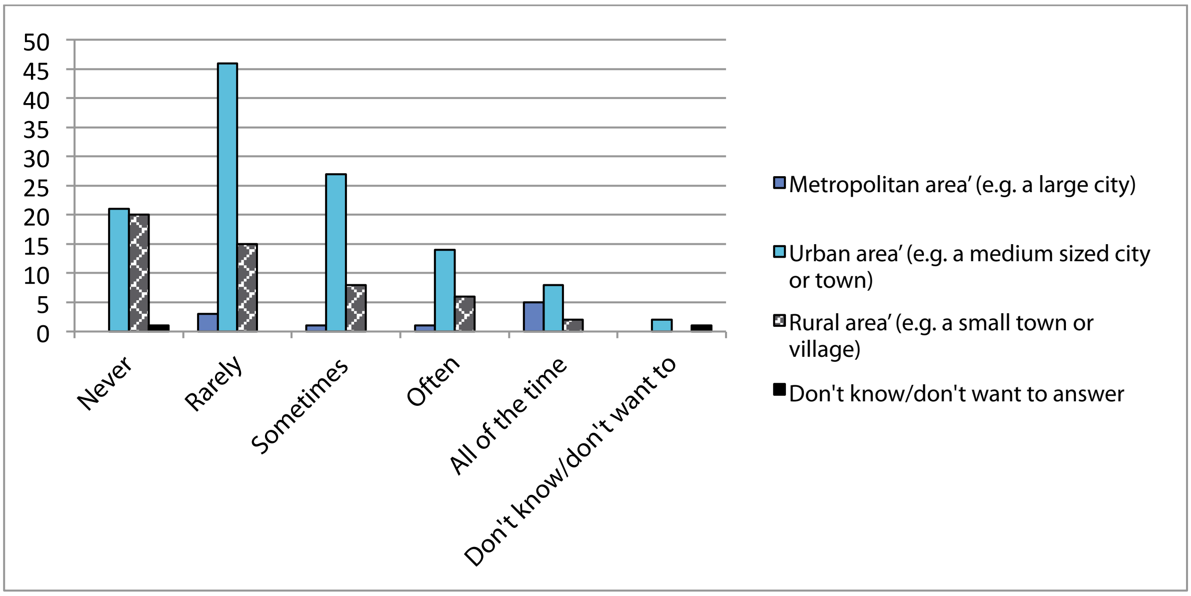


Figure 3: Awareness of CCTV surveillance visualized (Q11)

Consequently, it seems that public space CCTV is in general a rather unobtrusive security measure but still, a number of citizens actively keep their eyes out for these cameras. This result suggests that for parts of the population, CCTV surveillance is not yet perceived as the normal setting in public spaces. Q14 shows that after being provided with the information material prior to the summit and being shown the explanatory short film during the event, the majority of citizens (82.2%) well understood what Smart CCTV is.

### *Smart CCTV*

| | | | Strongly agree | Agree | Neither agree nor disagree | Disagree | Strongly disagree | N/A |
|---|---|---|---|---|---|---|---|---|
| | | **N** | **Percentages** | | | | | |
| I understand what Smart CCTV is | Q14 | 185 | 46.5% | 35.7% | 11.9% | 4.3% | 1.1% | 0.5% |

Table 9: Comprehension of the Smart CCTV technology

The correlating questions regarding the prevalence of smartphone use and comprehension of the technology are Q13 and Q16 (see tables 10 and 11 below). Q13 shows that the majority of summit participants (overall 68.6% either often or all the time) use mobile devices such as mobile phones or smartphones, whereas still 19.1% said they use these sometimes and only smaller percentages answered they use them only rarely (8.5%) or even never (3.7%).

### *Smart phone location tracking*

| | | | Never | Rarely | Sometim es | Often | All of the time | N/A |
|---|---|---|---|---|---|---|---|---|
| | | **N** | **Percentages** | | | | | |
| How often do you use mobile devices, such as mobile phones or smartphones | Q13 | 188 | 3.7% | 8.5% | 19.1% | 16.5% | 52.1% | 0.0% |

Table 10: Prevalence of mobile device use

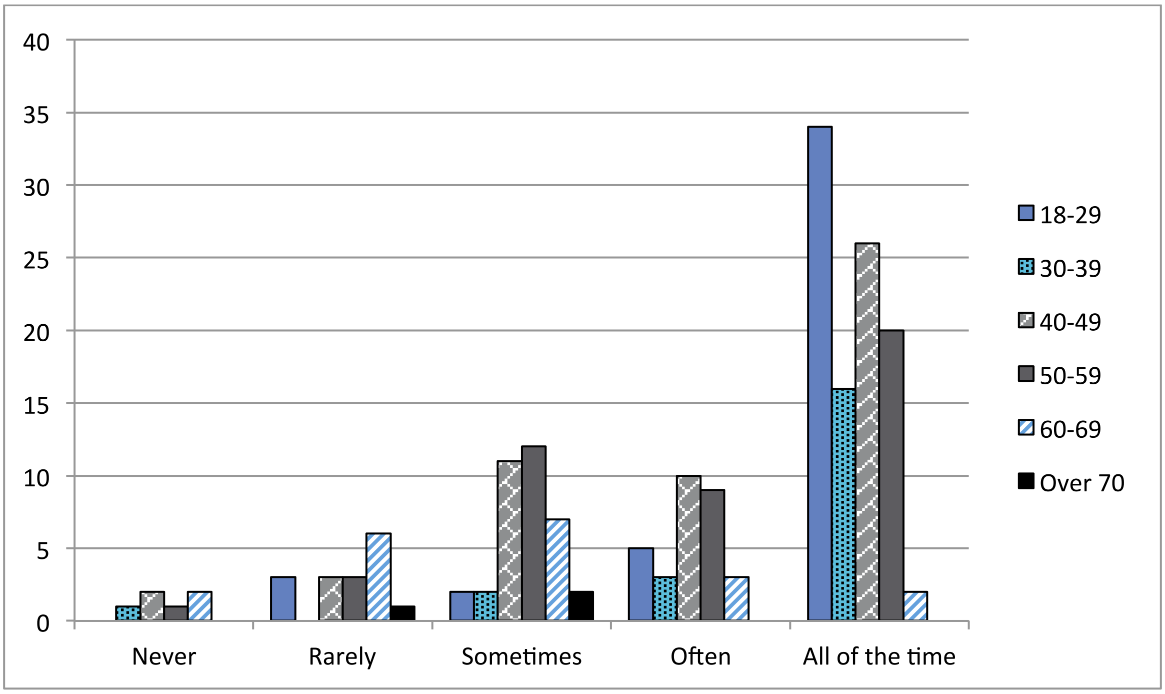


Figure 4: Prevalence of mobile device use visualized (Q13)

In comparison to Smart CCTV, citizens assess their comprehension of the technology much higher when it comes to SLT, as the results of Q16 (see below) show.

### *Smart phone location tracking*

| | | | Strongly agree | Agree | Neither agree nor disagree | Disagree | Strongly disagree | N/A |
|---|---|---|---|---|---|---|---|---|
| | | **N** | **Percentages** | | | | | |
| I understand what Smartphone Location tracking is | Q16 | 186 | 74.2% | 18.3% | 4.8% | 1.1% | 1.1% | 0.5% |

Table 11: Comprehension of the Smartphone Location Tracking technology

So it appears that mobile devices are relatively common among German citizens, who use them frequently or even regularly in their everyday lives. In this context and building upon the aforementioned information distribution through information material and film, a vast majority of citizens (92.5% strongly agree or simply agree) said they understand what Smart phone location tracking is.

Thereby, it becomes clear that while Smart CCTV and Smart phone location tracking are at least partially new developments in the field technology, the general overview knowledge regarding these surveillance-oriented SOSTs is in principle conceivable in relatively short time by citizens, if it is presented in a clear and concise way. Therefore, the information material and the films gave the citizens a well-founded basis to assess the deployment and impact of SOSTs during the event, empowering them to express their opinions on this technology. Still, they were made aware that the functional details are not the centre of evaluation, but rather the opinions of the citizens regarding the technology's privacy intrusiveness and correlating acceptance factors.

### 4.2.1 Perceived effectiveness vs. intrusiveness of SOSTs

At the citizen summit, the participants had the chance to express their opinions on the perceived effectiveness of surveillance oriented security technologies. Moreover, they could share their thoughts on the perceived intrusiveness of the discussed SOSTs on citizen's privacy. Thereby, the first introductory questions addressed their general stance on SOSTs being used as a security tool. To give a better overview over the results, introducing tables per technology will in the following give insight to the in-depth outcome of the individual questions asked, beginning with Smart CCTV.

*Smart CCTV*

| | | | Strongly agree | Agree | Neither agree nor disagree | Disagree | Strongly disagree | N/A |
|---|---|---|---|---|---|---|---|---|
| | | **N** | **Percentages** | | | | | |
| Smart CCTV is an effective national security tool | Q17 | 186 | 7.0% | 16.7% | 29.0% | 24.2% | 21.5% | 1.6% |
| Smart CCTV makes me feel uncomfortable | Q18 | 187 | 43.9% | 27.3% | 10.7% | 11.2% | 6.4% | 0.5% |
| Smart CCTV makes me feel more secure | Q19 | 185 | 3.8% | 10.3% | 17.8% | 22.7% | 44.3% | 1.1% |
| Feeling that Smart CCTV is forced upon me without permission | Q20 | 182 | 67.0% | 15.4% | 6.0% | 2.7% | 6.0% | 2.7% |
| Smart CCTV appropriate way to address security threats | Q21 | 185 | 6.5% | 7.6% | 21.6% | 29.7% | 33.0% | 1.6% |
| Smart CCTV does not bother as long as it targets only criminals | Q32 | 186 | 4.8% | 4.3% | 8.1% | 12.9% | 61.3% | 8.6% |
| I worry how the use will develop in future | Q33 | 181 | 61.3% | 19.3% | 8.3% | 6.1% | 3.9% | 1.1% |
| Smart CCTV bothers only if it's used in the area where I live and work | Q34 | 182 | 3.8% | 4.4% | 4.4% | 13.2% | 68.7% | 5.5% |

Table 12: Perceived effectiveness of Smart CCTV

As these results show, most of the citizens do not perceive Smart CCTV as an effective national security tool (45.7% overall either disagree or even strongly disagree). A large percentage of 29.0% was not decided on their stance regarding this statement while only 23.7% of the participants agreed or strongly agreed on Smart CCTV being an effective tool to foster national security.

Thereby, a large majority of citizens said that Smart CCTV makes them uncomfortable. In this context, it is noticeable that a quite high percentage of 43.9% even agreed strongly on this statement while still 27.3% chose the simple agreement, making it overall a rate of 71.2% of citizens being uncomfortable with the observation of public spaces via Smart CCTV. Consistent with this statement, only 14.1% of the citizens agreed that they would feel more secure due to Smart CCTV operation while in contrast, about 67.0% said they disagree or even strongly disagree with that statement that this observation would make them feel more secure. Rather, a vast number of citizens feel that this SOST is forced upon them without their permission (82.4% agree/strongly agree) while at least 62.7% expressed disagreement on Smart CCTV being an appropriate way to address national security threats and still 21.6% were undecided.

As a rather interesting fact, the citizens did not reduce their disaffirmation of Smart CCTV as security tool to the question whether they are personally affected. This shows in the results of Q32, where 61.3% strongly disagreed and still 12.9% simply disagreed that this SOST would not bother them of if would target only criminals. It is noticeable in the context of this statement in comparison to the others shown in the table above that here, a slightly larger number of citizens (8.6%) chose the do not know/want to answer option.

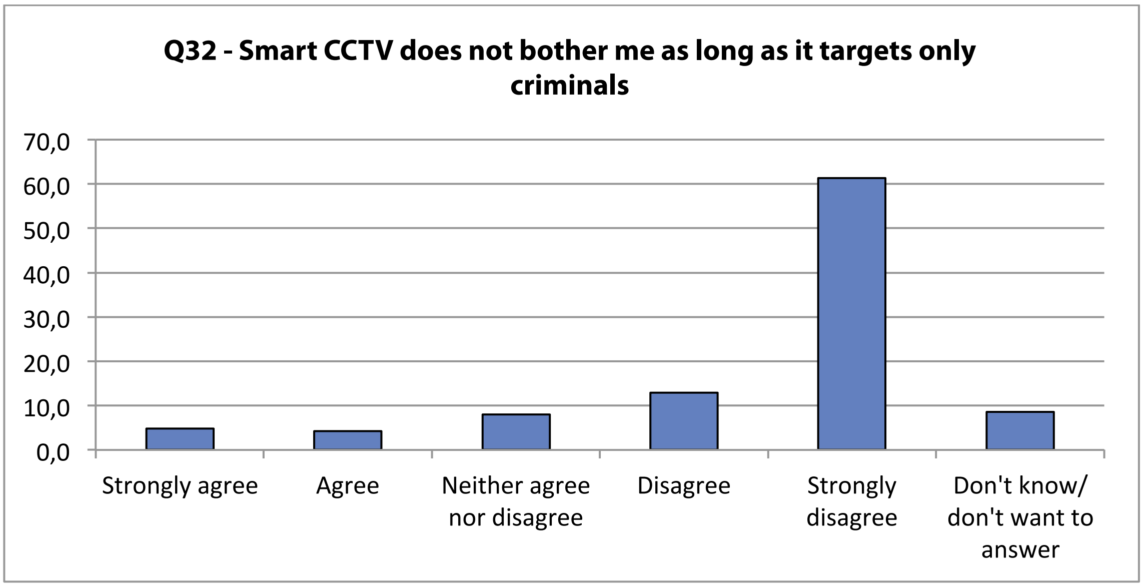


Figure 5: Impact of personal concernedness regarding Smart CCTV

In relation to those expressed insecurities or doubts regarding the effectiveness of Smart CCTV as security-enhancing measure, Q33 reveals that with 70.6%, most of the participants expressed worry about the future development of this SOST. A majority of citizens disagreed on being just concerned by Smart CCTV if it is used in the area where they live and work (Q34). There, an overall of 71.9% disagreed or even strongly disagreed with the given statement.

Beyond the citizen's general stance on the two SOSTS being used as security tools, the questionnaire also addressed the perceived intrusiveness of these, delving further into citizen's opinion whether they deem them useful as well (see table below).

**Q78 - Choose the options which better reflect your opinions (total of valid answers: N= 184)**

| | |
|---|---:|
| Smart CCTV is useful and not very intrusive | 8.7% |
| Smart CCTV is useful but highly intrusive | 28.8% |
| Smart CCTV is useless and highly intrusive | 54.9% |
| Smart CCTV neither useful nor intrusive | 1.1% |
| Don't know/don't want to answer | 6.5% |

Table 13: Perceived intrusiveness of Smart CCTV

Thereby, a large majority of citizens (54.9%,) found Smart CCTV useless as well as highly intrusive, whereas 28.8% perceive the technology as useful, but still highly intrusive. Only 8.7% fully agreed with the statement of Smart CCTV being useful and not very intrusive.

In the group discussion for Smart CCTV, citizens acknowledged that the visual surveillance of public spaces can provide some benefits. So for example, it was assumed that the observation of crime hotspots may have a deterring effect on individuals with criminal intent, thus this measure could be useful for crime prevention purposes. Also, the detection of dangerous objects by the enhanced functions of smart devices could support in securing of especially vulnerable places like airports or train stations. Furthermore, citizens said that eventually, the security in cases of large-scale public events could be supported to prevent accidents. One specific example mentioned several times where it was assumed by citizens that Smart CCTV could have helped with prevention was the crowd disaster at the Love Parade in Duisburg in 2010, where a mass panic of visitors caused the death of 21 people and several hundred getting injured. Beyond prevention, citizens said Smart CCTV could help in crime investigation, thereby the visual recordings providing possibly a higher success rate in investigations as well as more neutral evidence material than the statements of human witnesses. One middle-aged female citizen told about having a daughter who got stalked for some time and that she would have wished for more public space CCTV in fear for her safety. More positive aspects mentioned about Smart CCTV were that it could support security staff, reduce personnel costs, and limit human arbitrariness through its neutral algorithms providing the decision ground for security enhancing actions. Additionally, it was believed by the citizens that the technology, though still being fairly new, will get more reliable in short time and could support the most diverse purposes like intelligent traffic management including danger warnings, simplified procedures e.g. for levying toll charges or urban planning.

However, citizens also had some significant criticism related to Smart CCTV, as well as CCTV in general. While CCTV in the private sector is mainly perceived as effective e.g. against store theft (though being an endangerment for employees), citizens often doubted the effectiveness of governmental deployment against crime. Thereby it was assumed that criminals and terrorists could either circumvent or trick such systems. Other objections raised were that the technology is costly, crime spots just get relocated and police presence is reduced. The participants mainly voiced questions about which direct benefits the observation has for a victim the moment a crime really occurs and said that maybe increased presence of police staff in dangerous areas would make more sense instead of stronger camera surveillance. Furthermore, the summit participants fear that the noticeable surveillance diminishes civil courage of fellow citizens. Reasons for this might be people either perceiving an area safer due to the technology or just hoping that in case of an incident, the CCTV observation leads to security staff being called. Therefore, it was highly doubted that Smart CCTV could serve as prevention tool at all. Citizens also stated that the technology in general cannot fully replace the empathy, experiences and instincts of a police officer present in the area and that the technology cannot and should never have any crucial decision competence despite its "smart" algorithms.

Most prominently criticized with regard to Smart CCTV was the repudiation of the encompassing monitoring of citizens in public spaces, whereas the question if this causes a feeling of increased security or quite the opposite was subject of some controversy at the tables. Several times, the feeling of a panoptic setting was mentioned, and many citizens said they change their behaviour once they are aware of CCTV surveillance, up to the point of a chilling effect, e.g. at demonstrations. A focal point of criticism was the "smart" aspects of this technology mainly related to anomaly detection in human behaviour. Citizens expressed strong worries about who defines "normal" behaviour, reflecting on the societal impact of such definitions. Depending on how "abnormal" behaviour is defined, citizens are very concerned that the population may be subjected to an external pre-definition of new moral thresholds Citizens perceive the technology leaving increasingly less tolerance for atypical behaviour of any kind and that it might be prone to misjudgement. Thereby, there is some worry that this way, innocents become criminalized just because they do not fit the norm in behaviour, like minorities, children, or disabled people. Resulting of this, the participants assume that smart CCTV provides for some discrimination potential, as well as it may stigmatize individuals. This is explicitly said as a quite likely scenario once the visual data collected by the technology gets matched and linked to already existing information from various sources, like criminal data bases. One example mentioned was that of a former criminal who already served the sentence, where the facial recognition of Smart CCTV may lead to this person getting stigmatized, a fact which might endanger re-socialization and re-integration into society. Overall, the blanket surveillance through smart CCTV is perceived as a risk for the constitutionally guaranteed presumption of innocence and that it can be prone to misuse, for example to suppress dissenting political opinions. Mentioned several times in this context was the misuse of surveillance technologies by oppressive regimes like the Egyptian government during the Arab spring.

This misuse potential is also felt strongly due to perceived lack of transparency mostly regarding the scope of the data collection, the security of the data, the responsible entity, the time period of data retention and the purposes in general. One concern oftentimes mentioned was that the data collected may be stored for long time and used for other purposes than originally intended. Therefore, citizens repeatedly wished for more effective transparency measures and suitable control of governmental institutions using Smart CCTV.

As for Smart phone location tracking (SLT), the results yielded similar results, with only slight variations. 39.8% overall either disagree or even strongly disagree to the statement of SLT being an effective national security tool while only 27.4% agreed. In contrast to Smart CCTV, with a result of 32.3% on this option, an even larger number of participants were undecided on this statement.

In comparison to Smart CCTV, a significantly smaller overall percentage of 59.4% (33.2% strongly agree + 26.2% agree) stated that SLT would make them uncomfortable while only 23.5% disagreed on this statement. Correlating to this, 60.1% disagreed or even strongly disagreed that they would feel more secure due to the use of SLT. In this context, only 16.5% of the citizens overall agreed feeling more secure when this SOST is being deployed. Noticeable is the quite considerable number of participants (22.9%) who expressed undecidedness on this statement.

*Smart phone location tracking*

| | | | Strongly agree | Agree | Neither agree nor disagree | Disagree | Strongly disagree | N/A |
|---|---|---|---|---|---|---|---|---|
| | | **N** | **Percentages** | | | | | |
| SLT is an effective national security tool | Q27 | 186 | 11.8% | 15.6% | 32.3% | 21.5% | 18.3% | 0.5% |
| SLT makes me feel uncomfortable | Q28 | 187 | 33.2% | 26.2% | 17.1% | 13.9% | 9.6% | 0.0% |
| SLT makes me feel more secure | Q29 | 188 | 6.9% | 9.6% | 22.9% | 28.7% | 31.4% | 0.5% |
| Feeling that SLT is forced upon me without permission | Q30 | 187 | 60.4% | 21.4% | 7.5% | 2.7% | 7.0% | 1.1% |
| SLT appropriate way to address security threats | Q31 | 189 | 5.8% | 12.2% | 25.4% | 25.9% | 29.1% | 1.6% |
| SLT does not bother as long as it targets only criminals | Q38 | 184 | 13.0% | 8.7% | 9.8% | 19.0% | 42.4% | 7.1% |
| I worry how the use will develop in future | Q39 | 187 | 62.6% | 13.9% | 11.2% | 7.0% | 4.3% | 1.1% |
| SLT bothers only if it's used to track my own smartphone | Q40 | 185 | 5.4% | 4.3% | 7.0% | 11.4% | 66.5% | 5.4% |

Table 14: Perceived effectiveness of SLT

Just as for Smart CCTV, a rather high number of citizens (81.8% agree/strongly agree) perceive SLT as being forced upon them without their permission while only 9.7% do not seem to feel that way. In comparison to Smart CCTV, a smaller percentage of 55.0% expressed disagreement on SLT being an appropriate way to address national security threats. Moreover, 18.0% expressed agreement and still 25.4% were undecided in assessing if this SOST is suitable to address national security threats.

Compared to Smart CCTV, the SLT part yielded similar results regarding citizen's perceptions when the SOST targets only criminals. 61.4% strongly disagreed while 7.1% were undecided and 21.7% agreed on not being bothered in such a case. Likewise for Smart CCTV, a slightly higher number of citizens chose the do not know/want to answer option here with 7.1%.

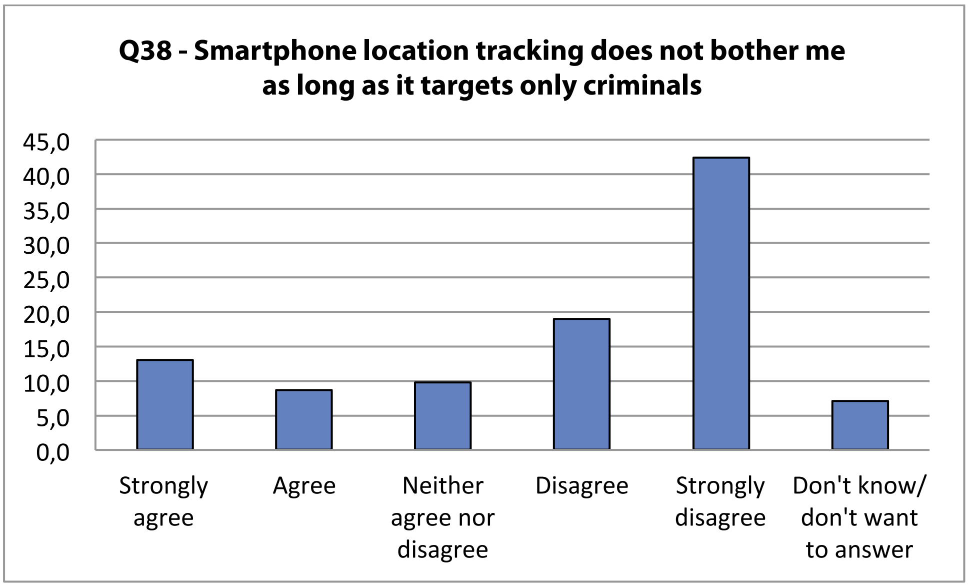


Figure 6: Impact of personal concernedness regarding SLT

With overall 76.5% in the strongly agree/ agree range, an even greater majority of citizens (in comparison to Smart CCTV) worry about the future development of SLT while 11.9% said they do not. Similarly to Smart CCTV, a high percentage of 77.9% would be bothered by SLT even it is not used in the area where they live and work. Only 9.7% said they would not be bothered in that case.

The opinion of citizens regarding the intrusiveness of SLT differs significantly from those concerning Smart CCTV (see table below).

**Q80 - Choose the options which better reflect your opinions (total of valid answers: N= 185)**

| | |
|---|---:|
| Smart phone location tracking is useful and not very intrusive | 13.0% |
| Smartphone location tracking is useful but highly intrusive | 56.2% |
| Smartphone location tracking is useless and highly intrusive | 23.2% |
| Smartphone location tracking neither useful nor intrusive | 1.1% |
| Don't know/don't want to answer | 6.5% |

Table 15: Perceived intrusiveness of SLT

Here, SLT is seen as mostly useful, but still highly intrusive (56.2%), while a smaller percentage of 23.2% deem the SOST as useless alongside the perceived high intrusiveness. Also, in comparison to Smart CCTV, a higher number of citizens (13.0%) acknowledge the technology as both useful and not very intrusive.

During the group discussions, the participating citizens said that they perceive Smartphone location tracking as effective mostly in individual cases for specifically tailored purposes. In the private sector, tracking functions can serve a multitude of convenience-enhancing purposes like navigation, location recommendation services, or the like. More focused on the governmental deployment of location tracking for security goals, examples were the locations of missed persons (like children, lost and helpless people like elderly or disabled ones). Also, the location of accident casualties or crime victims, targeted criminals, and stolen phones was mentioned. Furthermore, it was acknowledged that tracking could be useful in case of hazardous or very valuable goods. Beyond these oftentimes mentioned examples, some also said location tracking could help in the resolve of serial crime, serve as backing of findings in investigation cases, or even prove that someone originally assumed being at a certain crime location at some time is innocent.

But citizens also had some serious objections against the use of SLT as security measure. The effectiveness as preventive tool was doubted highly while regarding the information of an individual's location was deemed as having only limited usefulness in court since it could only serve as piece of circumstantial evidence. Generally, it was assumed that professional criminals can anticipate and circumvent/trick the deployment of SLT. The legal framework was sometimes perceived as insufficient and some wished for a more effective and competent application of judicial oversight.

Similarly to Smart CCTV, the broadness of the measure was criticized strongly. Especially the phone record collection of all people within the range of one cell tower was seen as disproportionate dragnet surveillance creating a general suspicion including many innocent people. In particular with regard to political demonstrations and the constitutionally manifested freedom of association, SLT is perceived as having a chilling effect installing a feeling of permanent surveillance and powerlessness. Mentioned oftentimes was the possibility of creating movement profiles of persons revealing intimate and sensitive details of the everyday life and social environment. In this context, the misuse potential was topic of many discussions, resulting of a strongly perceived lack of transparency regarding data collection, storage period, purposes and analysis criteria.

### 4.2.2 Avoidance, resistance against surveillance

The results of the citizen summit show a quite differentiated picture regarding the active challenging of SOST usage. In the context of Smart CCTV, the results of Q57 show that 20.1% of the citizens would campaign actively against the use of this SOST, while even 23.9% would use any means to prevent the deployment of this security measure. At least 10.9% would support others protesting against the use of Smart CCTV. However, a less direct approach against the technology, but rather a defensive stance was also expressed by a large number of citizens - 33.7% of the participants said they would like to find out more how to protect their privacy with regard to Smart CCTV. Only 8.7% of the citizens said they do not oppose the use of Smart CCTV at all. In the context of Smart phone location tracking, the answers given for Q59 show that 17.1% would campaign actively against SLT. And 19.3% would even use any means to prevent the use of SLT. 10.5% would support others protesting against its use. In comparison to Smart CCTV, an even larger majority of 40.9% would like to know more how to protect their privacy, presumably, directly on their own devices. Only 8.8% of the citizens said they do not oppose SLT at all.

At the German citizen summit, the participants were also asked in the context of Smart CCTV and SLT, if they would actively try to avoid being observed or tracked by these surveillance-oriented technologies (Smart CCTV = Q60 and SLT = Q62). A considerable number of citizens said they would change their behaviour when they were aware of these surveillance technologies being applied. This stance was expressed regardless which of the two SOSTs were addressed, thereby showing a 31.3% result for Smart CCTV and 38.0% for SLT. Still, in the case of Smart CCTV, a large number of the citizens said the surveillance of public space by Smart CCTV would not or even definitely not cause them to change their behaviour (overall 39.6%). But 23.1% said they would instead avoid going into areas where this kind of visual surveillance is deployed. Only a very small number of citizens (1.6%) said they would never go into areas where Smart CCTV is used. Similar numbers shows in the case of SLT where overall 34.2% of the citizens said they would not or even definitely not change their behaviour because of this SOST. However, 13.6% would actively try to avoid using a smartphone because of SLT, and even 8.2% would not use such a device at all due to this measure. This results in an overall 21.8% of citizens who are hesitant to use mobile devices in awareness of the possibility of being located and tracked.

During the group discussions, it became apparent that mostly the younger participants are quite well versed in using modern technologies like the internet or smartphones. This even encompasses relatively detailed knowledge about the ways private companies as well as governmental institutions perform personal data collection and surveillance for the most different purposes. However, those young people also admitted that by being native users of those technologies, they became used to the feeling of being observed, surveilled, and judged on the basis of the personal data they reveal either willingly or by lack of choice. In one case, a young woman said she feels used to the atmosphere of governmental surveillance since she grew up in the former GDR and her parents were observed by the secret service Stasi for some time and files existed about them. With the background of Germany's historical experiences stemming from the Nazi regime and the GDR, mostly the older citizens are more reluctant to accept SOSTs. Consequently, primarily the older citizens present at the summit said that they actively avoid of modern technologies generally, even though it was admitted that they can be convenient sometimes. In some cases, citizens even said they stopped using those technologies due to the vast data collections possible with which they felt uncomfortable. Some few citizens stated: “He who does nothing wrong would have nothing to fear from surveillance.” But the majority of the participants disagreed with such a statement and said everyone who is innocent could unwillingly become the target of surveillance.

### 4.2.3 Perceptions of individual and collective aspects

In this section, the concerns from a personal point of view as well as from a more collective or societal view are focus of the results evaluation. In general, it can be said that privacy as term as well as comprehensive concept can have an entirely different meaning to many citizens. Where some may see privacy as a concept meant to merely focus on the protection of the individual, some may take a broader perspective, assuming a greater societal value beyond the individual control over the own personal information. Anyway, aside from the impact of data collection through surveillance-oriented security technologies, the opinions expressed on the usage purposes and abuse potential of these (see table below) show that the citizens have a quite differentiated view of the matter.

| | | | Strongly agree | Agree | Neither agree nor disagree | Disagree | Strongly disagree | N/A |
|---|---|---|---|---|---|---|---|---|
| | | **N** | **Percentages** | | | | | |
| Use of SOSTs improves national security | Q84 | 180 | 5.6% | 10.0% | 32.8% | 26.7% | 25.0% | 0.0% |
| SOSTs only used to show something is done to fight crime | Q85 | 182 | 14.3% | 20.9% | 18.1% | 20.9% | 21.4% | 4.4% |
| If you have done nothing wrong, you don't have to worry about SOSTs | Q86 | 185 | 5.4% | 5.9% | 8.1% | 14.1% | 64.3% | 2.2% |
| If SOST is available, national governments make use of it | Q87 | 182 | 70.3% | 17.6% | 9.3% | 1.1% | 0.5% | 1.1% |
| Once SOSTs are in place, they are likely to be abused | Q88 | 185 | 56.2% | 27.6% | 10.3% | 4.3% | 0.0% | 1.6% |
| SOSTs should be routinely implemented to improve national security | Q94 | 183 | 8.7% | 11.5% | 19.1% | 22.4% | 37.7% | 0.5% |

Table 16: Stance on technology in general

The results show that a vast majority believes that surveillance technology is used by governments if it is available (87.9% share this opinion). However, 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. When comparing the results of Q94 in the table above and the results of the correlating earlier question Q7 (9.4% strongly agree and 14.4% agree to the question that security technologies should be used to improve national security, see chapter 4.1), it can be seen that overall, the support of SOSTs as a standard tool for security purposes is low and significantly dropped further during the citizen summit. So the participating citizens took an even more critical stance on SOSTs after having the opportunity of focusing on the several aspects of this topic through the information material, the films, and the group discussions. Notable is the expectation of technology abuse being rather high with 83.8% (agree/strongly agree) while the assessment regarding the potential for security improvement is quite adversely with 51.7% on the disagreement scale. This shows that the citizens have a quite differentiated view regarding the technologies themselves. It seems that citizens see security technologies as per se a neutral tool, equipped with the potential to be utilized for both good and inappropriate purposes. This impression is further supported by the opinions expressed during the group discussions.

During the discussions, it was pointed out that the German government is obliged to protect privacy/liberty as well as security in the country whereas the former matters have been neglected too much for some time. It is perceived that politicians generally concentrate too strongly on the aspect of national security, thereby focusing on issues in fact much less risky than they are portrayed in the politics and media. An example was made with politicians oftentimes focusing more on the dangers of severe crime and terrorism, while traffic accidents and climate change would provide much higher security risks to German citizens. In general, citizens said that policy makers and other stakeholders rely too much on the vague promises of modern technology without scientific backing while it was criticized that the security technology industry has a too powerful lobby in the German government.

Regarding perspectives on the personal privacy impact vs. the more general, societal consequences of such technologies, the citizens had a significantly multi-layered view as well. Considering the results of the questions addressing this issue, it seems obvious that while citizens often feel concerned by SOSTs on a personal level, they take a more comprehensive stance with regard to the impact of surveillance on the German population as such (see table below).

| | | | Strongly agree | Agree | Neither agree nor disagree | Disagree | Strongly disagree | N/A |
|---|---|---|---|---|---|---|---|---|
| | | **N** | **Percentages** | | | | | |
| I am concerned that too much information is collected about me | Q89 | 183 | 71.0% | 14.2% | 7.7% | 4.9 % | 1.1% | 1.1% |
| I am concerned that information about me may be inaccurate | Q90 | 181 | 37.6% | 20.4% | 19.3% | 9.4% | 5.5% | 7.7% |
| I am concerned that my personal information may be shared without my permission | Q91 | 178 | 83.7% | 8.4% | 5.6% | 1.1% | 0.6% | 0.6% |
| I am concerned that my personal information may be used against me | Q92 | 183 | 57.9% | 21.9% | 8.7% | 7.1% | 2.2% | 2.2% |
| I am concerned that the use of SOSTs is eroding privacy in general | Q95 | 182 | 63.7% | 15.4% | 8.8% | 6.0% | 4.4% | 1.6% |
| I am concerned that the use of SOSTs is eroding my privacy | Q96 | 183 | 65.0% | 16.4% | 7.1% | 7.1% | 3.8% | 0.5% |

Table 17: Individual and general concerns

These results reveal some differences in the assessment of personal privacy threats in contrast to privacy as a common and societal concept. The privacy issues of SOSTs in the individual sphere trigger some considerable concerns. But it also becomes obvious that the direct comparison of personal and general impact show slightly higher concerns related to the erosion of privacy for the commonality (79.1% vs. 81.4% on the strongly agree/agree range).

Broken down to the level of the individual SOSTs addressed at the citizen summit, the opinions linked to Smart CCTV as already shown in table 12 under chapter 4.2.1 express some worry of being affected by the technology on a personal level, mostly depending on the focus of the measure on specific targets and the areas where it is deployed. However, this worry does seem not entirely restricted to personal concernedness.

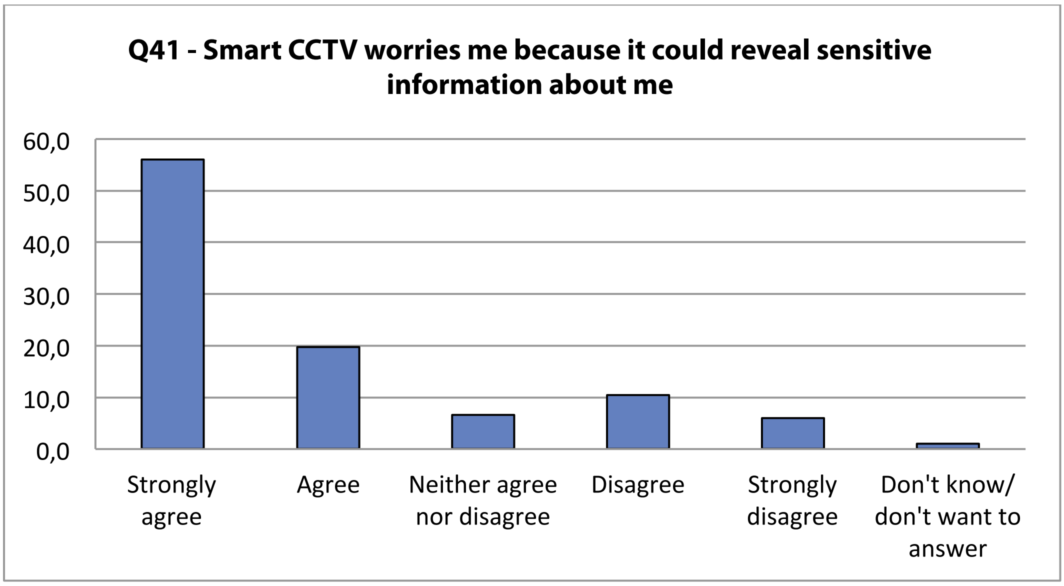


Figure 7: Concerns related to sensitive information disclosure

Furthermore, the figure above and the table below indicates that citizens worry about the sensitivity of the information that could be revealed about them, the potential misinterpretation of their behaviour, and the possible impact of Smart CCTV for their own human rights.

| | | | Strongly agree | Agree | Neither agree nor disagree | Disagree | Strongly disagree | N/A |
|---|---|---|---|---|---|---|---|---|
| | | **N** | **Percentages** | | | | | |
| Smart CCTV worries me because it could reveal sensitive information about me | Q41 | 182 | 56.0% | 19.8% | 6.6% | 10.4% | 6.0% | 1.1% |
| Smart CCTV worries me because it could let strangers know where I am | Q42 | 185 | 59.5% | 19.5% | 8.6% | 7.6% | 2.2% | 2.7% |
| Smart CCTV worries me because it could result in my behaviour being misinterpreted | Q43 | 186 | 68.3% | 11.3% | 7.0% | 7.5% | 3.8% | 2.2% |
| Smart CCTV worries me because it could violate my fundamental human rights | Q44 | 182 | 63.7% | 11.0% | 8.8% | 7.1% | 7.1% | 2.2% |
| Smart CCTV worries me because it could violate everyone's fundamental human rights | Q45 | 180 | 64.4% | 15.0% | 7.2% | 6.7% | 5.0% | 1.7% |

Table 18: Smart CCTV – sensitive information, behaviour interpretation & human rights concerns

And yet, the concerns related to the collective aspects receive even stronger attention by the citizens, which shows in the deviating percentages emerging from the answers to Q44 and Q45. While 74.7% of the citizens worry about a negative impact of Smart CCTV on their fundamental human rights, the number is with 79.4% even higher when the rights of fellow citizens are affected.

The results related to Smartphone location tracking allow for a similar evaluation. Already in the tables 14 and 15 under chapter 4.2.1, the infringement on personal privacy of this technology was seen as considerable but collective aspects played a role as well. Especially significant is the uneasiness with SLT despite the possible assumptions of criminals being the specific targets only. Therefore, citizens obviously do not limit their concerns to situations where they would expect that their own phone is tracked. This is complemented by the concerns about SLT revealing sensitive information and the location of the citizens (see table below). Ultimately, there are also strong objections against SLT due to fear of possible behaviour misinterpretations. About 74.0% of the citizens worry that their behaviour may be subjected to misinterpretation when they are affected by SLT is being used by security agencies.

| | | | Strongly agree | Agree | Neither agree nor disagree | Disagree | Strongly disagree | N/A |
|---|---|---|---|---|---|---|---|---|
| | | **N** | **Percentages** | | | | | |
| Smartphone location tracking worries me because it could reveal sensitive information about me | Q52 | 187 | 52.9% | 20.3% | 14.4% | 7.0% | 5.3% | 0.0% |
| Smartphone location tracking worries me because it could let strangers know where I am | Q53 | 186 | 62.4% | 17.2% | 10.2% | 5.9% | 3.2% | 1.1% |
| Smartphone location tracking worries me because it could result in my behaviour being misinterpreted | Q54 | 185 | 55.1% | 18.9% | 10.8% | 8.1% | 5.4% | 1.6% |
| Smartphone location tracking worries me because it could violate my fundamental human rights | Q55 | 187 | 58.8% | 19.8% | 5.9% | 8.0% | 7.0% | 0.5% |
| Smartphone location tracking worries me because it could violate everyone's fundamental human rights | Q56 | 186 | 59.7% | 16.7% | 8.1% | 7.0% | 7.0% | 1.6% |

Table 19: SLT – sensitive information, behaviour interpretation & human rights concerns

The collective aspects are also apparent when it comes to the aspect of fundamental human rights on personal as well as on general level. However, in contrast to the results related to Smart CCTV, there are slight differences in the emphasis of collective aspects. While the concerns related to the societal impact are still strong (76.4%), the personal sphere appears slightly more important to citizens when it comes to SLT since the results show that 78.6% strongly agree or agree on worries related to impact on personal fundamental human rights. Still, and similarly to Smart CCTV, the critical stance of citizens is quite strong in both aspects.

Independently from the SOSTs, the group discussions evolved with regard to individual and collective aspects around the erosion of privacy on both levels. It was stated that a democratic state supporting the constitutional rights of its citizens must endure some degree of insecurity to maintain its nature. By vast dragnet surveillance activities of governmental institutions, the trust in the state would get undermined because citizens perceive themselves subjected to a blanket suspicion. Broad surveillance measures involving large parts of the population are seen as disproportionate function or mission creep. This would result in the factual erosion of innocence presumption as laid down in the German constitution. Consequently, citizens feel a chilling effect on their behaviour, deriving from the wish to be left alone. Many citizens at the summit said that they perceive the increasing use of new SOSTs as the rise of a big brother creating an atmosphere of mistrust already experienced in the German history.

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

As already elaborated above, the participants of the citizen summit expressed highly critical opinions regarding the level of intrusiveness for the SOSTs discussed at the event. But still, these technologies were in principle seen as neutral means eventually suitable to achieve security improvements, whereas there is some misuse potential. Therefore, it became clear that the way these technologies are used is a crucial factor of acceptance. Consequently, the trustworthiness of the authorities deploying such security technologies is one key aspect. The usage purposes, scope and means of realization regarding the utilization of such security measures are arguments citizens closely scrutinized to determine the benevolence and competence of the governmental entities entrusted with the security of the German population.

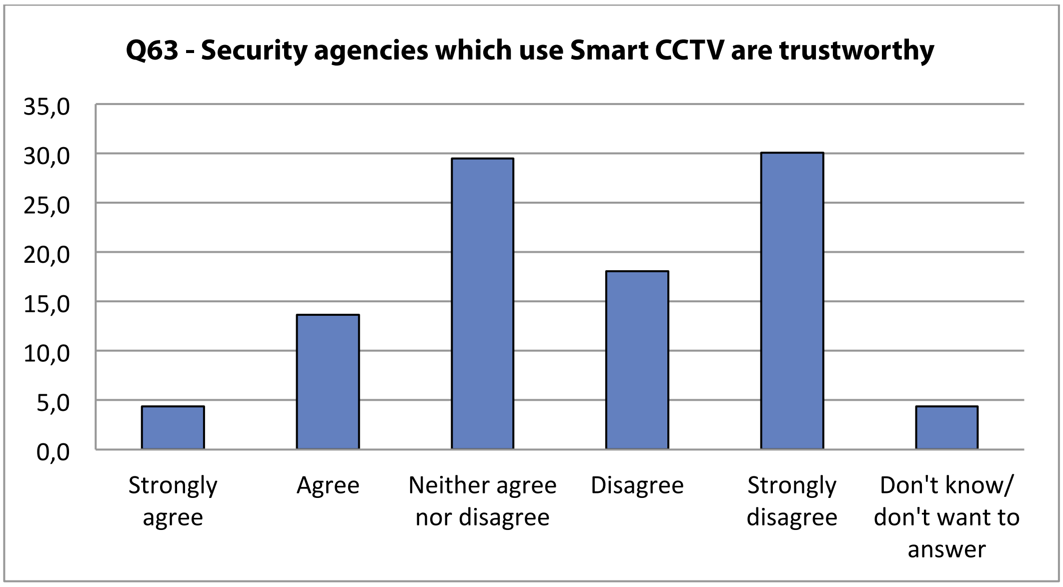


Figure 8: Perceived trustworthiness of institutions deploying Smart CCTV

So focusing on the SOSTs discussed, citizens expressed some doubts regarding trustworthiness, and competence of security agencies deploying them. With regard to Smart CCTV, only 18.1% strongly agreed or simply agreed that security agencies using them are considered trustworthy. Overall, the "Neither agree nor disagree" as well as the "Strongly disagree" positions almost hold a balance. The figure above visualizes this ambivalence citizens feel regarding the trustworthiness of governmental institutions tasked with the deployment of CCTV surveillance. This ambivalence underlines that trustworthiness seems to be a very important issue to the citizens. Even less agreement rates resulted during the assessment of competence, whereas just 9.9% of the citizens believe governmental security agencies being competent at using this technology.

| | | | Strongly agree | Agree | Neither agree nor disagree | Disagree | Strongly disagree | N/A |
|---|---|---|---|---|---|---|---|---|
| | | N | Percentages | | | | | |
| Security agencies which use Smart CCTV are trustworthy | Q63 | 183 | 4.4% | 13.7% | 29.5% | 18.0% | 30.1% | 4.4% |
| Security agencies which use Smart CCTV are competent at what they do | Q64 | 181 | 2.2% | 7.7% | 32.6% | 24.9% | 26.0% | 6.6% |
| Security agencies which use Smart CCTV are concerned about the welfare of citizens as well as national security | Q65 | 183 | 5.5% | 19.1% | 31.1% | 16.9% | 21.3% | 6.0% |
| Security agencies which use Smart CCTV do not abuse their power | Q66 | 182 | 4.9% | 11.0% | 25.8% | 18.7% | 34.1% | 5.5% |

Table 20: Trustworthiness of security agencies in the context of Smart CCTV use

But even going beyond trustworthiness in general and the ability of using this technology in the proper way, the results reveal a deep mistrust in the benevolence of German security agencies wanting to utilize surveillance-oriented measures. Less than a quarter of the participants (24.6% on the strongly agree/agree range) believe that the intention of such agencies is focused on the welfare of citizens and national security. In contrast, the risk of misuse is rated fairly high. More than half of the number of citizens (overall 52.8%) thinks that security agencies eventually abuse the power this technology gives them.

**Q75 - Choose the options which better reflect your opinions**

**(Several answers possible, total of valid responses without counting the single selections: N= 176)**

| | |
|---|---|
| Laws and regulations ensure that Smart CCTV is not misused | 13.6% |
| I believe that Smart CCTV improves national security | 35.2% |
| I believe that Smart CCTV is intrusive | 84.7% |
| I think that the level of intrusiveness is acceptable given the benefits smart CCTV offers | 23.3% |
| None of the four listed in case of Smart CCTV | 1.7% |
| Don't know/don't want to answer | 1.7% |

Table 21: „Opinions on Smart CCTV"

This apparent mistrust in governmental security agencies does not even seem to be diminished by some faith in legal restraints intended to regulate the use of SOSTs as well as factual benefits do not. While only 13.6% of the citizens believe that laws and regulations are fit to limit misuse possibilities, a large number (84.7%) strongly focus on the intrusiveness of the measure. Still, some citizens (35.2%) acknowledge the potential of Smart CCTV to improve security. But taking the overwhelming perception of intrusiveness into account, only 23.3% deem this usefulness as enough to accept this technology as standard security measure.

| | | | Strongly agree | Agree | Neither agree nor disagree | Disagree | Strongly disagree | N/A |
|---|---|---|---|---|---|---|---|---|
| | | **N** | **Percentages** | | | | | |
| Overall I support the adoption of Smart CCTV as a national security measure | Q81 | 182 | 5.5% | 8.2% | 19.8% | 17.0% | 48.4% | 1.1% |

Table 22: General support of Smart CCTV as security solution

This results in a quite low level of support for Smart CCTV as a security solution with a rate of 13.7%. In comparison to Smart CCTV, the results related to the SOST Smartphone location tracking show a slightly more positive attitude towards security agencies, whereas the overall results are show a still low-tuned sentiment of citizens related to that matter (see table below).

| | | | Strongly agree | Agree | Neither agree nor disagree | Disagree | Strongly disagree | N/A |
|---|---|---|---|---|---|---|---|---|
| | | **N** | **Percentages** | | | | | |
| Security agencies which use smartphone location tracking are trustworthy | Q71 | 185 | 7.6% | 14.1% | 35.7% | 18.4% | 21.1% | 3.2% |
| Security agencies which use smartphone location tracking are competent at what they do | Q72 | 185 | 4.9% | 7.6% | 29.2% | 26.5% | 25.4% | 6.5% |
| Security agencies which use smartphone location tracking are concerned about the welfare of citizens as well as national security | Q73 | 186 | 5.4% | 20.4% | 32.3% | 21.5% | 14.5% | 5.9% |
| Security agencies which use smartphone location tracking do not abuse their power | Q74 | 185 | 5.9% | 11.9% | 23.8% | 25.9% | 28.6% | 3.8% |

Table 23: Trustworthiness of security agencies in the context of SLT use

About 21.7% believe security agencies using SLT being trustworthy, while a lower number of 12.5% believe in the general ability to handle this field of technology competently. Concerning SLT, the trust in the good intentions of governmental security agencies is a bit higher as for Smart CCTV (here 25.8%) but yet not quite high overall.

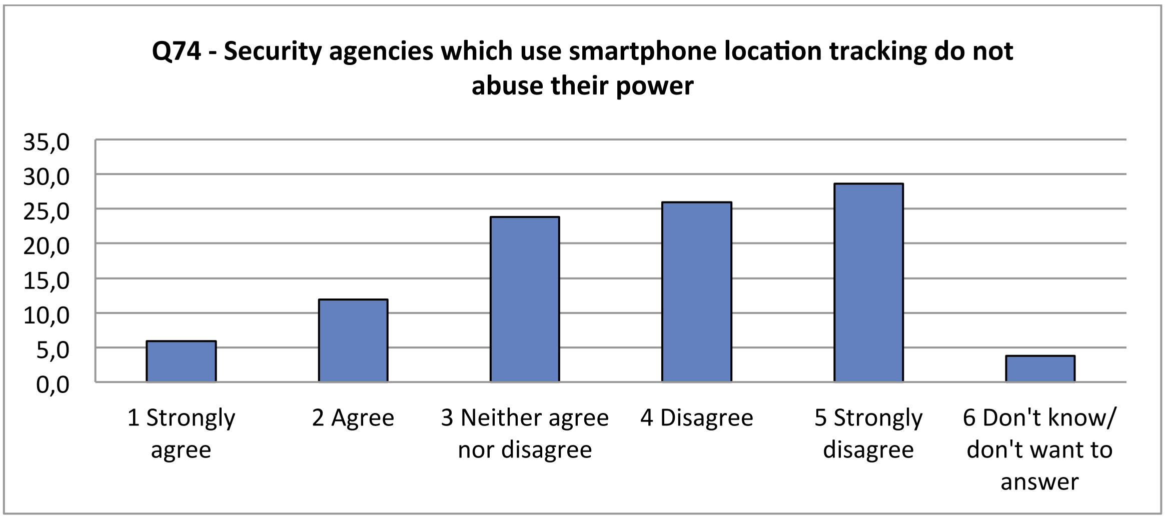


Figure 9: Perceived potential of SLT abuse

The risk of misuse was rated higher in the context of SLT than for Smart CCTV with a rate of 54.5%. This stands in notable contrast to the higher belief in the good intentions of governmental security institutions. While the reason for this is not entirely clear, this difference might be explained by citizens eventually taking into account unintentional mistreatment of personal data obtained through smartphone location tracking. However, 54.5% of the responding citizens seem to fear abuse of power when it comes to the question of Smartphone location tracking. 23.8% of the participants still seem to be quite uncertain how to assess this question. These results allow the assumption that regarding the question of SLT abuse, citizens feel a high amount of uncertainty regarding the issue of trust.

**Q77 - Choose the options which better reflect your opinions**

**(Several answers possible, total of valid responses without counting the single selections: N= 171)**

| | |
|---|---|
| Laws and regulations ensure that smartphone location tracking is not misused | 14.6% |
| I believe that smartphone location tracking improves national security | 33.9% |
| I believe that smartphone location tracking is intrusive | 86.5% |
| I think that the level of intrusiveness is acceptable given the benefits smartphone location tracking offers | 25.7% |
| None of the four listed in case of smartphone location tracking | 3.5% |
| Don't know/don't want to answer | 0.0% |

Table 24: „Opinions on smartphone location tracking“

Taking the legal frameworks applicable and the factual benefits of SLT into account, the results are fairly similar compared to Smart CCTV, with only a slightly more positive stance. About 14.6% voiced their belief that laws and regulations can prevent misuse and 33.9% think SLT can improve national security. Yet, an even higher number (here 86.5% in comparison to 84.7% for Smart CCTV) deem the tracking of mobiles as intrusive. Balancing benefits and drawbacks, just over a quarter of citizens (25.7%) find the intrusiveness acceptable.

| | | | Strongly agree | Agree | Neither agree nor disagree | Disagree | Strongly disagree | N/A |
|---|---|---|---|---|---|---|---|---|
| | | **N** | **Percentages** | | | | | |
| Overall I support the adoption of Smartphone Location Tracking as a national security measure | Q83 | 186 | 8.1% | 12.4% | 18.3% | 20.4% | 39.8% | 1.1% |

Table 25: General support of SLT as security solution

In the end, SLT is supported by about 20.5% of the citizens to be used routinely as a national security measure. Overall, it can be said that citizens are quite wary of surveillance-oriented security technologies being used by governmental institutions, even though their potential of effectiveness is acknowledged partially. Citizens seem to feel that the possible benefits do not outweigh the perceived infringement on personal as well as everyone's privacy.

In the group discussions, citizens said they trust German politicians and governmental institutions to some extent with solely national security matters. But this trust is less strong once foreign police and intelligence services are involved. Adding up to this, the already sparse trust was diminished further since the NSA scandal. During the summit, some citizens expressed deep disappointment with German government reacting only cautiously to the all-encompassing infringement of German citizen's privacy. Furthermore, the public-private partnership for security purposes is seen critically since it transfers the state's governance monopoly to private companies. Because the collection of personal data is ever-increasing in both the private sector (for commercial purposes) and on governmental side, citizens starkly feel powerless and exposed to the market power of companies and the privacy-infringing possibilities modern technologies provide. But even with solely governmental activities with good intentions for security purposes, citizens do not always trust that the outcome might be beneficial to the German population. The misuse potential is generally rated high, and even though there is trust in the current government, citizens see the possibilities of future abuse by oppressive regimes.

To enhance the trustworthiness of security agencies, citizens deem a higher level of transparency and independent controls as important factors. Checks and balances were mentioned often as chances to regain citizen trust in the competence and benevolence of German security institutions. This includes a clear, honest effectiveness evaluation of the technology as well as a reliable legal framework involving productive means of enforcement. Thereby, the summit participants noted several times that a solely national solution might be insufficient. Rather, German politicians should strive for comprehensive European solutions respecting the high level of civil rights protection in Germany compared to some other EU countries. Thereby, it becomes necessary to catch up with the technical development and to shape the knowledge of German officials entrusted with security policy making.

Moreover, Privacy by Design (PbD) was mentioned sometimes in the table discussions as an approach to prevent the misuse of SOSTs. Examples for such PbD measures are technical means to reduce data collection to the level necessary to achieve the security purpose, the fostering of anonymity online, and the support of open source software. In general, citizens feel more confident once the technology is designed in a way which does foster a privacy-friendly use, or even hinders misuse.

Aside from these quite specific aspects and on a more universal notion, citizens often and intensively expressed their wish that German government officials would grant a stronger support for a shift further away from technology-centred security solutions. As already elaborated above, citizens explicitly miss the human factor when it comes to possible countermeasures against risks to national security. Also, it was said that usually, the specific frame conditions and the pre-settings of the individual cases matter when considering the deployment of surveillance-oriented security technologies.

This also shows in the results when citizens were asked about non-technological alternatives. While at the beginning of the summit, citizens already said they would wish for a stronger focus on alternative approaches (70.9% on the strongly agree/agree range, see the results for Q10 in the table below), at the end of the day this stance became even stronger among the participants.

About 76.6% of the citizens strongly agreed or simply agreed on the statement that alternative approaches to resolve security issues should be given higher priority, which shows a clear increase.

| | | | Strongly agree | Agree | Neither agree nor disagree | Disagree | Strongly disagree | N/A |
|---|---|---|---|---|---|---|---|---|
| | | **N** | **Percentages** | | | | | |
| Alternative approaches to security which do not involve surveillance-oriented security technologies should be given higher priority | Q10 | 186 | 47.8% | 23.1% | 19.9% | 4.8% | 2.2% | 2.2% |
| Alternative approaches to security which do not involve surveillance-oriented security technologies should be given higher priority | Q97 | 179 | 59.8% | 16.8% | 15.1% | 4.5% | 2.2% | 1.7% |

Table 26: Prioritization of alternative (non-technological) approaches

Thereby, the most significant shift or change in opinion throughout the day was from the number of undecided participants who in the later question tended more towards the non-technological solutions. This correlates with the above mentioned disagreement of citizens on the statement that SOSTs should be routinely implement as security solutions (see the results to Q7 and Q94 in the chapters 4.1 and 4.2.3).

At the tables, citizens gave some examples of alternative approaches, such as the investment in more police staff, non-technological crime prevention approaches, political and factual solutions to reduce poverty, and more education. In general it was said that it could be worth to investigate even more possibilities in that direction which might be suitable to bring relief on security issues in Germany.

## 4.4 Citizens' recommendations to policy makers

At the various tables at the citizen summit, the participants had the opportunity to formulate one recommendation per table which is addressed at policy makers on European as well as national level. With regard to the quantitative results, the recommendations were largely in tune with the opinions and concerns raised throughout the whole day of the citizen summit, addressing the core worries of citizens with regard to privacy, security and surveillance-oriented security technologies.

In general, the citizens had little difficulty in finding to an agreement on one recommendation for their table. In some cases, citizens felt that just one recommendation per table was not sufficient enough. Those citizens had the opportunity to use little postcards as an additional way to express further aspects not entailed in the recommendations. Many citizens took advantage of this opportunity. The translated text of the recommendations in detail as well as the postcards can be found in the annex of this document.

Throughout the day of the citizen summit, citizens had voiced miscellaneous concerns related to privacy, security, and SOSTs. Main concerns expressed were a strongly perceived infringement on human rights through the increasing use of surveillance-oriented security measures, as well as lack of transparency, effective oversight and control of SOST-deploying security institutions. The majority of citizens felt that they had little to no influence on policy maker's actions with regard to data protection and the use of surveillance technologies. Many times throughout the day, citizens said they feel exposed to vast surveillance by national as well as foreign governments. Consequently, with their recommendations, citizens first and foremost demand less surveillance. Furthermore, they demand meaningful transparency in favour of European citizens, e.g. by proactive information and objective evaluation in which cases surveillance for security purposes may be necessary and proportionate. This also entails a genuine scrutiny of SOST efficiency and its impact on society. Moreover, citizens demand effective control of SOST-deploying security agencies by suitable organizational, technical and legal means.

It was acknowledged that sometimes the use of surveillance technology could be necessary. But according to the citizens, this should always be considered on a case to case basis backed by objective and comprehensive evaluation. So a crucial point repeatedly addressed in the group discussions as well as in the table recommendations was the urgent need for more transparency in security policies. According to the citizens, this transparency should entail at minimum information about source, scope and purpose of personal data collection, means of data processing, retention period, and the entities involved in the process.

Aside from transparency as a mandatory pre-condition to be served prior to the deployment of SOSTs, citizens heavily criticized the often unconditional faith in technology as the resolve of all security problems. Therefore, the summit participants suggested to security policy makers within Europe to shift their focus more towards a meaningful, objective technology effectiveness and impact evaluation as well as to take alternative methods to resolve security issues into account. Several times, it was mentioned that many security matters in the criminal field have their cause in poverty, lack of education and other social inequalities. So already during the group discussions, suggestions were made to address these issues directly. Examples were mentioned like the improvement of education or social programs. Beyond going to the root of why people become criminals, it was suggested that instead of deploying more surveillance-focused technology, the staffing of the police and other security agencies should be improved. Overall, main objective of citizens present at the summit was stronger human factor in addressing security challenges and correlating to this demand, several recommendations entail this aspect as well.

Furthermore, recommendations addressed the need for a comprehensive legal framework going beyond the restrictions of national borders to ensure that constitutionally guaranteed human rights are enforced more effectively. The most frequently named recommendation was the establishment of a harmonized, international (at least EU-wide) legal framework for the effective protection of personal data. As reason for that demand, citizens said that in the digital age where personal data is often collected, transferred and shared across borders routinely, mere national solutions aren't sufficient anymore. For the demand of a comprehensive and internationally applicable data protection framework, the participants of the summit wished for the German data protection law setting a minimum standard on the protection of citizen's privacy. Moreover, the new legal framework should provide well defined preconditions for the deployment of surveillance technologies including practical control and sanction mechanisms. Such mechanisms could be realized organisationally, for example through the establishment of an independent data protection authority on European level which is addressable by every citizen and empowered with instructive authority towards governmental and private entities in Europe. For this supervisory authority being able to effectively safeguard citizen’s privacy, it would have to be equipped adequately in regards to financial and material resources. But aside from organizational means of control, technical solutions were also mentioned in recommendations by the demand to take Privacy by Design approaches and research better into account. With such solutions, so the expectation of citizens, a violation of privacy would not be possible right from the start. Another aspect mentioned for a comprehensive legal framework in Europe is the further strengthening of citizen's right to get informed once concerned personally.

# 5 Summary and Conclusions

In Germany, the historic experiences from the Nazi regime and the later SED dictatorship in the GDR have sustainably shaped citizens view on governmental power, surveillance and security. The oppressive activities in the eras of the past left a noticeable imprint on part of the German society, resulting in mistrust towards security institutions, especially intelligence agencies. The spying on a large part of the German population during these periods in history is still perceived as having an ultimately destructive effect on societal cohabitation as well as on the constitutionally guaranteed human rights of individuals.

To some extent, this mistrust has diminished a bit in the last decades, leaving room for a stronger demand regarding national security. This resulted in a shift of focus by security agencies towards more pre-emptively oriented activities and measures. This focus of governmental security policy in Germany was even sharpened by the terrorist attacks of September 2001 which resulted in a significantly increased acceptance of intensified security measures by the country's population. But still, German citizens in principle maintained their critical stance on surveillance as security approach, while shock and fear triggered by terroristic activities like 9/11 or Madrid wore off to some extent. Already prior to the so-called NSA-scandal, the direct effects as well as the indirect, not immediately recognizable implications of rising surveillance technologies was repeatedly discussion subject in the public discourse of society, media and politics. Since the Snowden revelations, an on-going public debate focuses on the consequences of global surveillance undermining human rights and civil liberties worldwide. While the impact on citizen's daily life is often not directly recognizable, the indirect effect on personal privacy and the societal implications increasingly come into the focus of media and politics. Vast, opaque data collections by security agencies, oftentimes ineffective judicial oversight, as well as the imbalance between extensive governmental security politics and democratic principles are the main subjects to growing public discourse.

At the German citizen summit, it became clear that citizens are aware that security measures, including SOSTs, are important under circumstances. However, they do not simply accept the privacy intrusions coming along with surveillance-based security measures. With regard to SOSTs, they view that these technologies entail considerable misuse potential reinforcing worries about future developments. Moreover, to some extent, citizens already doubt the effectiveness of the technology with regard to desired security enhancements. Overall, questionnaire results, group discussions, table recommendations, and the additional postcards give the impression that the citizens have a quite differentiated view on the topics addressed. They certainly acknowledge the purpose of achieving more security, taking into account their day to day experience with SOSTs and the question whether they are directly targeting criminals. But still, citizens also tried to take a more general view, also thinking about the indirect and long-term consequences of security measures. In doing so, it became apparent that the assumption of higher security risks automatically leading to increased acceptance of surveillance-oriented security technologies is false. In fact, the perceived infringement on citizen's rights was still weighted considerably more strongly by the summit participants than the potential benefit of the security measure in question. So regardless of the perceived effectiveness, a large number of citizens said they feel very uncomfortable with the deployment of surveillance technologies and do not necessarily feel more secure due to them being used.

Consequently, it cannot be assumed automatically that the effectiveness of a SOST or the personal concernedness can be single, stand-alone factors leading to technology acceptance. Rather, the classical trade-off assumption of people being willing to trade privacy and/or liberty for security does not work entirely. In fact, citizens have a multi-layered view on the matter, whereas the benefits do not automatically outweigh the drawbacks. There is a strong demand to genuinely analyse the implications of surveillance-oriented security technologies for the concerned individuals as well as for society in general.

In their recommendations to European security policy makers, citizens suggest several actions to be taken to resolve the issues aforementioned. Citizens demand with their recommendations:

- Less surveillance in general to reduce negative impact on privacy
- Create more transparency for European citizens
- Mandatory objective evaluations of SOSTs regarding
  - suitability,
  - necessity,
  - effectiveness,
  - and proportionality
- A harmonized international (at least EU-wide) legal framework not going below the level of protection on personal data as currently laid down in the German data protection law
- Effective means of control and enforcement

At this time, citizens sorely miss an objective, yet critical reflection on these matters by policy makers and security agencies. It can be presumed that this led to the quite blunt results on the trustworthiness of security institutions. These clearly show that citizens perceive the current security foci in Germany as too one-dimensional and unreflective with regard to individual as well as societal consequences of surveillance. During the event, citizens oftentimes relied on and referred to the historical experiences of the German population for exemplifying how official security policies can turn into mission creep and misuse of governmental power against the own citizens. Thus, it can be presumed that the better checks and balances are, the trustworthiness of institutions – as well as correlating, the acceptance levels regarding the use of SOSTs are. Still, the question of acceptance is a multi-dimensioned one for which citizens demand a careful balance of a SOST's benefits and its intrusiveness on citizen's lives. In that sense, citizens are not willing to unconditionally trade neither their personal privacy, nor the notion of privacy as all-encompassing societal concept in exchange for improvements in national security. Rather, they criticize the trade-off model as being too simplistic and demand balance between privacy and security. This includes the meaningful evaluation and permanent critical scrutiny of suitability, adequacy and proportionality of surveillance-oriented security measures going along with meaningful transparency and control on the side of the security institutions deploying them.

# 6 Bibliography

Alvares de Souza Soares, Philip, Spiegel Online, March 5th 2014, "Amtliche Spähsoftware: Staatstrojaner-Fiasko verbittert Polizisten": http://www.spiegel.de/netzwelt/netzpolitik/warum-es-bis-heute-keinen-staatstrojaner-gibt-a-956617.html

Arbeitskreis Vorratsdatenspeicherung, website information entry about the Federal Constitution Court complaint against the German implementation of the EU Data Retention Directive: http://www.vorratsdatenspeicherung.de/content/view/51/1/lang,de/%3E

Beckedahl, Markus, Netzpolitik.org, February 7th 2012, "Zwischenstand: 12 Millionen Funkzellenabfragen in Berlin": https://netzpolitik.org/2012/zwischenstand-12-millionen-funkzellenabfragen-in-berlin/

Berlin Administrative Court

- Decision of July 5th 2010, (Az. 1 K 905.09): http://www.gerichtsentscheidungen.berlin-brandenburg.de/jportal/?quelle=jlink&docid=JURE100068408&psml=sammlung.psml&max=true&bs=10
- Decision of April 26th 2012, (Az. Az. VG 1 K 818.09): www.gerichtsentscheidungen.berlin-brandenburg.de/jportal/?quelle=jlink&docid=JURE120017238&psml=sammlung.psml&max=true&bs=10

Berlin Data Protection and Freedom of Information Commissioner, report 3rd September 2012, „Abschlussbericht zur rechtlichen Überprüfung von Funkzellenabfragen": http://www.datenschutz-berlin.de/attachments/896/Pr__fbericht.pdf?1346753690

Biermann, Kai, Zeit Online article March 26th 2006, "Betrayed by our own data": http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz

Brinkmann, Bastian; Hollenstein, Oliver; Kempmann, Antonius, Sueddeutsche.de, November 16th 2013, "Was Spionagefirmen in Deutschland für die USA treiben": http://www.sueddeutsche.de/politik/amerikanische-auftragnehmer-was-spionagefirmen-in-deutschland-fuer-die-usa-treiben-1.1820034

Bundesministerium der Justiz (Federal Ministry of Justice), website entry June 10th 2011, "Quick-Freeze: Bundesjustizministerin legt Gesetzentwurf vor":

http://www.bmj.de/DE/Service/Newsletterversand/_doc/_inhalt/092011_001.html

Court of Justice of the European Union, judgment in joined Cases C-293/12 and C-594/12Digital Rights Ireland and Seitlinger and Others:

http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

Die Welt, November 13th 2011 "Friedrich spricht erstmals von "Rechtsterrorismus": http://www.welt.de/politik/deutschland/article13714953/Friedrich-spricht-erstmals-von-Rechtsterrorismus.html

Die Welt, June 22nd 2011, "EU leitet Verfahren gegen Deutschland ein": http://www.welt.de/politik/deutschland/article13443492/EU-leitet-Verfahren-gegen-Deutschland-ein.html

Ehrenberg, Markus, Der Tagesspiegel article published July 18th 2012, “Sinnvoll skandalös”: http://www.tagesspiegel.de/medien/datenschutz-sinnvoll-skandaloes/6888806.html

European Digital Rights, EDRI website entry about the German police increasingly using Silent SMS to locate suspects: http://www.edri.org/edrigram/number10.2/silent-sms-tracking-suspects

Fuchs, Christian; Goetz, John; Obermaier, Frederik, in Süddeutsche.de, article published September 13th 2013, "Verfassungsschutz beliefert NSA": https://web.archive.org/web/20131003031334/http://www.sueddeutsche.de/politik/spionage-in-deutschland-verfassungsschutz-beliefert-nsa-1.1770672

German Association of Towns and Municipalities together with the German Police Trade Union, position paper of January 27th 2014: " Sicherheit in Städten und Gemeinden – Positionspapier des Deutschen Städte- und Gemeindebundes (DStGB) und der Gewerkschaft der Polizei (GdP)"

German Bundestag, Printing matter 17/14600 August 22nd 2013, entailing the decision recommendation and concluding report of the 2nd NSU committee of inquiry, "Beschlussempfehlung und Bericht des 2. Untersuchungsausschuss es nach Artikel 44 des Grundgesetzes" (PDF-file): http://dipbt.bundestag.de/dip21/btd/17/146/1714600.pdf

German Federal Administrative Court, Decision of January 25th 2012, (Az. BVerwG 6 C 9.11): http://www.bverwg.de/enid/069768c9c3aa31f1baef81da1db91409,54e4b0736561726368f646973706c6179436f6e7461696e6572092d0931343036320 93a095f7472636964092d093133333430/Pressemitteilungen/Pressemitteilung_9d.html

German Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, BfDI), Tätigkeitsbericht (Bi-Annual Report) for the years 2011-2012: http://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/24TB_2011_2012.pdf?__blob=publicationFile

German Federal Constitutional Court

- Decision of 15th December 1983 (Az.: 1 BvR 209, 269, 362, 420, 440, 484/83):

https://openjur.de/u/268440.html

- Decision of 3rd March 2004, (Az.: 1 BvR 2378/98): http://www.bverfg.de/entscheidungen/rs20040303_1bvr237898.htmlDecision of 27th February 2008, (Az.: 1 BvR 370/07): http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html
- Decision of March 11th 2008, (Az.: 1 BvR 256/07): http://www.bundesverfassungsgericht.de/entscheidungen/rs20080311_1bvr025608.html
- Decision of April 24th 2013, (Az.: 1 BvR 1215/07): https://www.bundesverfassungsgericht.de/entscheidungen/rs20130424_1bvr121507.html

German Wikipedia, entry for the NSA scandal; subtitle "Basisdemokratische Initiativen" (Eng. Basic democratic initiatives): http://de.wikipedia.org/wiki/Globale_%C3%9Cberwachungs-_und_Spionageaff%C3%A4re#Basisdemokratische_Initiativen

Heise online, February 25th 2012, "Geheimdienste überwachten 37 Millionen Netzverbindungen": http://www.heise.de/newsticker/meldung/Geheimdienste-ueberwachten-37-Millionen-Netzverbindungen-1442867.html

Hunton & Williams LLP., Privacy and Information Security Law Blog, entry of July 7th 2011, "Germany Launches National Cyber Defense Center": http://www.huntonprivacyblog.com/2011/07/articles/germany-launches-national-cyber-defense-center/

Meiritz, Annett; Musharbash, Yassin; Weiland, Severin, in: Spiegel Online November 21st 2011, "Ermittlungspannen bei Neonazi-Mordserie: die Schuld der Behörden": http://www.spiegel.de/politik/deutschland/ermittlungspannen-bei-neonazi-mordserie-die-schuld-der-behoerden-a-799074.html

Mitteldeutsche Zeitung, August 3rd 2013, "Bundesanwaltschaft prüft Ermittlungen zur NSA-Affäre": http://www.mz-web.de/politik/bundesanwaltschaft-prueft-ermittlungen-zur-nsa-affaere,20642162,23903482.html

Müller, Thorsten, Bundeszentrale für politische Bildung (Federal Centre for political education), June 14th 2012, "Innere Sicherheit in der Europäischen Union": http://www.bpb.de/politik/innenpolitik/innere-sicherheit/76658/europaeisierung-von-innerer-sicherheit

Neumann, Linus, Netzpolitik.org, June 20th 2011, "Dresden: Demoüberwachung mittels Mobilfunknetz": https://netzpolitik.org/2011/dresden-demouberwachung-mittels-mobilfunknetz/

rbb-Kultursendung "Stilbruch" of August 15th 2013, titled "Freiheit im Internet": http://www.rbb-online.de/stilbruch/archiv/20130815_2215/freiheit-im-internet.html

Saxony Data Protection Commissioner, report over non-individualized cell tower inquiries and other means of telecommunication surveillance through police and prosecutors in Dresden in February 2011: http://www.saechsdsb.de/images/stories/sdb_inhalt/behoerde/oea/bericht-funkzellenabfragen.pdf

Scholz, Alexander, Searchlight magazine blog article published July 7th 2012, "Germany to tackle neo-Nazis with database": http://www.searchlightmagazine.com/news/international-news/germany-to-tackle-neo-nazis-with-database

Spiegel Online, May 10th 1971, "EDV im Odenwald": http://www.spiegel.de/spiegel/print/d-43176393.html

Spiegel Online (English news section), September 5th 2006, "Germany Agrees on Anti-Terror Database": www.spiegel.de/international/fighting-terrorism-germany-agrees-on-anti-terror-database-a-435244.html

Spiegel Online, August 31st 2011, „Flugsicherheit: Nacktscanner versagen im Praxistest": http://www.spiegel.de/reise/aktuell/flugsicherheit-nacktscanner-versagen-im-praxistest-a-783550.html

Spiegel Online, article of August 3rd 2013, "Überwachung: BND leitet massenhaft Metadaten an die NSA weiter": http://www.spiegel.de/netzwelt/netzpolitik/bnd-leitet-laut-spiegel-massenhaft-metadaten-an-die-nsa-weiter-a-914682.html

Tagesschau, report August 7th 2013, "BND-NSA-Kooperation: Streit über Steinmeiers Rolle": https://web.archive.org/web/20131004220036/http://www.tagesschau.de/inland/bndnsa102.html

The H Security blog, article published October 10th 2011, “CCC cracks government Trojan”: http://www.h-online.com/security/news/item/CCC-cracks-government-trojan-1357755.html

The H Security blog, article published October 26th 2011, “CCC criticizes new version of government Trojan”: http://www.h-online.com/security/news/item/CCC-criticises-new-version-of-government-trojan-1367160.html

The H Security blog, article published September 11th 2012, “Federal Commissioner unable to audit Federal Trojan source”: http://www.h-online.com/security/news/item/Federal-Commissioner-unable-to-audit-Federal-Trojan-source-1704460.html

Vensky, Hellmuth, Zeit Online July 9th 2012, “Die Fallstricke der Facebook-Fahndung”: http://www.zeit.de/digital/datenschutz/2012-07/facebook-fahndung-hessen

Zeit Online, January 14th 2014, " De Maizière sieht Deutschland gleich mehrfach bedroht": http://www.zeit.de/politik/deutschland/2014-01/de-maiziere-gefahren-terrorismus

Zeit Online, February 28th 2014, "Steinmeier rückt von Anti-Spionage- Abkommen ab": http://www.zeit.de/politik/ausland/2014-02/usa-kein-no-spy-abkommen

# 7 List of Figures

# 8 List of Tables

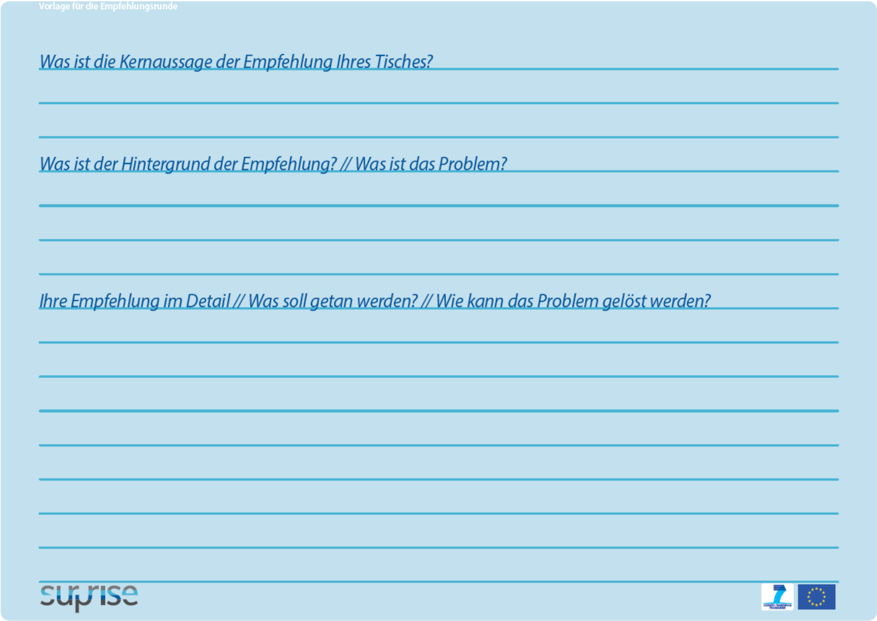
# 9 List of Abbreviations

| Abbreviation | Definition |
|---|---|
| BDSG | Bundesdatenschutzgesetz (“Federal Data Protection Act”) |
| BfDI | Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (“Federal Commissioner for Data Protection and Freedom of Information”) |
| BfV | Bundesamt für Verfassungsschutz (“Federal Domestic Intelligence Service for the protection of the constitution”) |
| BKA | Bundeskriminalamt (“Federal Criminal Police Office”) |
| BND | Bundesnachrichtendienst (“Federal Intelligence Service”) |
| CCC | Chaos Computer Club |
| DDR | Deutsche Demokratische Republik (“German Democratic Republic”) |
| CCTV | Closed circuit television |
| GdP | Gewerkschaft der Polizei (“Police Trade Union”) |
| Gestapo | Geheime Staatspolizei (“Secret State Police”) |
| GDR | German Democratic Republic |
| EC | European Commission |
| EU | European Union |
| LEA | Law Enforcement Agency |
| MAD | Militärischer Abschirmdienst (“Military Counter-Intelligence Agency”) |
| NSA | National Security Agency |
| NSDAP | Nationalsozialistische Deutsche Arbeiterpartei (“National Socialist German Workers' Party”) |
| NSU | Nationalsozialistischer Untergrund (“National-socialistic Underground”) |
| PbD | Privacy by Design |
| SD | Sicherheitsdienst des Reichsführers-SS (“Security Service of the Reichsführers”) |
| SED | Sozialistische Einheitspartei (“Socialist Unity Party”) |
| SIGINT | Signals Intelligence |
| SLT | Smartphone Location Tracking |
| SOST | Surveillance-oriented security technology |
| SS | Schutzstaffel der Nationalsozialistischen Deutschen Arbeiterpartei |
| Stasi | Staatssicherheitsdienst (“State Security Service”) |

# 10 Annex

## 10.1 Table recommendations

*Template*[46]



Vorlage für die Empfehlungsrunde

Was ist die Kernaussage der Empfehlung Ihres Tisches?

Was ist der Hintergrund der Empfehlung? // Was ist das Problem?

Ihre Empfehlung im Detail // Was soll getan werden? // Wie kann das Problem gelöst werden?

surprise

*Recommendations – content*[47]

| 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 transparency and limitations during collection, storage and processing of data | Protection against misuse of data and uncontrolled data collection, for example profiling | - Higher bars for data collection<br>- Report obligation in regular intervals for data collecting institutions and<br>- More influence for citizens |
| Development of harmonized European data protection on the highest protection level, e.g.<br>- comprehensible, practical control mechanisms<br>- the possibility for (mobile phone) users | - Danger of misuse<br>- Falling back on countries with lower data protection levels<br>- Factual pressure to consent<br>Missing possibility of really practical insight | - See above |

[46] 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.

[47] Translated from German

| | | |
|---|---|---|
| to object without negative consequences, to explain<br>- Enabling of transparency related to the carrier/provider, usage and storage means of data | | |
| An independent data protection authority should be introduced on European level. It should be equipped adequately with financial and material resources. Each citizen should be able to address it. | The right to informational self-determination is not upheld adequately | - Right of action in own name and on behalf of others<br>- Eventual direct instructive authority towards governmental entities<br>- Appointment by the EU parliament |
| - Holistic cost-efficiency analysis (political, societal, etc.)<br>- More transparency/ educational work | - Lack of knowledge<br>- New challenge due to new technologies<br>- Change of public space by permanent surveillance | - Remove technologies -> then do educational work -> involvement of citizens |
| - We want an "active information obligation of the data controller"<br>- Information obligation and right of involvement for the citizens regarding introduction, development, and deployment of security technologies | - Citizens are not informed appropriately about planned techniques and their deployment – presenting "fait accompli" to the citizens<br>- The opinion of citizens is not taken into account "in advance"/not to be taken into account at all | • "Active information obligation" for data collectors (public and private), means the citizen is not required to make a demand but rather that who collects data should be obliged to inform the concerned person -> what is stored, how long and why at all! E.g. also in form of a yearly report of the data collecting entity, where it is publicly declared for which purpose and how much data is collected ("Statement of accounts for collection")<br>• Information obligation -> citizen should be informed about introduction, development and deployment of security technology in such a way that they can form an own opinion which they can express with their freedom of expression at consultations prior to the planned use (citizens must be |

| | | |
|---|---|---|
| | | consulted before usage) |
| - Strengthening and specification of data protection and protection of general private law on European level | - Insufficient level of data protection and misuse of data in the past<br>- Imprecise legal norms and partially no consideration of new technologies | - Europe-wide data protection, which is on German level as minimum<br>-> Information obligation towards data subjects<br>-> Exclusion of commercial interests<br>->Higher bars for data misuse<br>-> Personnel/financial strengthening in the data protection and independence of supervisory authorities<br>-> information about citizen's rights<br>-> Safeguarding anonymous internet use |
| We recommend the European Commission not to research further in the field of citizen surveillance, but to invest in research on causes for social problems | - More technology currently does not lead to increased perceived security, but to less<br>- Without empirical proof of surveillance effectiveness, only lack of freedom ensues instead of the feeling of security | --- |
| For the use of security technologies, frame conditions must be created which hinder the violation of privacy in undue manner, as well as they enable they guarantee the control and transparency of those technologies | Fear of<br>1. Infringement on privacy and<br>2. Misuse of data | No deployment/prohibition of the technology |
| We don't want the "glass/transparent human being" and the same rules for states, government and economy | - Danger of data misuse. Not everything that is possible must be done (consequences must be recognizable)<br>- Human development must have degrees of freedom (being naturally) | - Binding Europe-wide data protection guidelines for companies and governmental entities. Clarification how foreign (non-EU) companies should be treated (sanctions of misuse, enforcement of acceptance of the data protection rules) -> working out compromises!<br>- Creating transparency -> Who has which data of me? For which purpose?<br>- Right to control the own data<br>- Protection of children and youths<br>-> they cannot estimate the consequences |
| A uniform EU regulation for data protection is needed to avoid loopholes | Solely national law does not help due to modern technologies | Uniform regulation (EU-wide):<br>- I have to know who stores which data about me<br>- Right to be informed/noticed |

| | | |
|---|---|---|
| | | (comparable with the Schufa)<br>- Control access of non-European organizations<br>- Privacy-by-default in programming new programs/technologies<br>- Right to determine what happens with the data (e.g. for sale)<br>- Right to delete data or to let it be deleted after a pre-determined time period |
| We need on EU<br>1. Critical investigation<br>2. A reliable legal framework and<br>3. Privacy from the start ("Privacy by Design") | Excessive possibilities of surveillance are differently handled in the various EU countries -> Agreement possible? | 1. Critical investigation: level/country-surpassing mediation, involving whole societies, from Kindergarten on<br>2. Reliable legal framework, clear responsibilities, transparency, also surveillance-free spaces, and excluding lobbyists in legislation process<br>3. Data protection built in: Protection against the misuse of data (also technical-organisational) |
| We recommend resolving security issues not only with technical surveillance | Privacy and data protection are important, especially the transparency of the processing. Security is complex; it concerns a responsibility-aware integration and social politics and criminal prevention | See above |
| More human factor instead of technology, taking into account the safeguarding of the personal freedom with the involvement of controllable security technologies whose deployment are legitimated through citizen consultations/referendums | - Individuality must be protected, so far too little information for the individual citizen<br>- So far too little possibility of influence of the individual citizen, doubts regarding the seriousness of the measures | --- |
| Desirable is more transparency in the following fields:<br>- Who processes what, where, for which purpose, for how long? | Insecurity about data collection without knowledge, felt loss of control, deficits of control | (colour-)marking of cameras with the address of the data controllers<br>More control by supervisory authorities regarding the realization of already existing rules, mandatory audit for providers of online services, all data concerning me shall fall under one law, clearer rules for legitimate use |

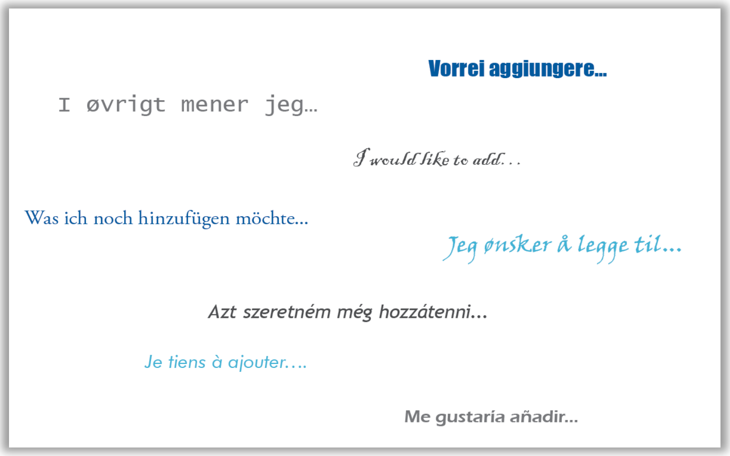
| | | |
|---|---|---|
| - Where can I get information what is stored about me and how can I eventually achieve deletion? | | |
| Extended transparency which improves also the control | - Feeling of control loss, "without alternative" will not be accepted<br>- Danger of future use of data due to new developments | - Surveillance needs clear legal ground regarding purposes, necessity and proportionality, also regarding linkage of data from different sources<br>- Transfer of data into third countries and also the storage time-wise (in the sense of a pre-defined expiration date) must be limited in Germany<br>- Evaluation of usefulness, publication of statistics regarding the effectiveness of the measures<br>- Citizen involvement also on regional level (e.g. for video surveillance)<br>- Limitations of the economy, because the data is also subject to governmental desires |
| Politics should define clear rules and conditions, limits and sanctions for technical surveillance PRIOR to their deployment. There must be regular controls and strict consequences for violations. Surveillance must not be conducted for private and commercial purposes. All measures must be transparently and open communicated. | Better protection of privacy. Too little control by supervisory authorities at the moment. Too much surveillance which is not recognizable. Misuse is not sanctioned. Too much unawareness (for example the mobile phone of Ms. Merkel) | - less ambiguous legal framework/conditions/approval/permission/sanctions<br>- Transparency regarding measures/possibilities/purposes<br>- Transfer of awareness regarding possibilities/information<br>- No automatic linkage, possession of a mobile phone is no consent |
| Increasing the significance of privacy | - infringement on citizen's personality and privacy through information and surveillance technologies | - Revelation which groups/lobbies exercise influence on legislation<br>- Exact information about functionality, usage and data storage of surveillance technologies generally and specifically<br>- No medium-term or long-term data retention (max. 6 weeks)<br>- Exact preconditions for usage purpose<br>- No automatic linkage of different data sources (anonymous surveillance)<br>- Everything for governmental as well as commercial data usage |

| | | |
|---|---|---|
| Data protection shall be strengthened actively | Data access through foreign governmental entities + private companies + processing | - Criminalize data misuse, not just minor/administrative offense<br>- Strengthening data protection supervisory authorities<br>- Virtual communication without surveillance, secure encryption<br>- No agreements with non-EU countries which undermine the German data protection law<br>- No transfer of data via trans-Atlantic cables |
| Restrictive use of surveillance technologies with effective control | Mo concentration of power, no concentration of data, safeguarding the presumption of innocence (rule of the law) | - Control though parliamentarian committees and through independent and competent government institutions (eventually also nationally)<br>- Transparency about data collections, right to be informed about the own data<br>- Citizen right of self-determination regarding data stored at governmental bodies and private entities<br>- No sanctions just due to suspicious behaviour |
| Extremely sensible control of the surveilling institutions, more transparency and information of the citizens | - Danger of misuse<br>- Missing knowledge of the citizens regarding the scope of the data collection, storage and processing | - EU-wide data protection laws, which apply for public entities as well as for private ones<br>- No softening/enforcement of the values and rules of the EU towards third countries<br>- Clear legal preconditions<br>- Independent control of the surveilling entities (means not: police controls police) |
| We demand the establishment of a European data protection level which meets the German law at the minimum | To our knowledge, the German data protection law is one of the strictest. A lower protection level is not acceptable. | - Enforcement must be guaranteed, especially in the form of sanctions, sufficient control<br>- Information, awareness-raising and involvement of citizens<br>- More transparency<br>- Giving the topic more significance |
| Regularly, robust (verifiable) data/statistics must be published to prove that the used surveillance techniques really increase security | This is necessary to legitimate the limitations of the individual freedoms. Increase of citizen's trust in the government. | - Supervision and control (verification) of data/statistics through independent committees with direct involvement of citizens (with most little politics/lobbyists)<br>- The benefit must always be proved with tangible data/statistics |
| Rather too little surveillance than too much | There is a certain gap between the competence of the government and distrust in the private sector. Transparency is especially important for the | If the benefits and drawbacks of surveillance could be better balanced, this is absolutely necessary. Then, surveillance can make sense. If this is not possible, it is better to reduce of terminate the surveillance. |

| | | |
|---|---|---|
| | private sector. So far, this does not exist. | To be improved:<br>Increase of transparency, decision based on purpose, minimize infringement on basic rights, proportionality, avoid decision influence of lobbyists |
| We demand the right to an unobserved life | The problem is the predominant, uncontrolled collecting mania of data and the misuse (through governmental, private and criminal entities) | - Collection of data only for significant causes<br>- Unconditional data minimization, transparency and time-wise limitation<br>- Deletion of all existent data sets from surveillance measures<br>- Protection of European citizens against foreign data collection (e.g. NSA) |
| A unified European Data Protection Regulation for security products for the effectiveness for the intended purpose | Hindrance of misuse:<br>Too much divergent standards lead to legal insecurity and misuse | Problem: Harmonization of very different data protection levels because the data protection laws in Europe do not have a uniform benchmark<br><br>Solution: giving the citizens transparent, scientifically proved information, so they can agree upon a unified Data Protection Regulation |

## 10.2 Postcards

### *Template*



Vorrei aggiungere...

I øvrigt mener jeg…

I would like to add. . .

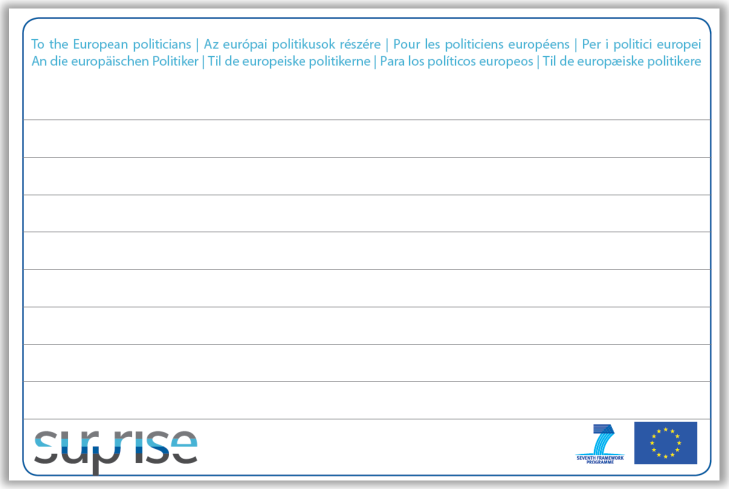
Was ich noch hinzufügen möchte...

Jeg ønsker å legge til...

Azt szeretném még hozzátenni...

Je tiens à ajouter....

Me gustaría añadir...



To the European politicians | Az európai politikusok részére | Pour les politiciens européens | Per i politici europei
An die europäischen Politiker | Til de europeiske politikerne | Para los políticos europeos | Til de europæiske politikere

### *Postcards - content*[48]

| |
|---|
| Alternative security systems not using surveillance should be given more attention and support.<br>• Foster neighbour support<br>• Eliminate prejudices and discrimination<br>• Spread more knowledge about other societal systems, religions, life styles. Foster encounters of different people/nations/religions<br>• Eliminate social differences |
| According to my opinion, the state, respectively, the EU, should not stand and watch as data about citizens are collected covertly, e.g.:<br>50% of all apps collect unnecessary location data<br>NSA stores (so far known) telephone calls of Germans with North America<br>Facebook stores... |
| No automatic facial recognition (!) through smart CTTV or the like (=no linkage: Recordings + identity) |
| According to my opinion, Smart CCTV should not be allowed for private persons and companies in Germany, but only at "exceptional places" like prisons, airports, train stations, cruising ships, or the like. And then only under strict conditions + without the permission to store the data longer than 1 week. |
| For privacy issues of products (e.g. Facebook), offer different alternatives/ regulate by law: |

[48] Translated from German

| |
|---|
| E. g. a) cost-free variant with data usage permission b) product subject to a charge without permission of data usage |
| Data retention shall and should be used only under balancing of all justified interests - based on the presumption of innocence. A transparent legislation process is absolutely necessary for that. |
| If an account is deleted, the data must be irreversibly deleted without it circulating further through the net. Profit-oriented companies shall not be allowed to enrich themselves through personal data without consent, i.e. prior agreement |
| The Data Protection Commissioner of Schleswig-Holstein should further contribute to clarification and regulating of data misuse. He is fun and a role model. |
| Do treat collected data with regard to Location Tracking (mobile pinpointing) and Smart CCTV or similar surveillance techniques as maxim of normal or correct behaviour. The presumption of innocence should be paramount. With regard to it, preventive measures should be kept a watch on in an especially critical manner. Noticeable behaviour must not necessarily indicate security-threatening or criminal activity. If innocence cannot be ruled out, preventive activities resulting of the analysis of surveillance data should be excluded (this should also be the case for low probability). |
| For each introduced technology and under regular evaluation of the current state of the art, always consider and integrate the possibilities of misuse. |
| An all-encompassing right of access/insight for own data stored at governmental entities and companies in all cases (model government department responsible for administering the former Stasi-files) |
| As little as possible, as unlinkable as possible. |
| The needed and necessary data protection laws should be drafted by independent specialized committees (state employees) without the involvement of lobbyists of companies which want to deploy and distribute software and technology for profit maximization. The safeguarding of privacy must have priority over the creation of jobs in this field of legislation. |
| The nations should have a greater interest as yet to invest in their own specialist workers for ensuring data protection compliance, so correlating specialist knowledge is available in the state that cannot be undermined by private companies. |
| There should be a stricter rule framework for the use of CCTV in the working world. If national parliaments have a higher standard for their country with regard to data protection, national law should be applicable. |
| 1. I want that according to German and European Law, my guaranteed rights, protection of privacy, personal fulfilment, freedom of expression, are enforced and protected<br>2. I want the drafting of clearer laws for the use of surveilling technologies and that the misuse will be punished with harder penalties.<br>3. The right to informational self-determination must be enforced. |
| It must be possible to partially revoke declarations of consent digitally, too. The withdrawal of consent must be valid. Example: Download of an app in the app store. Consent for network access, but not location information. Objection should not have any negative consequences. |
| I think it is fatal that many laws in Kiel do not label CCTV surveillance not properly. It is unclear what happens with the recordings. Because practically all stores perform surveillance, I have no customer choice. |
| The effectiveness regarding prevention and repression of surveillance technologies like smart CCTV and smartphone location tracking should be scientifically researched. |
| 1. Privacy is not a negotiable<br>2. Mid- and long-term surveillance data retention should be forbidden.<br>3. The automatic linkage and personalization of surveillance data should be forbidden.<br>4. Absolute transparency of surveillance processes should be ensured. |
| Democratic control!!! |
| No data retention!!! |
| In a democratic society, everyone should have the right and the possibility to hide something. This is a task for the politics. |
| It would be desirable/make sense to make security discussions more objective. In the discussion, the pretext "endangered security" served only the introduction of even more surveillance technologies. |

| |
|---|
| There should be a right of access for all personal related files (and deletion for non-governmental files) |
| No police staff/humans should be substituted by technology in the security context. Technology is a nice feature, if it is regulated properly. Laws should be adapted to the developing technologies regularly. |
| Do not protect the privacy protectors, but the information of the citizens. |
| I don't want to trade my citizen rights for assumed citizen protection |
| Foreign interests are not allowed in the German (resp. European) security politics data protection! (e.g. Google, Facebook, NSA) |
| It should be safeguarded that the participating group is representative. Moreover the time (2x35 min.) is not sufficient to evaluate some sort of result. For the group discussion, guidance's as well as a person with more knowledge in data protection than the participants would be helpful |
| Do not force member states through regulations and directives to issue legislation violating a fundamental right. |
| I want e.g. annually, to receive post or by email, a printout who, where, which data (at least in Schleswig-Holstein) about me (residents registration, insurances, Schufa) |
| No transfer of national state interests relating to data protection towards the EU. The respective nations should decide over the access to national state data (no preference ..................... |
| The 1st film contribution (Smartphone location tracking) has a very problematic source: "Die Linke Sachsen". That a party, derived from the SED and formerly responsible for the Mfs, is mentioned in this context is pure mockery. In a genuine and scientific context, such sources should not be used. |
| How could one reduce the incentive of data protection? How could one commercial.... |
| Please take care of the self-selection of participants which has a distorting effect on the questionnaire results. Citizens rather sensible regarding to the topic would participate in such an event. Also the media coverage of the last months (NSA etc.) has an effect on the questionnaire results. Just a short time earlier, the results probably would have been different. |
| Also property is a fundamental right that should be protected through new technologies! This point fell a bit too short. Otherwise, a very good event – please more of this! |
| I wish for politically mature citizens which inform themselves instead of always screaming for the government. |
| Surveillance only on technical level (in the sense of data retention) leads to overregulation if it is not limited conventionally. The data retention aims at a legitimate goal, yet it is not proportional. Central data storages are governmental privately commercial to be seen critically. Surveillance and data should be transitioned to infrastructural levels and limited conventionally. |
| Empirically, this study is quite questionable: Questionnaire results already published: Majority opinion set even before the discussion! Social-pedagogically problematic because prior to discussion....not representative (age, stance on data protection). Questions suggestive & partially unclear, e. g. 62, 77 A). It is important to develop Empiric for this topic but in my opinion this study is rather weak. |
| Security is not everything!! Freedom consists of the feeling of being able to do things without being observed and without fear of consequences. Wind back security standards. Citizens are not enemies. Data protection should also be an obligation for companies. |
| Please think more of the generation after the generation after the generation...! Without freedom, there is no security, no content, no trust, no "self-thinking", and surveillance means lack of freedom! How can there be unified EU-Regulation if each country should keep its own culture and gracious goodness, its own mentality? |
| Lobbyists should not be involved in votes... /and / or discussion, to avoid "conflicts of interest". |
| 1. Chain intelligence agencies<br>2. No weakening of the strict European data protection rules through the planned Free-Trade-Agreement with the USA.<br>3. The storage of collected data must be handled very restrictively, i.e. a data retention should not happen.<br>4. The right to informational self-determination must be enforced. |
| Each citizen has the right to learn where his/her data is stored, if and when this data is transmitted to security agencies and how the data is linked to each other. In case of mistakes he/she must have the |

| |
|---|
| right to demand the deletion. The commercial usage of the data must be limited – Google, Facebook, etc. must be limited in their collection activity. Always implement Privacy by Design immediately. |
| The security technology (smart) should be held in public sphere, under strict control. This should be in each case, also against the will of the population (or their will) in public places, where more people are present, resp. mainly to.....of attacks.... & and violent acts. |
| TAO (Tailored Access Operation) breaks all!!!! (special department of the NSA). A finally proper encryption against it please! Thanks Removal of all networked electronics (health insurance card with car with refrigerator with alarm clock with heater with internet with TV with telephone with....etc.) Because: Is in preparation. |
| I wish for more transparency and enlightenment about collected data and their usage. |
| Foster right to have a say in questions of supra-national regulations (e.g. data protection, data transmission (Base III)) |
| I beg to take data protection more into consideration |
| Address reasons for crime rates, violence, terror, etc. Also, better education, end poverty, social work etc. Preserve freedom! More human! |
| I am for a data.....from Smart CCTV to mobile phone location tracking, for that the technology must be changed massively (error quotes, protection against data theft & data misuse). Collected data must only be used to enhance national security (prevention of crimes, capital crimes, terror, attacks). Commercial interests must be excluded strictly, just as further foreign interests. All of this must be manifested by the governments in laws & breaches must be sanctioned uncomfortably high. |
| Smart CCTV: At the current state of the art, the technology should not be used for crime prevention, but for searches (car plate numbers, facial recognition). Tagging should occur smartly i. e. persons, vehicles not searched for, private areas (windows, gardens) will not be recorded along, but will be blacked out. Recognition of abandoned bags, "suspicious behaviour" in crowds e.g. at airports could (as piece of circumstantial evidence) make sense |
| Technology should not be allowed, if it is not regulated. This is a general problem that should be addressed. That the legislation is lagging behind the technological advance (e.g. also for new financial products -> financial crisis) |
| No misusing (purpose-diverting) collection, use, storage of data, but a factual handling in a manner least infringing into rights and the concrete, real everyday life. The data should have a definite expiration data. Citizens should be involved more, e.g. like in this citizen summit. I wish for taking into account more the opinions and this is primarily more privacy and that this will become more secure again. |
| Responsible handling of the data – this includes a better information of the citizens what is happening with those data. Obligation of transparency: who collects which data? What is done with it? How long is it stored? To whom will it be transmitted and what does the recipient with it? |
| A clear and arranged danger classification (traffic light) of apps/websites/software/observed area this I wish for, without having to read and understand pages of privacy policies, i.e. terms of use + control of the classification correctness + 1 unified EU responsible and known party. |
| Stop storing and analysing so much data about us all. |
| In schools, the children and students must be informed about data protection and fundamental right to privacy and about their responsibility if they reveal data also of others. |
| I wish for efficient and unified European data protection. Investigation and security institutions should be subject to efficient and comprehensible control mechanisms to prevent misuse, each citizen should, as far as it does not hinder investigation work, have the right to learn if and to which extent he is surveilled. |
| Do not create more regulations -> In case of breaches sanctions! |
| No reduction of staff at the police in combination with technical solutions. |
| CCTV – needs no country: too expensive in the development, too insecure in deployment, danger of discrimination etc. etc. Because of this I wish that the European countries invest the money in countermeasures for the reasons of crime, terrorism and crisis. |
| Each citizens must have the opportunity to get information without hassle about who, what, how data is collected, and how long and for which purpose it is stored. These requests must not be interpreted as |

| |
|---|
| drawback for the citizen. |
| The European democratic project.....free citizens who can express their opinions freely. Do not risk this freedom not for an exaggerated focus on public security. |
| Apply privacy of letters to emails. |
| - Shortened time-bound storage of data in companies and governmental institutions<br>- Interface in Germany, over which data streams to further countries are limited.<br>- Improve transparency for citizens about data collections and usage<br>- Create laws for national and foreign companies (business) to protect German citizens more, that less data is used.<br>- Avoid linkage of different data. |
| Please do not apply blanket suspicion to citizens, but protect them against commercial and secret service interests; enable and protect a life with self-responsible transmission of data! Check and destroy collected data after expiration of time period (through an specific, independent data protection authority) |
| Wish for more national decision power, because in other countries, data protection has not so much priority. |
| I must be given the possibility to comprehend where and which of my data is stored. |
| Internationally active companies must orient themselves to the legal rules of the country of the end user. It must not be possible that our democratic principles are circumvented by territorial side steps. |
| Technologies must not be measured with the related popular topics, like e.g. terrorism as argument for Smart CCTV. The technologies must be evaluated independently from them, costs/benefits as well as factual possibilities must be assessed independently from the politics. |
| As for all the surveillance, a cost/benefit analysis is important - ....professional terrorists/criminals know how to protect themselves against surveillance systems – is someone who lives near a mine field sure that he.... |
| More citizen summits about topics concerning the population. Immediate stop of all technologies to be addressed. Consideration if technology, especially in security matters, or the "human" is first choice. |
| Instead of addressing/treating symptoms, go to the core. Make clear/grant citizens more education, more responsibility. Strengthen the courage of the individual. |
| Please limit the data collection and processing by large internet companies through clear rules. |
| Please foster privacy-enhancing technologies and privacy by default with self-determination, transparency and constitutional control! |
| Ensure the security of women and children by sufficient number of women's refuge places. |
| Data misuse/trade (illegal) should be punished more severely and pursued more often. The customer and user should not feel powerless but have the government as "big brother" on his side for information, transparency and in conflicts. |
| For the SurPRISE-organisators: 10-15 minute more time would have delivered a better result. |
| The trans-Atlantic networking and the free trade make a European net necessary. From my point of view, the infringement in German mobile telecommunication networks and my private data is too extreme and unjustified. |
| Support of Open Source solutions – software – hardware compatibility (smartphone, computer) – support of security standards and security solutions which make a thorough encryption on "hostile" servers possible and which grant the customer a hundred percent control/knowledge about his data. For example would it be super if there would be a data protection/security sand box for email accounts (like VPN tunnel) |
| Support of a user-friendly GPG-Open-Source solution (decentral) – with prior competition |
| Do not make a Free Trade Agreement which undermines the current data protection laws.<br>- support Open Source software smartphones of providers like Ubuntu<br>- No processing of data by private companies<br>- no security agreements which provide data of German citizens to foreign countries or foreign governmental agencies. |
| Include media competence into school education |

| |
|---|
| To protect the personal freedom of the individual, it is important that the responsible institutions are in permanent dialogue to guarantee at the same time a sensitization and related self-control in the sense of a democratic state under rule of law. |
| How could the incentive of data collection be decreased? By using software solutions which are not proprietary. By decoupling profit and data effectively. |
| Minimize all surveillance – take care of data minimization – encounter data misuse decisively – it is no "super fundamental right"! Better information of the population – obligation of notification...... |
| Restoration of the fill competence for the regional data protection centers i.e. the informal self-determination rights of the individual. No differentiation of Länder and federal data protection laws. |
| Less technology – more people |
| Self-employed and freelancers and all business registrations should go to the Länder data protection authority in copy – like for tax office, BG, etc. – better control of e.g. ambulant care services, which would treat sensible data then more carefully. Fear of consequences etc. Create data protection law, data protection liability laws, data protection criminal law similarly to copyright law. |
| Strengthen data subjects (§ 34/35 BDSG) – install de-central data protection authorities, employ more practicing people, less legal staff<br>– shape data protection – only administrate –<br>Business notices in copy to data protection of the Länder....????<br>- Make violations against data protection penalty-enabled |
| Stop the filming and the wiretapping – we do not want a surveillance state under the motto 1984 Orwell |
| Misuse must be prevented. Where and when there is surveillance, it must be brought to the attention of all persons. Protection of the privacy should be preserved. |
| As little surveillance and storage as possible! Only in case of severe risks for persons, animals and good, surveillance should occur or a s help in emergencies. |
| Right to access like at the Schufa through all data collectors of all kind! Right to deletion of the citizens anytime! Camera with number and telephone number and internet address for data deletion. |
| Which success are there with the current methods and clearance of crimes? – Do they preserve our freedom rights + the multitude of life ways, personality???? – Security evolves through involvement of citizens, transparency of the politics + integration bottom-up! |
| Public discussions about privacy + security politics – needs due to facts: Numbers, evaluation about benefit of electronic data processing supported surveillance and the constitutional alternatives – Revelation of the treatment of electronic data processing supported data + transparency especially by comparison – right to access to collected data |
| Protection against data collection of foreign services, companies, etc. – right to get own data deleted -> everywhere – qualified control + coaching + further training of the concerned personnel |
| EU-universal rules concerning security agencies and data protection<br>- these rules must not serve one-sided security or commercial interests, but must give citizens/consumers the choice how much information they reveal and for which purpose. |
| World-wide, at least EU-wide possible deletion procedures for stored data about me – right to know who has my data and how I can contact them. Less technology, more police staff, no private security staff for governmental tasks. |
| Importance: Control of the initiators/question givers – make analysis public/comparable – right to ask/access, deletion for citizens |
| Offer regular events in the Schleswig-Holstein Länder provinces (in cooperation with the province parliaments) |
| Why must it be that federal politicians + government institutions "make use of" internet data service providers (her especially Yahoo, Google, Facebook etc.) which refuse to apply German data protection law for German users? Politicians and governmental institutions are role models! I wish either for a purely German or??? – internet (other service providers must be blocked) I also want (under encryption of my original IP) to use "international" internet. |
| Why must it be that in Schleswig-Holstein Länder(+local) politicians make use of internet data service providers |
| Security abandons freedom always a bit more!!! No thanks!!! Peace for all |

| |
|---|
| I don´t want to be treated as a potential threat |
| Create possibilities for all EU-citizens to receive information about collected data and take the severe concerns of the population seriously and self-oblige regarding data protection |
| Do not obligatory realize what is possible in theory! Focus also on alternative measures! Especially regarding public security, the answer cannot be more surveillance. |
| To the politicians of the EU: I as directly concerned person in Germany with the name XXXX, I ask you to the EU and international levels to advocate to human rights and law of nations in the security agencies and secret services. So governments and politicians do not use this in their own interests for power and their country. The also EU intern...??? Transparency for the population |
| To the politicians of the EU: That committees and commission... ..... the current real situation in the national member states ....., with their security agencies. This international with the UN members under consideration of the human rights and international law. This with transparency for the population. |
| To the politicians of the EU: advocate on EU or UN level against national misuse of security technology against people and citizens. This with evaluations on general level with the police as security agency. Additionally, the "Five eyes" USA, UK and Germany with UNO and BfV. With transparency for the population. |
| For the assessment of benefits and drawbacks, do not only hear security agencies and companies, but to the same amount citizen initiatives + human rights organizations. Privacy by Design, noticeable sanctions against misusing parties (also state institutions). Do not allow surveillance technologies for private/commercial interests (with exception for providers) |
| Living secure is good and desirable. Freedom is a higher human right. The more surveillance technologies are used to ensure security, the more freedom is limited.<br>Freedom dies with security! Transparency is necessary, regular information politics also. |
| Data protection should not apply for citizens, abandonment of....! Data protection of protection of the personality, .....the perception of democratic rights like freedom of expression and the right to be left alone. Stock up of data protection authorities + data protection officers in companies. |
| Data protection for children, help for abused, data protection and surveillance in public places, show offenders publicly |
| More transparency regarding intended/used security measures and right to have a say of the citizens with prior information. |
| About mobile tracking: Each function of a mobile, which goes beyond mere telephone function, should be allowed only with the explicit consent of the user. Furthermore, add the product documentations of each mobile-type and the necessary telephone functions.....(analogue description list of ingredients) |
| I wish that there is no data retention – that the purpose of data bases are described precisely and that their possibilities to link information is strongly limited and that they are determined precisely. , - that the misuse of data will be sanctioned more severely, - that the possession of "hacker software" will be legalized, because only through penetration security loopholes can be discovered. |
| Who sanctions the state? If German government institutions misuse data? If other states violate the rights of German citizens and persons living in the country? |
| The whole input, no matter of brochure, the videos, the questions etc. were very polarizing. This is no matter of objectivity or scientific approach. I see it more as opinion making/polarization. Questionable is also, how the participants were recruited. The polarization went towards the contra. |
| Citizens should in general be involved more in decisions, like through this summit – only more objective! |
| I demand more severe consequences for illegal acts / illegal use with/by security competences and technologies by governmental bodies. Data subjects must receive high compensation from the governmental institutions which is suitable to prevent a repetition due to the effect on the budget of the institution. This shall also apply for illegal or invalid administrative decisions or the like. |
| I have the opinion that freedom goes over security and that the deployment of smartphone location tracking and smart CCTV should not be used, because data and personal profiles are created although a crime has not happed yet. This data could get into the hands of the wrong persons! "Who observes the observers?" |
| I wish that the exchange of data of persons will be limited world-wide – that Safe Harbour will be |

| |
|---|
| terminated – that Swift will be terminated – that more will be done to sensitize the citizenship – reduce the number of persons with access to sensitive data – that the powers of secret services will be limited and their control increased |
| I want an internet that makes anonymous surfing possible – that encryption is supported and governmental bodies renounce building in weaknesses – that governmental bodies convert their computer systems to open source – that governmental institutions do not always try to ignore freedom of information laws |
| Topic security – freedom – technology should be made central content of education (elementary-). So we + our children neither technology...become neither unnecessarily fearful nor manipulable. |
| Make information a governmental task/obligation to enable aware and responsible decisions. |
| Question and analysis catalogue too vague and not concrete/specific enough. Think that the questions are not very meaningful. What are the questions supposed to achieve? I really worry about the scientists who have developed these questions. Little message. |
| Free development is under pressure due to digitalization and get into danger. Individuality gets lost. Wish: for more free development (individuality) Solution: Support in education systems. Support of individuals and not apply one standard to all. Early child education. |
| More human instead of technology – Back to the roots. |
| More joint decision-making power in relevant topics like Free Trade Agreement, data retention and surveillance measures, eventually plebiscite. |
| More controls at companies should be conducted, not only on request. |
| Instead of steadily increasing surveillance and control measures, staff of security agencies should be racked up and social problems as reason of perceived "insecurity" should be given more priority |
| I ask the provincial and the federal government, to evaluate the already existing security technologies and competences, like e.g. cell tower inquiries, [... ], telecommunication surveillance etc. independently and scientifically |
| 1. Citizen rights shall not be subordinated to commercial interests<br>2. The control of the observers must be guaranteed steadily<br>3. Security technology shall only be analysed by governmental institutions |
| That our data protection (BDSG) will be adopted and improved trend-setting, not loosened. |
| Surveillance of EU citizens should be abandoned completely. Data retention should only be possible within a narrow, limited frame. Mobile phone tracking should be handled like in Germany EU-wide. "Intelligent" CCTV should only be conducted at "hot spots" EU-wide. |
| Surveillance by CCTV cannot replace human investigation + help. Security staff, police, justice, but also train personnel + streetworkers are more important and more effective than computer programs. Facial recognition has many dangers (linkage of collected data with e.g. Facebook, YouTube etc.) but almost no benefit. Children and adolescents must be protected against unreflected data settings in the internet. No! data storage of children (photos etc.) |
| Follow-up in 5 or 10 years. Result realised. Limit data misuse. Strengthen data security. |
| More information already in school + Kindergarten + also retirement homes |
| I found the wording of the questions for the "clicker" too suggestive i.e. to directional. Sometimes, the wording of the questions was too vague, respectively the answer possibilities too little differentiated. The question about the security agencies was too unclear since it is not clear if German security agencies (do not deploy CCTV!) or European agencies are meant (European study!) |
| Also the development of the young generations has to orient itself to democratic principles. A Europe-wide discussion should be initiated about what privacy means and which value it has for each one and in future. The storage and usage of data collected through digital technologies must be regulated clearly and in a transparent way, in case of possible misuse, the collection and storage must be limited, respectively stopped. |
| Democracy as political system has the task to enable and protect the free personal development and freedom of expression of its citizens. Digital surveillance shall only be used if it supports and fosters the democratic personal development and does not lead to a limitation of individual rights and democratic basic attitude. |

| |
|---|
| In my view, the basis of the question in this study is too narrow. It concern due to the volume of the data and the availability if the data may be accessible at all and under which conditions. Not only governmental institutions but also private companies have access to that data. Because of this, rules for all must be manifested. |
| Unconditional focus on sustainable practices. It must never be forgotten how grave the misuse of these (+ also other comparable) technologies can damage societies + individuals, because rulers and laws can change. |
| Enforcement of the European Data Protection Regulation, respective reform to anchor Europe-wide binding minimum level of data protection principles |
| Focus on terrorism does not align with the measureable, real dangers, but even the real dangers which can be dealt with Smart CCTV & handy/smartphone location tracking are so low that it makes little sense to use these technologies at all. Security agencies have in this context a too big influence on political stakeholders and tend towards fostering security measures by presenting problems in an elevated manner. Instead, the research in this area should be extended. |
| Set a clear sign against surveillance technologies like smartphone location tracking, Smart CCTV and cyber surveillance, those are not desired by the majority of the population! (cause massive fears of misuse, limiting on privacy and fundamental rights) |
| Crime clearance rates could be increased afterwards through CCTV and Smart CCTV, i. e. contributes to the recognition of patterns. Can, from my point of view, not prevent attacks/crimes. |
| Criminal prosecution through police/ Verfassungsschutz. Convenience. Localization of friends, providers of apps on the own mobile. The linkage of knowledge which I reveal myself or others about me (this could also be friends). The unauthorized usage/linkage through private/companies. Potential misuse. Revelation of own data through others. Can one trust the data collecting organisations? |
| Deployment at airports and other security sensitive areas. For effective use against vandalism and for the increase of security feeling. Inappropriate storage of data. The handling, use, analysis through security companies (who eventually do this in governmental mission). Illegal access through organised crime. Access/processing through foreign governmental institutions and/or in foreign countries. Purpose-diverging use of the knowledge gained from this data. |
| Use technical services that are important to me -> e.g. location systems for traffic navigation. Location of "helpless" persons, e.g. elderly, children. Missing transparency – > This way I cannot retrace who is using my data |