"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 6.8 – Citizen Summits on Privacy, Security and Surveillance: Country report Switzerland

Lead Beneficiary: TA-SWISS

Author(s): Danielle Bütschi (TA-SWISS), Lucienne Rey (TA-SWISS), Dilini Sylvie Jeanneret (TA-SWISS)

Due Date: June 2014

Submission Date: October 2014

Dissemination Level: Public

Version: 1

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

This document was developed by the SurPRISE project (http://www.surprise-project.eu), co-funded within the Seventh Framework Program (FP7). SurPRISE re-examines the relationship between security and privacy. SurPRISE will provide new insights into the relation between surveillance, privacy and security, taking into account the European citizens' perspective as a central element. It will also explore options for less privacy infringing security technologies and for non-surveillance oriented security solutions, aiming at better informed debates of security policies.

The SurPRISE project is conducted by a consortium consisting of the following partners:

Institut für Technikfolgen-Abschätzung / Österreichische Akademie der Wissenschaften Coordinator, Austria	ITA/OEAW	
Agencia de Protección de Datos de la Comunidad de Madrid*, Spain	APDCM	
Instituto de Politicas y Bienes Publicos/ Agencia Estatal Consejo Superior de Investigaciones Científicas, Spain	CSIC	
Teknologirådet - The Danish Board of Technology Foundation, Denmark	DBT	
European University Institute, Italy	EUI	
Verein für Rechts-und Kriminalsoziologie, Austria	IRKS	
Median Opinion and Market Research Limited Company, Hungary	Median	
Teknologirådet - The Norwegian Board of Technology, Norway	NBT	
The Open University, United Kingdom	OU	
TA-SWISS / Akademien der Wissenschaften Schweiz, Switzerland	TA-SWISS	
Unabhängiges Landeszentrum für Datenschutz, Germany	ULD	

*APDCM, the Agencia de Protección de Datos de la Comunidad de Madrid (Data Protection Agency of the Community of Madrid) participated as consortium partner in the SurPRISE project till 31st of December 2012. As a consequence of austerity policies in Spain APDCM was terminated at the end of 2012.

Table of Contents

Executive Summary

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

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

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

In this report the results from Switzerland are presented.

A key feature of Switzerland is its direct democracy: several times a year, Swiss citizens vote on various subjects such as taxes, immigration policies, military affairs, social security issues, etc. Topics related to security, surveillance and privacy do not make an exception, and Swiss citizen are regularly called to ballot to have their say on issues such as video surveillance, biometric passport, regulation of surveillance authorities, etc.

Direct democracy is not the only specific feature of this country of 8 million inhabitants, where four languages and related cultures coexist. Switzerland is also characterized by it federal structure: power is distributed between the Confederation (the central State), the cantons (26) and the municipalities. The cantons and municipalities have wide-ranging powers and their own sources of income.

Last but not least, it is important to remember that Switzerland is not part of the European Union and is a neutral State. Neutrality means that the country cannot enter into military alliances and its army essentially has the function of defending the territory in case of an attack or for ensuring internal security. However, Switzerland is far of being an isolated inland in the middle of Europe. Much of its regulation is based on European regulation and it is part of the Schengen area.

Security, surveillance and privacy in Switzerland

Switzerland, in common with most other European countries, has a broad security policy, which is no longer limited to the concept of defence and control of violence against the national territory, but includes many other direct and indirect threats and dangers that may affect both the country and the lives or physical integrity of individuals. In that sense, security policy is viewed as a responsibility of many actors at federal, cantonal and municipal levels. While the government and the army ensure the integrity of the country with respect to various threats, the cantons - or municipalities - play an important role in maintaining security. Swiss security policy is also interconnected to other policies, such as foreign and economic policies. On the organisational and operational levels, the core of the governmental security strategy relies in a national security network allowing for efficient interaction between the Confederation (federal level), the cantons and the municipalities.

Both the cantons and the Confederation are entitled to conduct surveillance activities, but under a strict legal framework. As a general rule, cantonal surveillance aims at internal security, whereas federal surveillance aims at external security. Surveillance can be ordered for preventive purposes and for

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

criminal investigations, and can use many measures, from traditional ones such as interception of post or wiretapping to more recent and sophisticated ones such as video surveillance, biometrics or drones. Surveillance activities undertaken in the context of criminal investigations have to be ordered by a law enforcement authority and approved by a judicial authority. At the federal level, the Intelligence service activities are regulated by the Federal Act on Measures to Safeguard Internal Security and the Federal Act on Responsibilities in the Area of the Civilian intelligence Services.

Privacy protection is a constitutional right in Switzerland: article 13 of the Constitution states that “Every person has the right to privacy in their private and family life and in their home, and in relation to their mail and telecommunications" and that "Every person has the right to be protected against the misuse of their personal data". This principle is regulated at the federal level by the Data protection Act, which governs the collection and processing of data by private bodies and federal agencies. The role and duties of the Data protection commissioner is also defined in this act. Data processing by the cantonal authorities is not subject to the Federal law on data protection and is regulated by cantonal legislation.

DPI, smartphone location tracking and video surveillance in Switzerland

The Federal Act on Measures to Safeguard Internal Security (ISA) rules the means available for the Swiss intelligence service. In that law, the use of technical surveillance such as DPI is not provided, meaning that it cannot be used for surveillance purposes. However, Edward Snowden revelations about surveillance activities of the NSA showed that the United States – and maybe other countries - had some illegal surveillance activities in Switzerland based on sophisticated technologies. Swiss authorities are currently investigating to what extent Swiss citizens have been under surveillance of foreign governments.

Smartphone location tracking by State authorities is permitted only in the context of legal and criminal investigations, and has to be authorized by a judge. As for DPI, it cannot be used by intelligence services, which have to rely on other legal means (cf. Federal Act on Measures to Safeguard Internal Security). The situation is of course different with private and commercial actors, as they may collect and use location data for their commercial activities. In this case, they have to comply to the Federal Law on Data Protection, which regulates collection and processing of data by private bodies and federal agencies (see section 2.4.1).

Video surveillance (CCTV) is also subject to strict rules. When private individuals install CCTV cameras, for example to protect people or deter acts of vandalism, this is governed by the Federal Act on Data Protection if people appearing on the recorded images can be recognised. Where CCTV cameras are installed and run by cantonal or local authorities, cantonal legislation usually applies. This may differ from canton to canton, but is essentially based on the provisions contained in the Federal Law on Data Protection. At federal level, there is no legislation about video surveillance. But several regulations (ordinances) regulate the use of CCTV cameras in trains, public transport, railway stations, airports and custom offices. The Confederation also enacted some recommendations based on the Data Protection Act and the Labour Act.

Legal debates on surveillance and data protection

Several laws related to surveillance activities are currently being discussed in Switzerland. The Parliament is currently examining a new legal basis for the activities of the Federal Intelligence Service (FIS), the Intelligence Service Act. It should provide a comprehensive legal basis for the FIS.

Closely related to surveillance activities is the Federal Act on Surveillance of Post and Telecommunications, which determines the cases in which the law enforcement authorities can intercept phone calls and mails. This law is currently under revision in order to cope with technological developments, and especially the major role of the internet in communications.

The Federal Council is currently investigating the possibilities for strengthening the Federal Act on Data Protection and to strengthen the role of the Federal Commissioner for Data Protection. A group of experts has been nominated to consider these issues, and depending on its conclusions, the Federal Council will then propose a revised version of the Federal Act on Data Protection, which will then have to follow all the legislative steps (consultation phase, inclusion of comments from the consultation phase, parliamentary debate, decision and, if demanded, referendum).

Public discourse on surveillance-oriented security technologies and related practices

The protection of privacy emerged as an important issue in the public debate at the end of the 1980s, when a Parliamentary committee discovered the existence of a large number of files illegally constituted. Since the beginning of the 20th century, about 700,000 persons had their daily activities traced in more than 900,000 files for state security reasons. As a response to the heated criticism from the media and public opinion, the government decided to open the files to the citizens concerned. It also undertook major reorganisations of the Federal police and the services of the attorney general. This strong response to the scandal have reassured public opinion, as in 1999 Swiss voters rejected an initiative requiring the abolition of the political police and the prohibition to monitor anyone in the exercise of their opinions and political rights («S.o.S.- pour une Suisse sans police fouineuse»).

Current discussions on the revision of the Federal Law on Surveillance of Post and Telecommunications and the elaboration of an Intelligence Service Act are generating strong criticism. But, on the whole, Swiss citizen are rather confident with respect to security policy and related surveillance activities, as showed in several surveys.

The SurPRISE citizen consultations in Switzerland – an organisational challenge

In Switzerland, three citizen consultations have been organised in order to cope with the linguistic variety of the country: one each in German-speaking (in Zurich), French-speaking (Grandson) and Italian-speaking Switzerland (Lugano). These consultations offered an unique opportunity to scrutinize the opinions and arguments of Swiss residents on issues central to the country's security policy: how far do they feel safe in their country and everyday life, how do they consider surveillance-oriented security technologies (SOST) and how important is privacy for them? Moreover, as the format of the summits included polling sessions where participants were asked about their opinions and discussion sessions, we could get a rich and diverse picture of citizen views, including their opinions and the reasons for them, their hesitations and ambivalence, their hopes and fears and their demands to policymakers. The Swiss citizen consultations focused on two technologies (Deep Packet Inspection and Smartphone Location Tracking).

The recruitment strategy for the Swiss citizen consultations aimed at setting up a group of 200 to 300 persons who reflected the national demographic in terms of age, gender, educational level and occupation. In order to be able to constitute such a large and heterogeneous group, TA-SWISS sent contact letters to 45,000 randomly selected citizens, 15,000 in each linguistic region of the country. Information about the project and the recruitment process was also posted on the TA-SWISS website, in TA-SWISS newsletter and on Facebook. Moreover, the TA-SWISS network (advisory group, steering committee) has been used to promote the event. And citizens who had already participated in previous participatory events in the last decade also received an invitation. Finally, flyers were created and distributed in different places such as supermarkets, universities and other public spaces.

All these efforts resulted in more than 1300 registrations for the three events. A group of 110 persons was selected for each citizen summit on the basis of the information on age, gender, education and occupation. The selected citizens received prior to the summit an information brochure about surveillance, security and privacy which presented the surveillance technologies at the core of the SurPRISE project. Finally, on the day of the citizen summits, 88 persons attended the German-speaking citizen summit, 91 the French-speaking citizen summit and 75 the Italian-speaking citizen summit (a total of 254 participants). All three Swiss discussion rounds were characterised by a strong presence of persons with a higher level of education and of people holding a senior management position. The two youngest age groups were clearly under-represented in comparison to the whole population.

Insights on opinions about security, surveillance and privacy

The three Swiss citizen consultations provided qualitative and quantitative insights on how the Swiss population perceives both security and privacy issues. First of all, answers given during the voting sessions showed that most of the Swiss resident population feels safe in their country, or even very safe, with some differences across the linguistic regions. Averaging to other SurPRISE countries, Swiss participants rate high in the sense of personal security. However, when security relates to the Internet, the sense of security is not as widespread.

Compared to other SurPRISE countries, Swiss participants are less prone to accept surveillance technologies to be routinely adopted. Consequently, privacy is very important to the Swiss participants.

These views on surveillance and privacy are confirmed by other questions, where Swiss participants rate pretty low. This is for instance the case with the argument that anyone who has nothing to hide has nothing to be afraid. The table discussions showed that the main reasons for citizen not to be at ease with surveillance technologies are related with their lack of transparency, resulting in a lack of trust. Some participants also put into question the efficiency and relevance of surveillance technologies to increase security.

Greater opposition to DPI than to Smartphone location tracking

Overall, slightly less than half, 47 percent, of Swiss participants would accept DPI as a measure to strengthen national security , while 34 percent opposed it. The fact that the conduct of users could be misunderstood, personal details fall into the wrong hands, privacy and ultimately even fundamental human rights be violated, worried many of the participants.

Geolocalisation does not meet with unreserved approval either. The statement that geolocalisation as a measure for protecting national security is welcomed achieved the score of 55 percent. Compared with DPI, geolocalisation might yet win over somewhat wider range of people for itself. This could be connected to the fact that its benefits are experienced directly in everyday life, as some participants expressed it during the dialogue sessions. For the participants, localisation technology also has an «institutional face»: users know who their provider is, so they can visualise who keeps their data and what purpose it is used for. Despite the obvious usefulness of mobile phone localisation, many people mentioned disadvantages of the technology. They seemed particularly disturbed by the fact that private individuals could access data. Social constraints and upheavals were another issue linked to geolocalisation which concerned the participants. The lack of transparency was another reason for criticism with regard to geolocalisation – often voluminous and confusing terms of use. Furthermore, in all discussion rounds people argued strongly that localisation technology should be deactivated on mobile phones as standard; it should only be switched on if the user had expressly agreed.

Citizens recommendations and doubts about their achievability

At the end of the events, the participants discussed possible solutions for toning down the disadvantages of surveillance technology and thereby reducing the sense of unease.

In all discussion rounds the call was made for effective legal safeguards. At the same time, however, doubt was also expressed in all round table discussions as to the achievability of this demand: firstly, because experience shows that legislation always lags behind the technology, and secondly, because the global flow of data through national legislation can be difficult to direct into the right channels. The different legal opinions and moral convictions around the world also fuel doubts about the enforceability of laws.

Another major concern for citizens participating in SurPRISE was maintaining control over their data. In this connection the call for stronger data protection was made repeatedly. Also closely linked with the wish for control is the desire for transparency.

Because they expect little from regulatory guidelines, a number of participants are relying more on the personal responsibility of every individual. Several participants also referred to customers' market power. On several occasions reference was also made to the possibility that personal electronic communication can also be disguised by an appropriate choice of language and terminology.

The need for control and transparency, as well as the concern to be able to adapt one's own behaviour, matches the desire for education and information. Particularly with regard to the younger generation, who in the view of a number of participants often handle electronic media in an overly uninhibited and careless way, the call for clarification was loud and clear.

1 Introduction

Most recently following the revelation by the American whistle blower Edward Snowden to a stunned general public that their data were being spied on by the National Security Agency (NSA) on a large scale, not just experts but also the wider public now takes an interest in what's going on the Internet and in electronic communications. Correspondingly numerous were the applications received by TA-SWISS after the Centre had issued invitations to three citizen consultations whose brief was to look at the area of tension between the preservation of privacy and the use of surveillance technologies to protect national security and to combat crime. These consultations were part of the European project SurPRISE (Surveillance, privacy and security) and occurred simultaneously to similar consultation in eight other countries.

In Switzerland, actually three citizens consultations have been organised in order to deal with the linguistic diversity of the country. Each event dealt with two surveillance technologies: Deep Packet Inspection (DPI), which enables connection data and the contents of electronic communication to be spied on; and smartphone location tracking, which enables for people's geolocalisation to be detected via their mobile phones. The discussions focused on state surveillance, i.e. the use of appropriate technologies by authorities to protect national security. Participants were nevertheless free to go beyond this framework and during their exchanges they also tackled the use of surveillance technologies for private or commercial purposes.

The present report gives an overview of the discussions that took place during these three events by providing both quantitative and qualitative results related to related to DPI and Smartphone Location Tracking. In a first part (Chapter 2), the report presents the Swiss political system which has to be taken into consideration to understand the Swiss results of the Swiss consultation. It also describes the national security strategies and policies and the legal framework for surveillance activities and privacy in Switzerland. Chapter 3 describes the way citizen consultations have been organised in Switzerland: how participants were selected, who were the persons involved in running the consultation, what type of data have been gathered and how, etc.

The results of the three Swiss citizen summits are presented in Chapter 4, where figures relating to opinions on security, surveillance and privacy issues are complemented by qualitative statements from the participants. Throughout the chapter, the results of both the quantitative opinion survey and the discussions underline how important it is that surveillance technologies should be used in a reasonable way and within a clearly defined legal framework. In its conclusions (Chapter 5), the report puts the Swiss findings into perspective with some of the hypotheses made by the SurPRISE consortium. For instance, it was possible to confirm the hypothesis assuming that persons who feel personally secure have little sympathy for surveillance technologies. The working hypothesis whereby persons who are worried about their privacy are particularly strongly opposed to surveillance technologies, is likewise confirmed by the Swiss results.

2 Privacy, security and surveillance in in Switzerland

2.1 The Swiss democracy

Switzerland is a federal state of nearly 8 million inhabitants. Although in the centre of Europe, it is not member of the European Union. However, in practice, much of its regulation is based on European regulation, and the EU is the main economic partner of Switzerland. Another key feature of Switzerland is its direct democracy: several times a year, Swiss citizens vote on various subjects such as taxes, immigration policies, military affairs, social security issues, etc. As in other countries, they also elect their representatives at the federal, cantonal and municipal levels. The country's political organization is another specificity of Switzerland: power is distributed between the Confederation (the central State), the cantons (26) and the municipalities. Last but not least, Switzerland is a neutral State, so that the country cannot enter into military alliances and its army essentially has the function of defending the territory in case of an attack or for ensuring internal security. But neutrality doesn't prevent Switzerland from supporting humanitarian efforts in conflict situations worldwide and from being a member of supranational bodies such as UNO.

2.1.1 A decentralized political organisation

In Switzerland, state power is divided between the federal government, the cantons and the municipalities. The cantons and municipalities have wide-ranging powers and their own sources of income. Federalism is a key feature for the coexistence of the four linguistic cultures of the country (German, French, Italian, Romansch) and of the socio-economic diversity of the country.

There are in all 2396 municipalities in Switzerland. Municipalities have many tasks such as protection and support services, school buildings, social services, roads, local planning, etc. The level of autonomy of municipalities is ruled by each canton, and therefore varies considerably from canton to canton.

There are 26 cantons in Switzerland (six of them are actually half-cantons), each having equal rights with respect to the federal State. Healthcare, education and culture are policy domains which mainly rely under the authority of cantons. Actually, the cantons are responsible for all areas which are not formally attributed to the federal State. Each canton has its own Constitution, parliament, government and courts.

The Confederation is the name given to the Swiss federal State. It has responsibilities only in those areas where it is granted powers by the federal Constitution, for example in foreign and security policy, in customs matters and in defence.

The Swiss parliament has two Chambers, the National Council and the Council of States, which together constitute the United Federal Assembly. The National Council represents the overall population. It has 200 seats (the number of deputies from a canton depends on the size of its population). The Council of States represents the cantons and has 46 seats (two per canton irrespective of its population; and one seat for the 6 half-cantons). For each canton, the seats are distributed according to the principle of majority voting: the one or two persons with the most votes in their canton are elected. These two chambers reflect the two principles on which the structure of the Swiss State is based: the democratic principle of one person one vote, and the federalist principle allowing that all cantons are treated equally. The members of the National Council and the Council of States generally also have another job, so that their work as elected members is part-time. They usually meet for three-week sessions in spring, summer, autumn and winter, and committee meetings are held between sessions. This arrangement where representatives take on public tasks and mandates on a part-time basis is known in Switzerland as the militia system.

The Swiss government is organised as a Council (the Federal Council), constituted of seven members (federal councillors). The federal councillors are elected by the United Federal Assembly for a four-year term of office. The president is elected for one year only. Each federal councillor has equal rights as a member of the collegial body. The President chairs the sessions, but has no more rights than the other members. Decisions are made together. Once a decision is made, members of the Federal Council must

adopt a unanimous position, even if it is against their personal opinion or if their party disagrees with it. This is the so-called « consensus democracy ». The seven members of the Federal Council belong to the five main political parties and represent the various linguistic and cultural regions of the country.

2.1.2 The initiative or when citizens can foster change

Citizens may request that an amendment to the Constitution or to existing laws is put on ballot. At federal level, only proposals for constitutional amendments can be made, whereas in Cantons it is possible to request a new law or an amendment to the law. At federal level, the signatures of 100,000 voters who support the proposal must be collected within 18 months for an initiative to come about (in the cantons, the number of signatures is lower and differs from case to case, and is usually related to the number of inhabitants). The authorities sometimes respond to an initiative with a direct counter-proposal (generally less far-reaching). In the event that voters approve both the initiative and the counter-proposal, the vote is also about which text (the initiative or the counter-proposal) should be given priority. For an initiative to be accepted, it must be supported by a majority of voters and a majority of the cantons.

2.1.3 The Referendum or when citizens voice their disagreement

Citizens are entitled to have their say on parliamentary decisions at federal, cantonal and municipal levels. In most cases, a referendum has to be requested by citizens, but there are also cases where the referendum is compulsory (i.e. it takes place automatically, without citizens asking for it). At federal level, federal laws and decisions of Parliament, as well as certain international treaties, are subject to a referendum if 50,000 or more citizens request it. If the parliamentary decision concerns constitutional amendments or major international treaties, they are automatically put out to referendum.

The referendum gives a power of veto to citizens, as they can block amendments adopted by parliament or the government or delay their effect. Referendums also contribute to political agreement because they prompt parliament to include as many interested parties as possible in the debate on new laws or legislative amendments in order to reach a compromise and thus avoid the launch of a referendum.

2.2 Security policy and strategies in Switzerland

Swiss security policy is marked by the country's federal structure. While the government and the army ensure the integrity of the country with respect to various threats, the cantons - or municipalities - play an important role in maintaining security.

2.2.1 The role of the municipalities, cantons and the Confederation

Before 1848, the date of the creation of the Swiss federal State, Switzerland was a Confederal State: each canton was a sovereign State with its own laws, its own currency and its own armed forces. This situation has influenced the way security has been organised in Switzerland since 1848, when the Federal State was established. While the cantons could not rule their own army, they kept their police forces. Nowadays, each canton has its own police force, which ensures respect for the laws and maintains order and the security of the people. Their authority covers multiple areas: traffic control, searching for people and objects, emergency interventions, etc. Depending on the canton, there are also local and municipal police forces, which are mainly in charge of community policing.

The Confederation's role with respect to security mainly concerns the defence of territorial integrity. The government is in charge of the army, whose mission is defensive as Switzerland is a neutral State. The strategic and preventive security tasks are covered by the Federal Intelligence Service, which was created in 2010 after two services have been amalgamated, the Strategic Intelligence Service and Service for Analysis and Prevention. The federal State also has its own police (the Federal Office of Police or fedpol), which is in charge of criminal investigations conducted under federal jurisdiction (such as crimes related to organised crime, money laundering and terrorism).

In the 1990s, with the end of the cold war period, the Swiss government established some links between its own security structures and the cantons to better cope with the new threats that emerged at that

time (mostly non-military threats). Since 2012, the cantons and the Confederation have been involved in the "Sicherheitsverbund Schweiz" (Security Alliance Switzerland). This coordination structure is a follow-up to the 2010 report of the Federal Council on security, in which it is stated that "the security policy covers all measures taken by the Confederation, the cantons and municipalities to prevent, dismiss and control the threats and politico-military or criminal actions aimed at limiting the power of self-determination of Switzerland and its people or harm them".[2]

2.2.2 Threats and dangers and related security strategies

The federal intelligence service (FIS) regularly publishes a situation radar, which offers an overview of the present and future security threats for Switzerland. In its latest report, published in 2014[3], the situation in Switzerland in terms of security is considered as safe and stable. Nevertheless, some threats are being considered, such as the fact that the country is the target of illegal intelligence activities: "The possibilities for illegal information gathering by intelligence services have taken on a new dimension, especially in the light of close cooperation between the USA and key technology companies, which may even extend to the corruption of product security. The problems go beyond illegal intelligence, as not only can data be gathered, but can also be altered or destroyed". The report also points out the changes in the strategic environment of Switzerland: "Switzerland's strategic environment is shaped partly by the transformation of the international system, triggered by the gradual shift in the balance of power eastwards to Asia and to the South. In addition, in our immediate environment we are still faced with several years of crisis management in order to overcome the European debt crisis and the consequences of the Arab Spring. Russia is consolidating its position politically, economically and militarily and is increasing its influence, particularly in Europe". The report does not consider terrorism and extremism to be major threats for Switzerland ("Switzerland is still not a priority target for jihadist attacks"), but it acknowledges that Swiss citizens may be at risk in areas of conflict in the Islamic world. It also considers the risks that persons coming to Switzerland from these areas of conflict may commit attacks or be involved in jihadist recruitment.

Security strategies are enacted by the Federal Council, which regularly submits a report to Parliament on its security policy. Such reports analyse the context and likely developments in order to set the direction for the Swiss security policy and its implementation instruments. In its last report, dating from 2010[4], the Federal Council defines security policy as a tool to protect the ability to act, self-determination and the integrity of Switzerland, its population and its conditions of existence against threats and direct or indirect hazards. It is also the task of security policy to contribute to stability and peace beyond borders.

Threats and dangers identified by the Federal Council for its security strategy are of a diverse nature, and can affect the security of the country and of the Swiss population in many ways. These are emergency situations caused by natural or human-caused disasters, supply difficulties due to international conflicts, military attacks (very low probabilities), economic constraints, illegal activities of intelligence services, attacks against IT and communication infrastructures, terrorism, violent extremism, organised crime, use of force against life and physical integrity. The Federal Council also considers some indirect threats, which may have an impact on the country's stability: proliferation of weapons of mass destruction, the collapse of States in some parts of the world, migration issues, climate change, pandemics and demographic changes are all included in the Swiss security strategy.

The governmental security strategy of Switzerland is deeply characterized by the federal structure of the country. The core of the strategy is to constitute a national security network allowing for efficient interaction between the Confederation (federal level), the cantons and the municipalities. Cooperation with other States and international organisations is also central to the Swiss security strategy.

---

2 Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweiz vom 23 Juni 2010 (http://www.news.admin.ch/NSBSubscriber/message/attachments/19697.pdf)

3 Federal Intelligence Service FIS, 2014. Switzerland's security : Situation report 2014, Berne (http://www.vbs.admin.ch/internet/vbs/en/home/documentation/publication/snd_publ.parsys.75250.downloadList.29258.DownloadFile.tmp/ndbsicherheitschweiz2014webe.pdf)

4 Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweizvom 23 Juni 2010 (http://www.news.admin.ch/NSBSubscriber/message/attachments/19697.pdf).

Implementation of this strategy is based on several means. First of all, Swiss foreign policy is considered as a crucial element: as it promotes stability, peace and security in regions affected by conflicts and crisis, it actually enhances Swiss security in a globalised and interconnected world. Foreign policy includes peace and the promotion of human rights, development cooperation and humanitarian aid, neutrality, etc. The Swiss army is also a central strategic resource for the governmental security strategy, as it can be deployed in case of an attack and can also be used to help civil authorities when the appropriate resources are lacking (for instance in case of catastrophe or major civil troubles). There is an obligation to serve in the army, so that the majority of Swiss male citizens perform their military service and can be mobilized. Other means of promoting security in Switzerland are related to population protection against catastrophes and emergency situations (involving the engagement of police, firefighters, technical services, civil protection service), to intelligence services, to economic policy (as enhancing the country's welfare and stability), to police forces and to customs administration.

Switzerland, in common with most other European countries, thus has a holistic security policy, which is no longer limited to the concept of defence and control of violence against the national territory, but includes many other direct and indirect threats and dangers that may affect both the country and the lives or physical integrity of individuals. In that sense, security policy is viewed as a responsibility of many actors at federal, cantonal and municipal levels. It is also interconnected to other policies, such as foreign and economic policies.

2.3 Surveillance in Switzerland

Due to the federal organization of the country, both the cantons and the Confederation are entitled to conduct surveillance activities. These activities are, however, subject to a strict legal framework, which has evolved over time. As a general rule, cantonal surveillance aims at internal security, whereas federal surveillance aims at external security. Surveillance can be ordered for preventive and repressive purposes, and can use many measures, from traditional ones such as interception of post or wiretapping to more recent and sophisticated ones such as video surveillance, biometrics or drones.

The Federal Intelligence Service (FIS) is a major instrument of security policy in Switzerland and is in charge of surveillance activities. This service resulted from a merger of the Service for Analysis and Prevention with the Strategic Intelligence Service in 2010. It conducts research information and analyses for the Federal Council, the federal departments (ministries), the executive bodies responsible for security (Security Committee of the Federal Council and Security Core Group) and the military leadership. It also assists the cantons with the task of safeguarding internal security and supports the law enforcement agencies at federal level. It also provides information to cantonal bodies, and also assists government bodies and private organizations with counterespionage. Finally, it informs Parliament, the cantons and the public about the internal and external security situation (cf. the FIS "Situation radar", see section 2.2.2). The FIS is supervised by the Parliament, the Federal Council, the Federal Administration and the Federal Department of Defence, Civil Protection and Sport.

2.3.1 Legal situation

The functions and activities of the Federal Intelligence Service are regulated by the Federal Act on Measures to Safeguard Internal Security (ISA) and the Federal Act on Responsibilities in the Area of the Civilian intelligence Services (CISA). The Federal Act on Measures to Safeguard Internal Security was adopted in 1997 and gives the federal government a mandate to take the necessary preventive measures for early detection of hazards associated with internal and external security. In this respect, it allows the federal authorities – actually the Federal Intelligence Service – to search information, i.e. undertake surveillance activities. The Federal Act on Responsibilities in the Area of the Civilian intelligence Services, for its part, concerns the collection of intelligence about foreign countries for external security and assigns this role to the Federal Intelligence Service (FIS). It also assigns to the FIS the task of comprehensive threat assessment.

These two acts are currently being revised so as to merge them on a new Intelligence Service Act. In February 2014, the Federal Council submitted a proposal to Parliament for an Intelligence Service Act. According to this proposal, the Act should provide a comprehensive legal basis for the FIS and stipulates

the conditions and basic principles according to which the intelligence services fulfil their mandate. Compared to the current situation, it makes a distinction between violent extremism taking place in Switzerland and other threats. It also introduces new measures for information retrieval (e.g. monitoring of postal traffic and telecommunications, including computers) in the fields of terrorism, espionage, proliferation and attacks against critical infrastructure or for safeguarding other essential interests of Switzerland. These measures should, however, only be used if they have been authorized by the Federal Administrative Court and the Head of the Federal Department of Defence, Civil Protection and Sport, after consultation of the Security Committee of the Federal Council. The proposal also includes provisions about data collection and treatment, so that data can be stored in different systems according to the theme, the source and their sensitivity. Finally, the Act proposes an extended control of the FIS activities by the Parliamentary Control Delegation, the Parliamentary Finance Committee, the Federal Department of Defence, Civil Protection and Sport, and the Federal Council. This proposal for an Intelligence Service Act is currently being discussed by Parliament. It is coming under considerable criticism from advocates of privacy and civil rights, who consider that the proposal is going too far by expanding the areas where intelligence services can intervene and the means of investigation. There are also some formal criticisms related to the control procedures of the FIS.

In case of criminal investigation, the Federal Act on Surveillance of Post and Telecommunications determines the cases in which the law enforcement authorities can intercept phone calls and mails: it sets conditions and exhaustively lists offences justifying the implementation of such surveillance measures. Outside of criminal proceedings, surveillance measures can also be ordered in the search for missing persons if their life or health is in danger. The act also governs the activities of the Federal Unit in charge of the surveillance of Post and Telecommunications (Service chargé de la surveillance de la correspondance par poste et télécommunication - SSCPT) and the tasks of operators providing postal and telecommunication services. For instance, the act stipulates that phone and internet providers should keep their customers' data for a period of six months. It is important to note that surveillance mandates are subject to judicial approval. The Federal Act on Surveillance of Post and Telecommunications is currently under revision in order to cope with technological developments, and especially the major role of the internet in communications. The Federal Council proposed a project for revision to Parliament in February 2013, which includes provisions for the use of governmental spyware (GovWare) under certain conditions (particularly serious offences). The amendment also proposes that the retention period for secondary data should be increased from six to twelve months. This revision project is currently being discussed by Parliament. The States Council adopted the project in March 2014, and it is now[5] being examined by the National Council. As in the case of the Intelligence Service Act, this project has attracted considerable criticism and a referendum has already been announced in case Parliament adopts the Act.

Other laws regulate the surveillance activities of public authorities, such as the Federal Act on police information systems (Loi fédérale sur les systèmes d'information de police) which regulates the treatment of personal data within the framework of national or international inquiries, the Federal Act on customs (Loi sur les douanes) regulating the use of various surveillance devices and the Foreigners Act (Loi sur les étrangers) allowing the use of biometric face recognition systems.

2.3.2 DPI, smartphone location tracking and video surveillance in Switzerland

According the current legal situation, Deep Packet Inspection for State surveillance is not allowed for Swiss authorities. The Federal Act on Measures to Safeguard Internal Security (ISA) rules the means available for the Swiss intelligence service. In that law, the use of technical surveillance such as DPI or smartphone location tracking is not provided, meaning that these two technologies cannot be used for surveillance purposes. However, Edward Snowden revelations about surveillance activities of the NSA showed that the United States – and maybe other countries - had some illegal surveillance activities in Switzerland based on sophisticated technologies. This gave raise to hatred political debates and

[5] Summer 2014.

headlines in the media, and the authorities are currently investigating to what extent Swiss citizens are surveilled by foreign governments.

Smartphone location tracking by State authorities is permitted only in the context of legal and criminal investigations, and has to be authorized by a judge. As for DPI, it cannot be used by intelligence services, which have to rely on other legal means (cf. Federal Act on Measures to Safeguard Internal Security). The situation is of course different with private and commercial actors, as they may collect and use location data for their commercial activities. In this case, they have to comply to the Federal Law on Data Protection, which regulates collection and processing of data by private bodies and federal agencies (see section 2.4.1).

Video surveillance (CCTV) is also subject to strict rules. When private individuals install CCTV cameras, for example to protect people or deter acts of vandalism, this is governed by the Federal Act on Data Protection if people appearing on the recorded images can be recognised. Where CCTV cameras are installed and run by cantonal or local authorities, cantonal legislation usually applies. This may differ from canton to canton, but is essentially based on the provisions contained in the Federal Law on Data Protection. At federal level, there is no legislation about video surveillance. But several regulations (ordinances) regulate the use of CCTV cameras in trains, public transport, railway stations, airports and custom offices. The Confederation also enacted some recommendations based on the Data Protection Act and the Labour Act.

2.4 Privacy in Switzerland

In Switzerland, the protection of privacy was incorporated into the legal system in 1912, as a general right of personality in article 28 of the Civil Code. This guarantee includes the protection of personal image and other rights of defence.

The concepts of data protection and of informational self-determination appeared later, in the second half of the 20th century, with the development of information and telecommunication technologies and the multiplication of data processing, the increase of personal information being disseminated and the related risks of privacy infringement. In 1976, the canton of Geneva was the first authority to recognize the need to protect the personal data of its citizens with the adoption of the Cantonal Act on the protection of information automatically processed by computer. Other cantons adopted similar legislation in the following years and decades, and the pioneer cantons such as Geneva revised their legislation so as to make allowance for technological developments. At federal level, the Act on Data Protection was adopted in 1992 and privacy protection became a Constitutional right in 1999, as part of the new revised Constitution that was adopted that year. Article 13, dedicated to the right to privacy, states that “Every person has the right to privacy in their private and family life and in their home, and in relation to their mail and telecommunications" and that "Every person has the right to be protected against the misuse of their personal data".

2.4.1 The Federal Act on Data Protection

It took more than 20 years between the first Parliamentary intervention in 1971 demanding “to protect citizens’ privacy against the misuse of computers” and the final adoption of the Federal Act on Data protection in 1992. Several experts and commissions were involved in establishing the principles and writing a legislative text that would achieve a large consensus among both public and private actors, while taking into account the cantons’ sovereignty in the areas covered. The law governs the collection and processing of data by private bodies and federal agencies. Its aim is to protect the privacy and fundamental rights of persons whose data are collected and used. More specifically, its goal is to protect private and family life against violations, protect personal information related to the exercising of fundamental rights and prevent individuals from being reduced to simple information objects (individuals must be able to determine the image and information they want to share with their environment)[6]. Data processing by the cantonal authorities is not subject to the Federal law on data protection and is regulated by cantonal legislation.

[6] Message du Conseil fédéral concernant la Loi sur la protection des données du 23 mars 1988.

The Federal Act on Data Protection has undergone several revisions since it came into force in July 1993. Their aim was mainly to adapt the law to related acts and governmental decisions, for instance in the domain of police and judicial cooperation. There was also a need to adapt Swiss legislation to the privacy standards of other European countries, especially with regard to the Schengen Convention (Switzerland signed an association agreement to Schengen/Dublin Convention in 2004).

In 2011, the Federal Council published a report assessing the Federal Act on Data Protection[7]. In this report, the government suggests that technological developments in recent years have led to new threats. The multiplication of non-transparent and cross-border data processing is referred to: in the current technological environment, it is becoming increasingly difficult to keep control of personal data once it is disclosed. The government is also considering related societal developments. In particular, it observes that whereas the general public attaches great importance to the protection of privacy, this is not always followed by concrete protection actions in everyday life, as individuals often feel overwhelmed or do not know how data are used and what the associated risks are. The Federal Council also recognizes that the possibilities of intervention of the Federal Commissioner for Data Protection are limited and that affected individuals rarely exercise their right of appeal.

On the basis of this report, the Federal Council commissioned the Federal Department of Justice and Police to review, by the end of 2014, the possibilities for strengthening the Federal Act on Data Protection. The review should consider the ways to increase transparency of data processing and to make users more aware of the risks related to personal data processing. The review should also consider data protection from the design phase of new technological tools ("privacy by design") and consider whether the role of the Federal Commissioner for Data Protection should be enhanced. A group of experts has been nominated to consider these questions, and depending on its conclusions, the Federal Council will then propose a revised version of the Federal Act on Data Protection, which will then have to follow all the legislative steps (consultation phase, inclusion of comments from the consultation phase, parliamentary debate, decision and, if demanded, referendum).

2.4.2 The Data protection commissioners

With the adoption of the Federal Act on Data Protection in 1992, the position of the Federal Data Protection and Information Commissioner was created. The Swiss Federal Data Protection and Information Commissioner (FDPIC) is appointed by the Federal Council and supervises the compliance by Federal authorities with the Federal Act on Data Protection. The Commissioner also has a mandate to advise public and private bodies in the field of data protection and to inform the general public. To accomplish his tasks, the Commissioner may investigate facts on his own initiative or at the request of a third party. He may then issue recommendations based upon these investigations. In the private sector, the Commissioner mainly has a consultative function. In particular, he clarifies and comments on the legal provisions about Data Protection, offers advice on the registration of data files, the registration of cross-border data flows, and requests for the right of access. He also gives advice on questions concerning legal problems or technical aspects of data security. In conflict situations between private bodies or between private persons and federal bodies, he acts as an "ombudsman" and tries to find solutions. In 2013, the Federal Data Protection and Information Commissioner had an annual budget of CHF 5,508,900 (about EUR 4,500,000) and his staff comprised 28.5 full-time positions.

Each canton (26) also has a Data Protection Commissioner (some cantons collaborate on that matter and have a common Data Protection Commissioner). However, their budget is often very limited and their staff is small (it is less than one full time position in small cantons, and less than 3 full time position in other cantons). The canton of Zurich is an exception, with an annual budget of CHF 2 millions (about EUR 1.65 mios) for the Data Protection Officer and a staff comprised of 8.2 full-time positions[8].

---

7 Rapport du Conseil fédéral sur l'évaluation de la loi fédérale sur la protection des données du 9 décembre 2011 (http://www.admin.ch/opc/fr/federal-gazette/2012/255.pdf)

8 Rudin, 2009.

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

2.5.1 The files scandal – emergence of a public discourse on State surveillance

The protection of privacy emerged as an important issue in the public debate at the end of the 1980s, when a Parliamentary committee discovered the existence of a large number of files illegally constituted. Since the beginning of the 20th century, about 700,000 persons had their daily activities traced in more than 900,000 files for state security reasons. Originally, the files mainly concerned German Nazis and Swiss engaged in the popular front during the Spanish civil war. Then, during the cold war, the files recorded activities of communists and then, over the years, included all kinds of political activists.

The report of the Parliamentary committee came rather as a shock to the political parties and public opinion. 35,000 people staged a demonstration in front of the Federal Palace to voice their anger. As a response to the heated criticism from the media and public opinion, the government decided to open the files to the citizens concerned. At the same time, an initiative requiring the abolition of the political police and the prohibition to monitor anyone in the exercise of their opinions and political rights («S.o.S.- pour une Suisse sans police fouineuse») has been launched and, in 1991, successfully submitted to the Federal Chancellery (the vote took place in 1998 only).

This files scandal led to major reorganisations of the Federal police and the services of the attorney general in the early 1990s. In particular, the Federal police is now controlled by Parliament, and the surveillance of individuals for State security has to follow strict quality control procedures. This strong response to the scandal have reassured Swiss public opinion, which in 1999 rejected the initiative "S.o.S – pour une Suisse sans police fouineuse" by 75.4% of the votes.

2.5.2 State surveillance: still a sensitive issue

The level of opposition to State surveillance was certainly at its peak during the files scandal. Nevertheless, since then, it is still a sensitive issue in the media and public opinion. In 2010, for instance, the Parliamentary commission in charge of controlling the Federal Police discovered that the intelligence services had accumulated unnecessary, inaccurate and outdated files. These revelations sparked media headlines, but the government was able to circumvent the scandal by rapidly taking appropriate measures.

The introduction of the biometric passport in 2010 is another example of public sensitivity with respect to State surveillance. During the discussions in Parliament, the parties of the Left (Social Democrats and Greens), together with some elected from the nationalist party (UDC) criticized the introduction of a biometric passport, and especially the fact that the digital pictures of citizens will be stored in a central database. This was not enough to prevent the Parliament to adopt the biometric passport, but opposition was strong enough to launch a referendum and collect the 50,000 signatures demanding a popular vote on the issue. Finally, the introduction of the biometric passport was accepted by 50.14% of the Swiss electorate, which was enough for the biometric passport to be introduced one year later but shows how sensitive an issue State surveillance is among the public.

The current revision of the Federal Law on Surveillance of Post and Telecommunications (see section 2.3.1) is also generating strong criticism, especially from professionals but also from a concerned public. For instance, the Association of IT providers is opposed to the extension of the data retention time to 12 months instead of 6. Other organisations and political parties are also against this revision, and large parts of the population seem to be reluctant. For instance, the newly created Pirate Party launched a petition against this revision which was signed by about 10,000 persons in a period of three months. The party announced that if the revised law is adopted by the National Council, it will consider launching a referendum. It may be joined by other parties if it does so.

The new Federal Act on Intelligence Service, even though in a less developed stage (it is currently being discussed within Parliamentary committees and content of the discussions are not publicly available),

might also give raise to debate and opposition. Some politicians already publicly stated their opposition to this new law, as well as some political parties (especially left wing parties and the Pirate Party). According to them, the new prerogatives given to the Intelligence service would impede with privacy, without contributing to security.

2.5.3 Security and public opinion

In the last two decades, security threats to physical integrity have become a major political issue. Large proportions of the public are concerned about assaults, robberies, drug trafficking and acts of vandalism. Surveys show a real public concern about security. In 2013, the "Credit Suisse worry barometer" measuring the main concerns of the Swiss population shows that 24% of the population is concerned about personal security[9]. This ranks personal security fifth among concerns, after unemployment (44%), immigration (37%), retirement provision (29%) and asylum issues (28%).

Other surveys, however, show that all in all, Swiss citizens feel safe in their country. This is for instance the case of the 2013 report on security from the Centre for Security Studies of the Swiss Federal Institute of Technology, which shows that 89% of Swiss citizens feel safe[10]. The report also shows that the Swiss population is basically supportive towards measures to maintain internal security, such as fighting and penalizing hooliganism (85%), monitoring the share of foreign nationals (76%) as well as using the armed forces to ensure law and order (77%). The population is, however, divided on measures such as intensive surveillance of phone calls (51% reject it) and of private computers (52% reject it). This survey also demonstrates that Swiss citizen trust their authorities, especially the police (mean value of 7.6 on a 1 to 10 confidence scale) and the courts (mean value of 7.1), the Federal council (mean value of 6.7) and Parliament (mean value of 6.3). The security policy of the Confederation is, in the whole, supported by the Swiss population. Four out of five respondents think that it is important to increase the fight against right-wing extremism (81%), but only 63% think the same for left-wing extremism. The idea of restricting personal freedoms in the fight against terrorism is supported by 66% of the respondents. The role of the army remains uncontested, as 62% of the Swiss electorate think it is important to have strong armed forces and 67% of the respondents demand well-equipped and trained armed forces.

2.5.4 The case of video surveillance

As in many European countries, the use of video surveillance has been increasing in recent years in order to fight crime and violence in public or private spaces. A majority of the public seems to accept these cameras as a tool to increase their personal safety, even though experts, NGOs and important parts of the public criticize their use and their effectiveness for preventing and fighting crime. In 2007, for instance, the installation of CCTV cameras in the canton of St. Gall had been contested in a municipal referendum: in the end, 63.3% of the voters in the city approved the CCTV project. Similar votes took place in other municipalities: in Yverdon (a small city in the French-speaking part of the country), 56.4% of the voters accepted a CCTV project in 2009, and in Renens (a municipality near Lausanne) 56% of the voters accepted a similar project in 2011.

[9] Crédit Suisse, 2013. What concerns the Swiss? What is important to them?, 1/2013 (https://publications.credit-suisse.com/index.cfm/publikationen-shop/worry-barometer/2013-what-concerns-the-swiss-what-is-important-to-them/)

[10] Szvircsev Tresch, Tibor et al. 2013. Sicherheit 2013. Aussen-, Sicherheits- und Verteidigungspolitische Meinungsbildung im Trend, Center for Security Studies und Militärakademie, ETH Zurich.

3 Process design – the citizen summit in Switzerland

In Switzerland it proved especially challenging to organise how SurPRISE would be carried out. Unlike the other project partners, each of which only had to organise one discussion event, three were held in Switzerland, one each in German-speaking (in Zurich), French-speaking (Grandson) and Italian-speaking Switzerland (Lugano).

3.1 Recruitment of the citizen panels

The recruitment strategy for the SurPRISE citizen summit aimed at setting up a group of 200 to 300 citizens who reflected the national demographic in terms of age, gender, educational level and occupation. Moreover, the group had to be constituted of laypersons, who were not professionals in the area of surveillance, privacy and security. In order to be able to be able to constitute such a large and heterogeneous group, TA-SWISS chose a combination of different methods for the participants' recruitment. Moreover, in order to increase the motivation of the people contacted, it had been decided to cover all travel expenses of the participants and give them an incentive payment of CHF 80 (about EUR 60) if they participated in the event.

First, TA-SWISS sent contact letters to 45,000 randomly selected citizens, 15,000 in each linguistic region of the country (we rented their post addresses to a private marketing company). Information about the project and the recruitment process has also been published on the TA-SWISS website, in the TA-SWISS newsletter and on Facebook. Moreover, members of the TA-SWISS networks (advisory group, steering committee) have been contacted to promote the event (one politician tweeted about the citizen summit). TA-SWISS also invited all the citizens who had already participated in previous participatory events in the last decade (about 120 persons). Finally, flyers were created and distributed in different places such as supermarkets, universities and other public spaces. In order to motivate potential participants, a incentive payment of about EUR 65.- (CHF 80.-) had been offered to participants.

The 45,000 citizens who were contacted via mail received, as well as the invitation letter, an information folder, an application form and a consent form. The information folder gave all necessary information about the project and some practical information about the citizen summit (how to get reimbursed, location of the event, timing, etc.). Those who heard about the event by other means could download these documents from the TA-SWISS website. Interested citizen had to fill in and send the application form and the consent paper. On the application form, they were asked to provide some personal information (address, age, gender, occupation, education) as well as their motivation for participating in the event. By signing the consent form, interested persons authorised TA-SWISS to store their information until the citizen summit or, if they wished, by the end of the project with the publication of the report.

All these efforts resulted in more than 1300 registrations for the three events (500 for the Swiss German citizen summit, 550 for the French-speaking summit and 260 for the Italian summit). A group of 110 persons was selected for each citizen summit. This was more than the number of participants that TA-SWISS was able to host, but previous experiences of participatory methods showed that between 10 to 20% of the people selected failed to show up at the event. The 330 participants were selected on the basis of the information on age, gender, education and occupation provided in the application form[11]. The motivation of the persons who registered was also considered, but only as an eliminatory criterion: persons having a kind of expert motivation were not selected.

The selected citizens received a confirmation letter about two weeks before the summit, as well as an information magazine (provided by the SurPRISE consortium and translated in the appropriate language) and details about the programme for the meeting. They also received a consent form which they were asked to sign and bring to the summit (by signing this consent form they agreed that their data would be anonymously gathered during the event, and used for the national report). The citizens who were not selected received an e-mail thanking them for their interest.

[11] Occupation was mostly used to exclude some persons who could be considered as experts in the topic.

Finally, on the day of the citizen summits, 88 persons attended the German-speaking citizen summit, 91 the French-speaking citizen summit and 75 the Italian-speaking citizen summit (a total of 254 participants).

3.2 Three similar events

In all the regions of Switzerland, the summits were conducted following the same programme and structure. DPI and Smartphone location tracking were the two technologies put under discussion, and the programme of the day was the same as in other SurPRISE countries.

In Zurich, the event took place in the aula of a regional educational centre for adults, ideally located nearby the city center. In Grandson, the location of the event had an impressive view of Lake Neuchâtel. The room was ideal for the purpose with its nice location, optimal size, large screen, and a supplementary room for the buffet and coffee break, registration, cloakroom facilities and space for the moderators briefing. In Lugano the event took place in the "aula magna" of the University. It was very spacious and had a very big lobby with plenty of room for the buffet and coffee break, registration and cloakroom facilities.

For each event, on arrival in the morning, participants received an empty name tag where they could write their name or any other name if they wished to remain anonymous, a folder with a short programme for the day, templates to write notes during the discussion rounds or personal remarks they would like to share with the organisers, a clicker (for the voting system) and a form for the reimbursement of travel expenses and of the incentive payment. They were also told at which table they should sit (organisers had prepared a seating plan in order to mix the different profiles of the participants). Participants had to hand over the completed and signed consent from, which had been sent to them together with the confirmation letter (there were a few additional copies of the consent form for those who had forgotten to bring it with them).

In Zurich, the summit was opened by the managing director of TA-SWISS, who also gave the closing speech. The Data protection officer of the canton of Zurich (and also member of the Swiss advisory group of the project) attended the first part of the meeting and spoke briefly to the participants just before the lunch break.

In Grandson, the project coordinator opened and closed the summit. A journalist from the Swiss-French daily newspaper "Le Temps" attended the summit and wrote an article about it. As in Zurich, one member of the Swiss advisory group of the project attended the meeting, but didn't come to speak. One of the reviewers of the SurPRISE project appointed by the EU also showed up for a couple of hours.

In Lugano, the summit was opened by the mayor of Lugano and by the rector of the University of Ticino, which hosted the event. The closing speech was given by the president of TA-SWISS, who is a former politician from the canton of Ticino.

3.3 Structure of the citizen panel

By comparison with the SurPRISE panels in the other participating countries, all three Swiss discussion rounds were characterised by a comparatively strong presence of persons with a higher level of education (see Table 1: Socio-demographic structure of participants (percentage)). Also well represented were employed people holding a senior management position. The same was true of well-trained persons, once again corresponding to demanding professional activities. By contrast, the two youngest age groups were clearly under-represented, at 5 (for the 18-29 age group) and 10 percent (30-39 age group) (compared to an average of 17 and 14 percent respectively for all countries). This imbalance was noted in all discussion rounds and sometimes commented on: «It is a shame that the 18-30 age group is under-represented. If there had been more young people, the outcome of the discussion would certainly have been very different», commented someone from Zurich, with similar comments made in Lugano and Grandson. To counter this deficiency in the sample, some of the results – especially in the questions about protecting privacy, which were particularly important for the project – were analysed by age groups.

	Participants in all Switzerland *N=254*	Participants in German part *N=88*	Participants in French part *N=91*	Participants in Italian parts *N=75*
Total	254	88	91	75
Age				
18-29	13	4	5	4
30-39	25	12	10	3
40-49	63	22	22	19
50-59	67	21	24	22
60-69	62	22	18	22
70+	17	1	7	5
n.a	2	1	1	0
missing	5	1	4	0
Gender				
female	102	34	38	30
male	142	50	48	44
n.a.	3	2	1	0
missing	7	2	4	1
Education				
primary school	2	0	2	0
lower secondary	5	2	1	2
upper secondary	15	3	4	8
vocational qualification	51	15	13	23
university – undergraduate	92	43	27	22
university – postgraduate	79	20	40	19
n.a.	3	2	1	0
missing	7	3	3	1
Living area				
live in a metropolitan area	29	15	14	0
live in an urban area	102	32	36	34
live in a rural area	112	39	36	37
n.a.	2	0	1	1
missing	9	2	4	3
Children at home aged 16 or under				
yes	72	25	25	22
no	170	59	59	52
n.a.	4	2	2	0
missing	8	2	5	1

Table 1: Socio-demographic structure of participants (percentage)

To make allowance for the under-representation of young people, the results were partly assessed by age groups – especially in respect of questions about the protection of privacy, particularly important for the project. Moreover, an evaluation based on age was carried out on all of the data series from the other countries participating in SurPRISE, to determine whether inter-generational differences really do exist. The results are not easy to interpret; nevertheless, they do not in any way allow one to conclude that the young generation would in general attach less importance to privacy or regard security issues differently. Hence 62% of 18 to 29 year-olds accept the contention that security technologies encroach on privacy in general (29% «strongly agree», 33% «agree» with the statement). In the 30 to 39 year age group the figure is 70% (42% «strongly agree», 28% «agree»), and in the 40 to 49 year age group, 63% are worried about their privacy (33% «strongly agree», 30% «agree»). It could not be said that this preoccupation grows with age, because in the 50 to 59 year age group, 62% are concerned about the protection of their privacy, 65% in the 60 to 69 year age group, and 55% in the 70 years and over age group. Moreover, evaluations based on age for the transnational SurPRISE sample (totalling 1773 persons) suggest that if more young people had taken part in Switzerland, the results would not systematically deviate from those currently available.

The Swiss panel constitutes a «special case» in yet another connection: while the proportion of indigenous people across all participant countries averaged just below 89 percent, the figure in Switzerland was just under 79 percent; in the French- and Italian-speaking areas of the country in particular, a lot of people with a foreign passport took part in SurPRISE. These figures reflect the demographic composition of the resident population in Switzerland, which according to the Federal Statistical Office at the end of 2013 recorded the proportion of foreign nationals as 24 percent[12].

The ratio of the sexes showed a slight preponderance of men, with the composition of the discussion round in Grandson, with 55 percent of men and 44 percent of women (some persons didn't answer this question), was the most balanced. The variety of professions, by contrast – from the category of administration and sales, via technical professions to agriculture and forestry – might well reflect the panels, even if in this respect, too, the strong presence of senior functions was once again evident.

3.4 How citizens assess the summit

All the three Swiss summits went very well and in a good atmosphere, with however some differences. The majority of the participants felt welcome and enjoyed participating at this event. They liked the different parts of the day (voting, discussion and films). In Zurich, the participants were strongly interested in the results of the voting, and they also reacted to the feedback charts with laughter or expressions of surprise. Interactions between the head facilitator and the participants as well as between the tables were very positive, so that the whole event was not only a major event consisting of 13 groups of people but it also functioned as one big group. In Grandson and in Lugano the atmosphere was also good but some participants complained that the voting part took too long. They would have preferred to have more discussion and less voting. The participants were nevertheless very interested in the result of the voting.

With regard to the discussion round, most participants were satisfied with it. They appreciated being able to exchange their ideas with other participants. Some participants would have liked to change the composition of the group for the second technology, so as to have more exchanges with their pairs. Regarding the recommendations round, the participants liked the idea of writing one recommendation for the table, even though it proved difficult to stay with one recommendation.

In respect of the questionnaire also a few critical comments were raised, some participants found the questions were kind of manipulative. The set of questions saying "I worry that…" came in for particular criticism: these questions created a feeling of fear and were criticized for not being neutral enough. Other questions were also criticized for being formulated in such a way that the results were quite obvious and could be guessed in advance. Some participants also expressed their ambivalence about the issues at stake and their difficulties to give a single answer (for them, the middle category or the don't know answer were not appropriate to show their ambivalence). It had also been pointed out that the questions didn't ask about opinions related to the commercial use of the technologies, which is also

[12] Source: STATPOP, Federal Statistical Office: http://www.bfs.admin.ch/bfs/portal/de/index/themen/01/02/blank/key/alter/nach_staatsangehoerigkeit.html

an important dimension of the topic. All in all, such critics mainly have been expressed during the events in Grandson and Lugano (so in the Latin region of the country). Moreover, many participants (especially in Grandson) wrote some individual comments on postcards provided by the organisers, which can be understood as a signal that they didn't feel that their voice will be heard via clickers and table discussions.

In a last session of the meetings, participants were asked to give their own evaluation of the process. All in all, 85% of the participants considered that they have gained new insights by participating in the citizen summit (see Figure 1: "I have gained new insight by participating in the citizen summit" (percentage, N=246)(all Switzerland)). But only 31% agreed or strongly agreed that the meeting had generated valuable knowledge for politicians (see Figure 2: I believe the citizen summit has generated valuable knowledge for the politicians" (percentage, N= 243) (all Switzerland)). Moreover, 32% of all participants said that they changed their mind during/after the event, with 26% having more negative opinions towards surveillance technologies and 6% more positive opinions (see Figure 3: "Has this experience changed your attitudes regarding security oriented surveillance technology?" (percentage, N=247) (all Switzerland)).

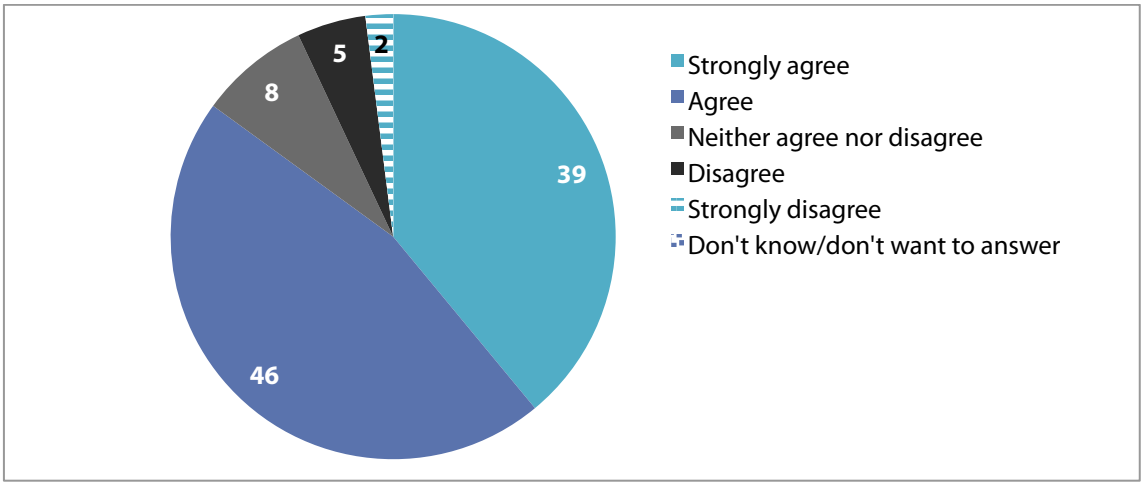

Figure 1: "I have gained new insight by participating in the citizen summit" (percentage, N=246)(all Switzerland)

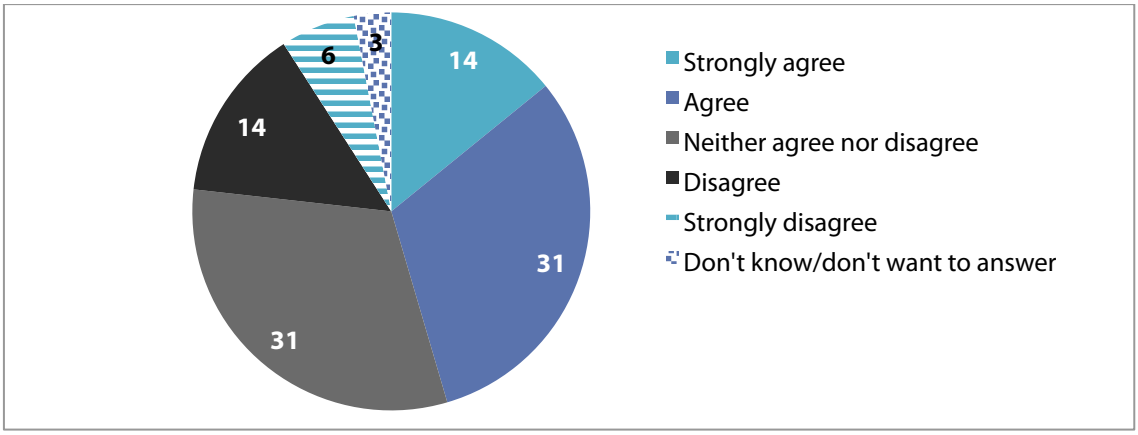

Figure 2: I believe the citizen summit has generated valuable knowledge for the politicians" (percentage, N= 243) (all Switzerland)

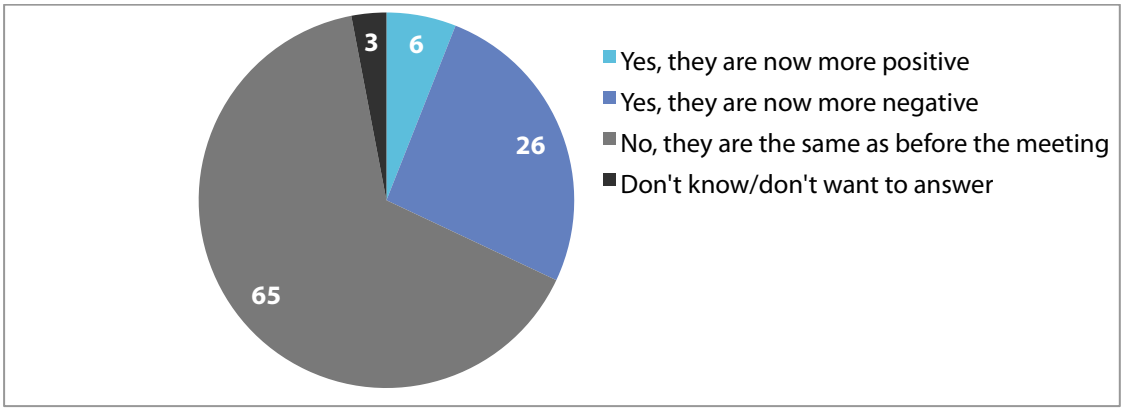

Figure 3: "Has this experience changed your attitudes regarding security oriented surveillance technology?" (percentage, N=247) (all Switzerland)

4 Empirical results of the citizen summit

4.1 Switzerland, a safe haven

How the general public perceives and judges security technologies depends not least on whether people feel protected at their place of residence and secure on an everyday basis. The SurPRISE questionnaire attempted with several questions to determine the personal sense of security of the participants.

It emerged from this that most of the Swiss resident population feels safe, or even very safe. About 85 percent of the participants (see Table 2: General attitudes on security in all Switzerland), for instance, agreed with the statement that they generally feel safe in their daily life (compared to about 79 percent on average in all countries); in this instance just under one-third came under the highest category of a marked sense of security, in that they chose the answer «strongly agree» as the relevant statement. Only Denmark and Norway scored higher in this category than Switzerland. One rather deliberately worded question, which asked about the level of security in Switzerland, confirmed the finding: while as an average for all participating countries 66 percent agreed with the statement that they live in a safe country, in Switzerland 85 percent agreed with the statement that Switzerland is a safe place in which to live (see Table 2) (with 40 percent agreeing «strongly» and 45 percent agreeing with the question without further comment).

	N	Strongly agree	Agree	Neither, nor	Disagree	Strongly disagree	NA	Total
		Percentages						
"I generally feel safe in my daily life"	*251*	28	57	11	3	1	0	100
"I feel that this country is a safe place in which to live"	*251*	40	45	12	3	0	0	100

Table 2: General attitudes on security in all Switzerland

There are verifiable differences between the three Swiss discussion rounds, and at a statistically significant level. Overall they therefore confirm the trend of a marked sense of security. The rate of agreement to the question "I generally feel safe in my everyday life" was highest, at 93 percent, in Zurich (see Table 3) (over 38 percent agree «completely» with the corresponding statement, while just under 56 percent agree, but without added emphasis). In Grandson 82 percent agreed with the statement that they generally feel safe in their everyday lives, but here too the category of those who emphatically agree with the relevant statement scores lower, at 30 percent, than the response category of those who merely agree, at 52 percent (see Table 4).

People clearly feel least safe in Lugano, where 77 percent were still able to confirm that in general they feel safe on a day-to-day basis: just 16 percent agreed completely, 61 percent responded positively to the question without further emphasis (see Table 5). To the specifically worded question which refers expressly to Switzerland ("Switzerland is a safe place in which to live"), however, the responses in Ticino achieved approval rates of 84 percent (40 percent agreed «completely», 44 percent agreed without emphasis).

	N	Strongly agree	Agree	Neither, nor	Disagree	Strongly disagree	NA	Total
		Percentages						
"I generally feel safe in my daily life"	*86*	38	56	2	3	1	0	100
"I feel that this country is a safe place in which to live"	*87*	44	46	7	2	1	0	100

Table 3: General attitudes on security in German part of Switzerland

	N	Strongly agree	Agree	Neither, nor	Disagree	Strongly disagree	NA	Total
		Percentages						
"I generally feel safe in my daily life"	*90*	30	52	12	3	3	0	100
"I feel that this country is a safe place in which to live"	*90*	37	43	13	7	0	0	100

Table 4: General attitudes on security in French part of Switzerland

	N	Strongly agree	Agree	Neither, nor	Disagree	Strongly disagree	NA	Total
		Percentages						
"I generally feel safe in my daily life"	*75*	16	61	19	4	0	0	100
"I feel that this country is a safe place in which to live"	*75*	40	44	16	0	0	0	100

Table 5: General attitudes on security in the Italian part of Switzerland

The SurPRISE data from the surrounding countries show a similar "North-South" pattern. Participants from Italy for instance, especially compared to those from northern countries and from Germany, express a much weaker sense of security: In their everyday lives, 38 percent of Italians feel safe, while for 23 percent feelings of being threatened seem to predominate. In Germany, 66 percent feel safe against 1 percent feeling threatened.

During the discussions a number of statements affirm that Switzerland is actually felt to be a kind of safe haven. Local relations are readily contrasted with the situation as it is perceived or assumed to be in other countries: «I actually trust our society and our politicians. But if I lived in Pakistan I might see things differently », opined one person, while another observed: "In Switzerland, with the current government, I feel safe. On the other hand, surveillance technology enables people who criticise the system to be found quickly. That is worrying, even if one is not directly involved". Another person has a similar argument: "I'm really not bothered about what I disclose. But in totalitarian states that can be terribly exploited. That's my main problem. Not that anyone can find out something about me."

4.2 Critical opinions towards surveillance

Those who imagine that they are safe in their own country are apparently more sceptical about state surveillance. This is in any case the conclusion that emerges from the quantitative data from SurPRISE. It therefore at the same time confirms one of the main hypotheses developed by the international partners in the project as the event approached (see also section 5). Whereas over 38 percent of the Swiss participants took the view that surveillance technologies should be routinely used to protect national security, over 42 percent opposed such use. Almost 20 percent declared themselves undecided (see Figure 4: „Overall I believe surveillance-oriented security technologies should be implemented to improve national security" (percentage). This means that the Swiss participants are much more cautious than the average for the countries taking part in SurPRISE. Averaging all countries (including Switzerland), more than half (specifically: 54 percent) were in favour of the routine use of surveillance technologies, while those opposed amounted to just 26 percent.

That the sense of personal security is associated with the rejection of surveillance technologies is also confirmed by a look at the results within Switzerland. The most votes in favour of the general use of surveillance technology were in Ticino, where residents generally feel least secure on a day-to-day basis. Here, over 56 percent agreed with the statement that surveillance technologies should be used systematically in order to strengthen national security. In French-speaking Switzerland this contention was only supported by just under 32 percent, while in German-speaking Switzerland, where subjective security is judged to be best, the figure was still around 29 percent. These differences between the language areas are statistically significant (see Figure 4)

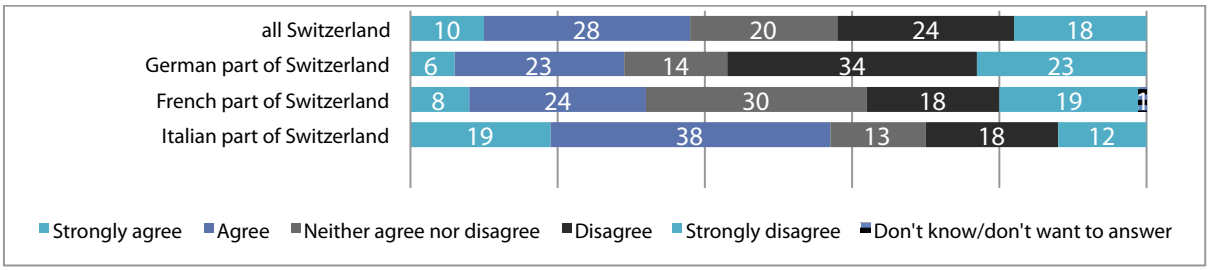

Figure 4: „Overall I believe surveillance-oriented security technologies should be implemented to improve national security" (percentage)

The argument that anyone who has nothing to hide has nothing to be afraid of is also dismissed in Switzerland: 64 percent rejected this vote, compared to 51 percent on average for all countries. Also in this case opinions across the linguistic regions are in line with the subjective sense of security: in German-speaking Switzerland (where the sense of security is the highest) the premise was most strongly rejected by a total of over 83 percent, followed by French-speaking Switzerland with just under 66 percent and Italian-speaking Switzerland with 40 percent; these differences are statistically significant (see Figure 5)

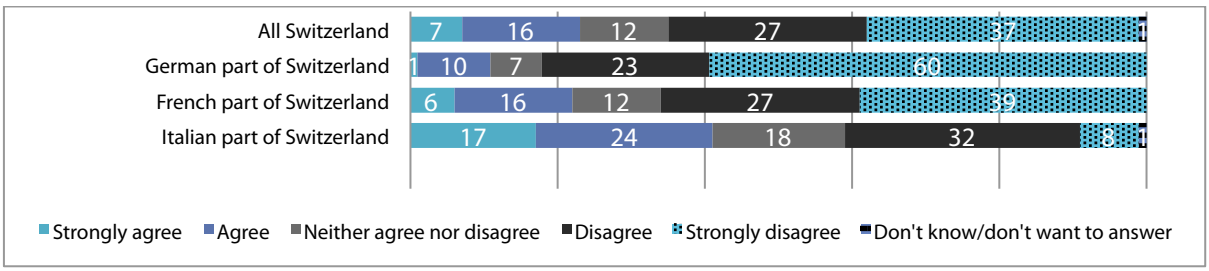

Figure 5: "If you have done nothing wrong you do not have to worry about surveillance-oriented security technologies" (percentage)

When it comes to assessing the general risk of abuse of surveillance technologies, here too the Swiss are more sceptical than citizens of other countries. In this country, for instance, a total of just over 80 percent agree with the statement that security technologies would be misused once they were available (36 percent agree strongly with the statements, 45 percent agree). On average for all countries a total of just 70 percent respond positively to this statement (35 strongly agree, 35 percent agree). Moreover there is evidence of statistically significant differences on this issue within Switzerland, in that Ticino with a total of 92 percent is especially skeptical (31 percent emphatically endorse the corresponding question, 61 percent agree). German-speaking Switzerland takes the middle ground with a total of 82 percent (45 percent strongly agree, 37 agree) while French-speaking Switzerland takes the least pessimistic stance, with a total of 70 percent (32 strongly agree, 38 agree) (see Figure 6: „One surveillance-oriented security technology are in place they are likely to be abused" (percentage)).

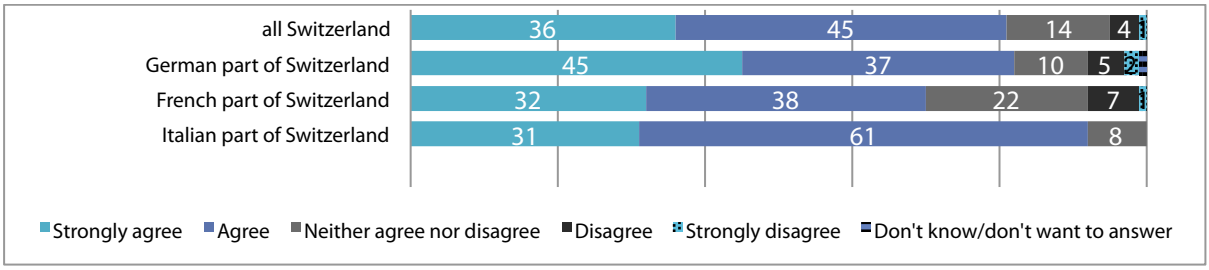

Figure 6: „One surveillance-oriented security technology are in place they are likely to be abused" (percentage)

Various views highlight the ambivalent attitude to surveillance technologies: "*Until now I have trusted technologies and how they are used. But with these new technologies I realise that I don't have good enough reasons to be trustful. Especially because I have no influence on how my data are collected and used*", and "*Technology is not the best solution for increasing security. Better to share wealth and education. It is more beneficial to invest in peace building than in security*". Similar statements were also noted on a number of postcards from all discussion rounds.

4.3 Security and Internet

Although participants in Switzerland feel rather less threatened in their daily lives than residents of other European countries, they tend to be more concerned than the latter about security once they start using the Internet. After all, over 66 percent in this country indicate that they worry about their security when they are online (see Figure 7: "I worry about my security when I am online" (percentage)).

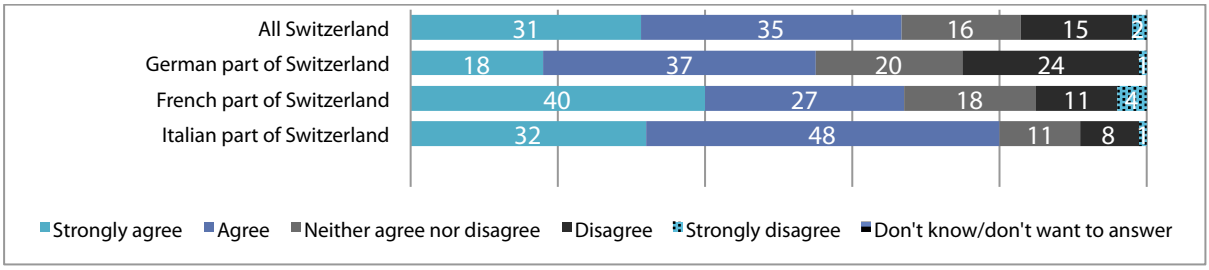

Figure 7: "I worry about my security when I am online" (percentage)

On average for all participating countries, the proportion of people who worry about online security is just under 62 percent. The Internet, according to one slightly exaggerated interpretation, is regarded from the Swiss point of view as a kind of gateway, through which all sorts of dangers can gain access to the domestic idyll. This view carries all the more weight because the Swiss participants are apparently online particularly frequently: 94 percent declare that they are often or even permanently connected to

the Internet. Averaged over all participating countries, the figure was 88 percent. Conversely, only 3 percent of the Swiss participants indicated that they are seldom or even never online, compared to 5 percent on average for the SurPRISE countries (see Figure 8: „How often do you use the internet" (percentage)). The results of the SurPRISE survey therefore also correspond with the findings of the World Internet Project (WIP): its 2012 Report notes that Switzerland is one of the group of countries which use the Internet most intensively – While in Italy 51 percent, in Spain 68.7 and in the UK 70.9 percent of the population use Internet, the Internet penetration in Switzerland is 77.8 percent and is higher than in the SurPRISE countries part of the WIP 2012 survey.

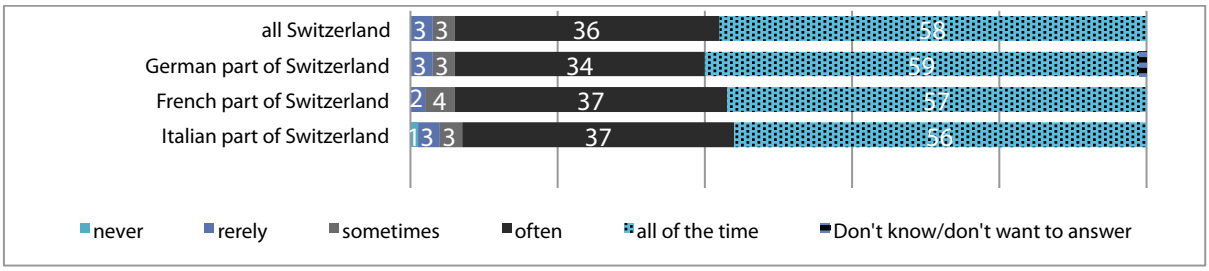

Figure 8: „How often do you use the internet" (percentage)

Concerns over security on the Web are not equally pronounced everywhere in Switzerland (see Figure 7: "I worry about my security when I am online" (percentage)) anxiety seems most pronounced in French-speaking Switzerland, where 40 percent agree with the statement that they are very concerned when surfing (and 27 are concerned). In Ticino too, uninhibited surfing is more the exception, since 32 percent are very concerned and 48 percent just concerned. In German-speaking Switzerland the issue is viewed in a relatively more relaxed way, with the percentage of those very concerned is 18 and of those concerned 37 percent. The differences are statistically significant.

In their statements about technology or about the Internet in general, the SurPRISE participants seemed to regard globality in different contexts more as an obstacle than a benefit; for them it represents lack of clarity, difficult communication and ungovernability: "*The fact that it's global is disconcerting too. National laws do not apply*", said one person, for example, with reference to DPI, while another stated, referring to the regulation of applications that rely on geolocalisation: "It's certainly more of a problem elsewhere than it is here". In Zurich, finally, someone is convinced: "Democracy only works where people to some extent think the same way. In other cultures we have completely different definitions".

4.3.1 The generational view of internet security and privacy

In the discussion rounds, and also in the comments recorded in writing, a number of participants were sorry that the younger generation of «Digital Natives» was underrepresented; so young people who have grown up with Facebook and Co are much more unconcerned or would value the amenities of the social networks more highly than protecting their data. "It would be fascinating to exchange views, regardless of age. What do teens or tweens think about this technology? My daughter-in-law loves the advertising on the right of Facebook. She loves special offers", someone commented, and another person observed: "I have two children, aged sixteen and ten. This technology is perfectly normal for them, and they don't care about the risks".

TA-SWISS has therefore analysed a series of questions on the basis of age groups – especially those which are aimed at attitudes to personal security and privacy.

It must be emphasised straight away that young people do not use the Internet any more uninhibitedly than the rest of the population. The statement that they are concerned about security when they are online was agreed by 79 percent of 18-29 year-olds (53 percent even say that they agree «completely» with the relevant statement). They are thus actually somewhat above the average of 67 percent for the whole participants.

However, because only 13 participants from the entire Swiss sample can be allocated to the youngest age category, for statistical reasons the age groups must out of necessity be grouped together and the values calculated for the 18-39 age group. In this case, there were still 63 percent who agreed with the statement that they are concerned about security when surfing the Web (with 37 percent agreeing completely and 26 percent just agreeing) (see Table 6: „I worry about security when I am online according the age"). They are therefore somewhat below the whole sample average and practically at the same level as the 40-59 age group with 63 percent. It is also revealing that only a few are completely unconcerned when surfing the Web: just 13 percent of 18-39 year-olds reject the statement that they worry about their security when they are online, and nobody in this age group emphatically rejected the relevant statement. Among the 40-59 year-olds, a total of 13 percent opposed the statement, 5 percent strongly (see Table 6: „I worry about security when I am online according the age")

	N= 245	Strongly agree	Agree	Neither agree nor disagree	disagree	Strongly disagree	Total
		Percentages					
18-39 years	*38*	37	26	23	13	0	100
40-59	*128*	23	40	19	13	5	100
Over 60	*77*	39	37	6	17	0	100
Don't want to answer	*2*	50	0	50	0	0	100

Table 6: „I worry about security when I am online according the age"

In other words, reservations about surfing the Web only appear to increase noticeably at retirement age – 77 percent of over 60s are concerned about their security when they are online (39 percent strongly agree with the relevant statement, 37 percent simply agree).

4.4 Privacy – no old-fashioned ideal

For the Swiss population, privacy is very important (see Figure 9: Concerns about privacy erosion due to SOST usage (percentage)). Right at the beginning of the event, 30 percent of the participants declared that they completely agreed with the statement that they were afraid that security technologies might undermine their privacy; a further 36 percent agreed with the statement without additional emphasis. With a total of 66 percent, Switzerland is therefore higher than the average of 57 percent for all participating countries. Mirroring this, Swiss concerns about privacy are confirmed by opposition to the relevant question: 12 reject the statement, 2 percent actually strongly reject it. Switzerland therefore has a lower total of opposing voices, with a total of 14 percent, than the average of 23 percent for all participating countries, or to put it another way: on a national average basis there is a larger percentage of persons who do not regard privacy as being at risk.

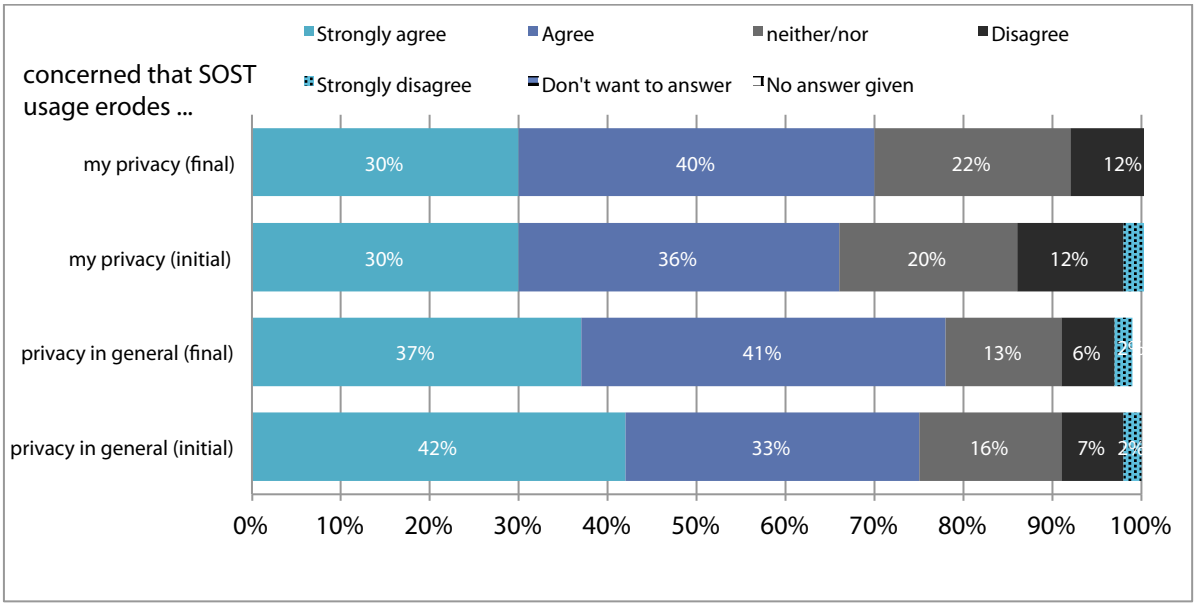

Figure 9: Concerns about privacy erosion due to SOST usage (percentage)

In the course of the SurPRISE Swiss events fears about the protection of privacy increased somewhat. After participants had watched and discussed the short video about DPI and localisation with mobile phones, in Switzerland a total of 78 percent agreed with the statement that surveillance technologies might undermine their privacy (compared to 67 percent on average for all countries).

Interestingly, basic fears about the erosion of privacy in general seem to be even more pronounced than concerns about personal intimate space. The assertion that security technologies threaten to undermine privacy generally was agreed, for instance, at the start of the events in Switzerland by a total of 75 percent, over 10 percent more than the total of those who agreed with the question about the risk to personal privacy. In this case, 42 percent strongly agreed to say they were concerned about their privacy in general and 33 percent agreed without additional emphasis. For this question too, the figures in Switzerland are higher than the average for all countries, with a total of 68 percent – whereby the phenomenon that concerns about privacy in general are more pronounced than concerns about personal privacy, is true for all countries other than Spain. This indicates that the consequences of surveillance are regarded more as a society risk that does not automatically have to be directly associated with personal everyday life. (see Figure 10: Concerns about personal information and security technologies)

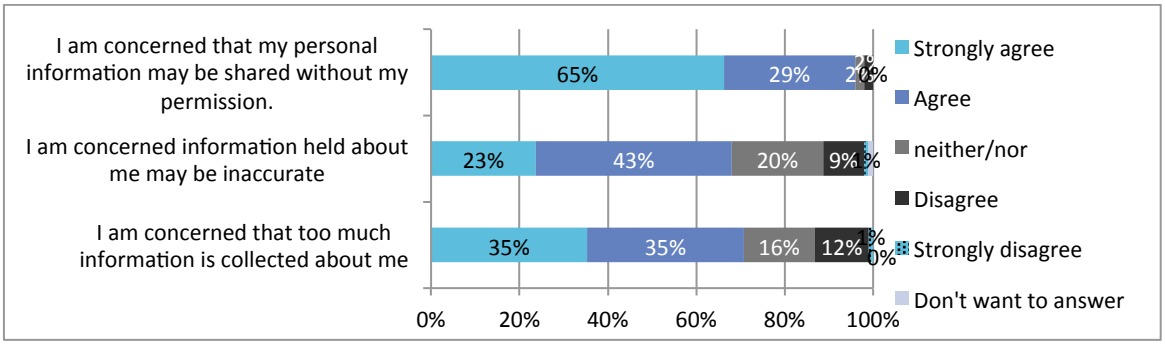

Figure 10: Concerns about personal information and security technologies

When the risks of surveillance technologies are more precisely described, in Switzerland fears feature slightly more strongly than on average for all participating countries. The statements saying that one is worried that there would be too much, or inaccurate, data collected or that data would be collected without the consent of the persons affected score high approval ratings. The statement that too much data are collected show approval percentages of more than 70 percent, and the one that inaccurate data are collected 66 percent. And 95 percent of Swiss participants are worried that data are collected without their consent. On average for all countries these three statements achieve approval rates of exactly 70 and 63 percent respectively («too much» and «inaccurate» data) and in the case of data collected without consent of 90 percent.

On one issue, however, Swiss participants take a rather more optimistic view than the average for all countries: in Switzerland a total of over 66 percent are afraid that the data collected would be used against them – compared to an average of almost 70 percent for all participating countries. If one breaks the response categories down further, the positive finding is actually confirmed: in Switzerland 27 percent strongly agree with the relevant statement, compared to 36 percent on average for all participating countries: an indication that supports the assumption that in this country the illicit collection of data and its consequences is regarded rather less seriously than in many other countries (see Figure 11: "I am concerned that my personal information may be used against me").

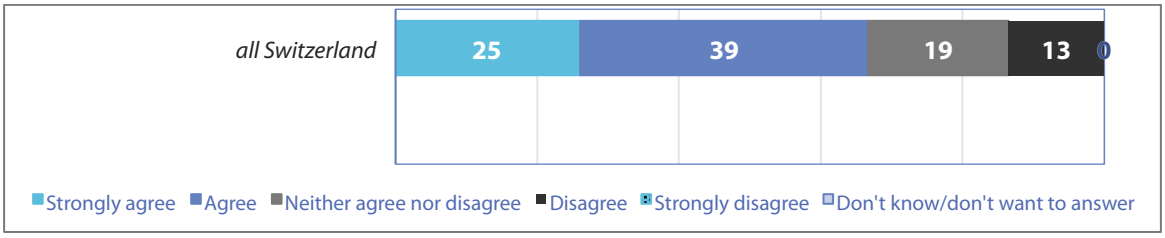

Figure 11: "I am concerned that my personal information may be used against me"

4.4.1 Younger people also place great emphasis on privacy

Privacy is just as much of a concern to younger people as it is elderly persons; among the 18-29 age group a total of 84 percent are concerned about privacy in general and 70 about their own. So the youngest people also consider the risks to their own privacy to be somewhat less than those to privacy in general. Because of the smaller number of cases, however, the results referred to below are those for the amalgamated age categories of 18-29 and 30-39.

In the "18-39 age group", 53 percent completely agreed with the statement that they feared that security technologies would threaten their privacy in general, and 26 percent agreed without additional emphasis (see Table 7: "I am concerned that the use of surveillance-oriented security technologies is eroding privacy in general according the age"). The majority of the two older age groups (i.e. persons over 40) also agree overall but the response «agree» scores higher than «completely agree».

	N= 245	Strongly agree	Agree	Neither agree nor disagree	disagree	Strongly disagree	Total
		Percentages					
18-39 years	*38*	53	26	13	5	3	100
40-59 years	*129*	43	35	14	5	1	100
Over 60	*78*	37	32	18	10	2	100

Table 7: "I am concerned that the use of surveillance-oriented security technologies is eroding privacy in general according the age"

Looking at the opposing votes, too, the conclusion that younger people would pay little attention to privacy is inadmissible. In the 18-39 age group, a total of 8 percent denied that security technology would undermine privacy, and 3 percent strongly opposed the statement («completely disagree»). By contrast, in the 40-59 age group a total of just 6 percent rejected the statement (1 percent strongly). In the over-60s age group, however, concerns about privacy are again comparatively less pronounced – in this case a total of 13 percent reject the relevant statement (2 percent do not agree with it at all, 10 percent reject it without emphasis).

These quantitative results do not, in any case, offer any support to the assumption that the younger people are the less concerned about privacy. Furthermore, the results broken down by age confirm that concern about privacy in general is more pronounced than about personal privacy (see Table 8: "I am concerned that the use of surveillance-oriented security technologies is eroding my privacy according the age").

	N= 247	Strongly agree	Agree	Neither agree nor disagree	disagree	Strongly disagree	Total
		Percentages					
18-39 years	*38*	40	26	16	13	5	100
40-59 years	*130*	29	40	20	11	0	100
Over 60	*79*	26	31	24	15	2	100

Table 8: "I am concerned that the use of surveillance-oriented security technologies is eroding my privacy according the age"

4.4.2 Privacy in the different language areas of Switzerland

The more positively people judge their own level of security, and the more opposed they are to the general use of security technologies, the more they fear the loss of privacy. The quantitative results suggest this conclusion if one breaks them down by language area.

In Zurich, where people feel most secure, and where at the same time opposition to the general use of security technology is strongest, a total of 80 percent agreed with the statement that the use of surveillance technology would undermine privacy in general (48 percent agreed completely, 32 percent agreed) (see Figure 12: „I am concerned that the use of surveillance-oriented security technologies is eroding privacy in general" (percentage)). With regard to their own privacy, 72 percent had similar thoughts (35 percent completely agreed, 37 percent agreed) (see Figure 13: „I am concerned that the use of surveillance-oriented security technologies is eroding my privacy" (percentage)). Grandson occupies the middle ground, in that a total of 77 percent expected an erosion of privacy in general (49 percent agreed completely, 28 percent agreed). Here, too, the figures are somewhat lower, totalling 72 percent, when it comes to the threat to one's personal private life (39 percent completely agreed, 33 agreed). Fears are lowest in Ticino, where in total 69 percent believed that there is a risk to privacy in general (27 percent completely agreed, 42 percent agreed). In southern Switzerland 50 percent saw a threat to personal privacy (12 percent agreed completely, 38 agreed). With regard to how the threat to personal privacy is viewed, the differences within Switzerland are statistically significant, while the differences in the general assessment of a threat to privacy are not at a significant level.

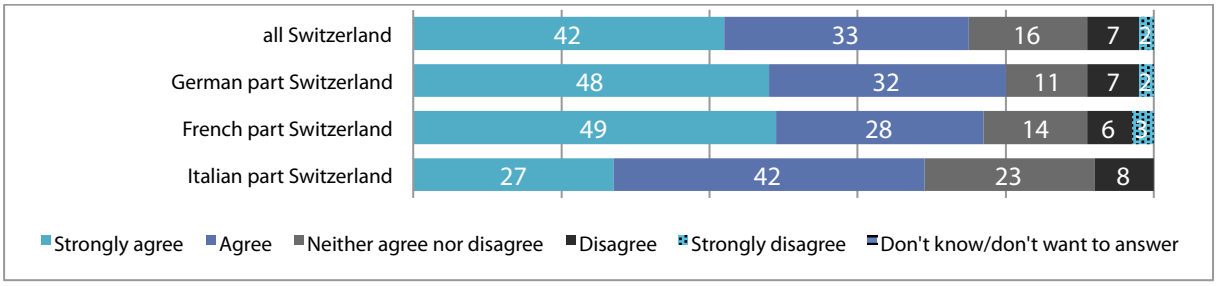

Figure 12: „I am concerned that the use of surveillance-oriented security technologies is eroding privacy in general" (percentage)

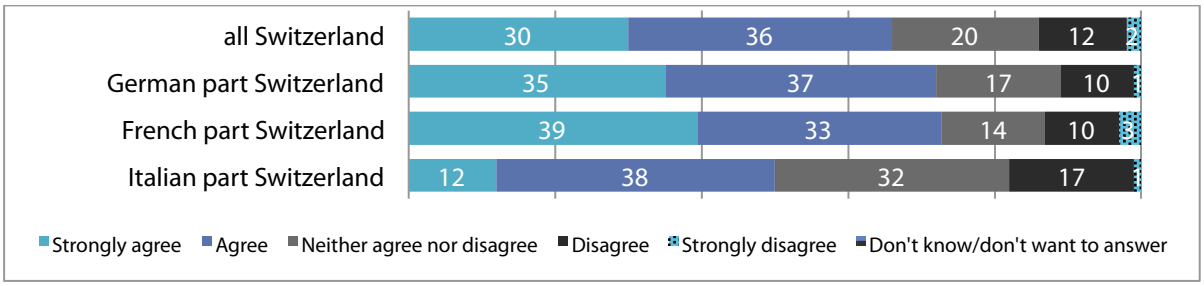

Figure 13: „I am concerned that the use of surveillance-oriented security technologies is eroding my privacy" (percentage)

These findings suggest that the feeling of personal insecurity plays a part in a tendency to accept security technologies, or at least not to reject them so strongly, and thus also to accept some losses in one's private life. The figures also possibly reflect a certain resignation, in that in Ticino there is a prevailing feeling that private has already become public to such an extent that there is no longer much more to lose: "I know that we're monitored, and sometimes that frightens me – but that's how it is these days".

4.5 Deep Packet Inspection: major reservations

As previously stated, DPI is the name given to a network technology that enables not merely to check the «header» but also the content of data packets which can be used for many different purposes ranging from malware and virus scanning but also for data mining and interference of communication. The data gathered as part of SurPRISE show that this tool for monitoring electronic communication meets major reservations. It should, however, be added that in Switzerland there is no kind of legal basis for being able to use DPI for preserving state security. In other words: national and local authorities are not allowed recourse to this tool. In other words, Swiss authorities are not allowed to use this instrument and this particular situation was taken into account or explained to the SurPRISE participants for the votes and discussions.

Overall, slightly less than half, 47 percent, of Swiss participants would accept DPI as a measure to strengthen national security, while 34 percent opposed it (see Figure 14: Adoption of Deep Packet Inspection (percentage)). Our country is therefore more or less in line with the average for the other participating countries (45 percent of the votes for and 34 against). Within Switzerland, the answers to this question also correspond with the sense of personal security: in Ticino, where participants felt least secure in their everyday lives, DPI tended to have most support, with 58 percent, followed by Grandson (43). The participants from Zurich expressed the strongest reservations (40). And as with the sense of personal security, the differences between the languages areas are also significant in the question about approval for DPI.

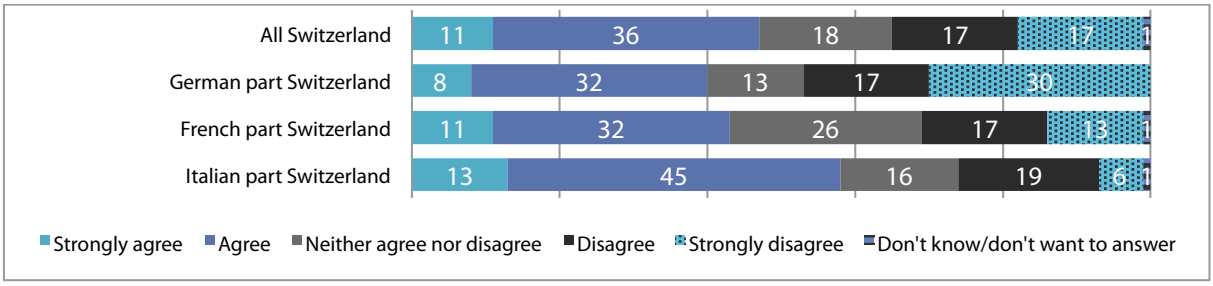

Figure 14: Adoption of Deep Packet Inspection (percentage)

Within Switzerland, this question also produced the already familiar pattern of opinions: in Ticino the use of DPI for national security was rated highest, at over 40 percent, and lowest in Zurich with figures around 30 percent. These differences are statistically significant. In Grandson, an interesting variation is again evident: over 40 percent of participants there certainly support the statement that DPI is an effective tool for protecting national security. However, only just under 27 percent also took the view that its use is appropriate(against 30 percent in Zurich and 45 percent in Tessin, (see Figure 14: Adoption of Deep Packet Inspection (percentage)). In Grandson the gap between effectiveness and appropriateness is most clearly evident. Or, to put it another way, it is possibly the efficacy of the method which kindles reservations about this technology.

4.5.1 Divides opinions and breaches privacy

DPI is used to pursue a number of goals; for instance, it is used to track malware, which means that it also protects the computers of private users. But the technology can also be used by government agencies for political or intelligence service purposes, and even control and oppress their citizens. The responses of the SurPRISE participants show that they do not have much regard for the benefits of this technology to their personal security, and have little faith in it altogether. About one-third were of the view that DPI would effectively and reasonably protect the security interests of Switzerland. Almost as large was the percentage of those who rejected this assessment, or who declared themselves undecided on this issue. Nevertheless, with regard to personal security, opinions of DPI were decidedly more negative: only 6 percent of participants held the view that they would feel more secure when surfing the Web if DPI were used, while 73 percent opposed this view. In the other participating countries opinions were similarly vague, and most, with the exception of Austria and Norway, tended to rate DPI more positively than Switzerland for individual security on the Web.

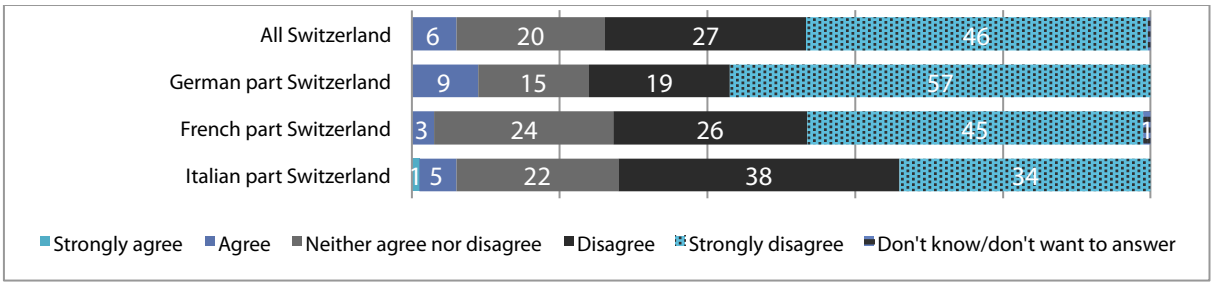

Figure 15: "When I am online, I feel more secure because DPI is used (percentage)

The quantitative surveys show that there are many reasons for the scepticism about DPI. The views identified in the Swiss discussion rounds are essentially no different from those in other countries. The fact that the conduct of users could be misunderstood, personal details fall into the wrong hands, privacy and ultimately even fundamental human rights be violated, worried many of the participants in Zurich, Grandson and Lugano, and those worries were also expressed in the qualitative round table discussions.

4.5.2 «Who's in control – and who controls the controllers?»

The lack of transparency gave rise to a great deal of discussion in all three areas of the country. The question of who exactly would use DPI and what aims would be pursued with it, unsettles many citizens. Someone, for example, is afraid that "One doesn't know who controls DPI: private companies or governments, sometimes states which are incapable of regulation", while others make the point that: "There's no transparency. Who controls what – and who controls the controllers?" and: "I'd like to know who controls the data and what will require attention. The loss of control is disturbing". Finally, someone thinks: "The problem of control is always there. We need commissions – and transparency. Because we don't know who controls what."

Equally opaque are the criteria which ultimately result in someone being targeted by the authorities. «Who decides who the potential criminals are?», is one question that was put, while someone else thinks: «We decide who the goodies and baddies are; it's becoming an ethical-moral issue.» The lack of clarity prevails, and not only about responsibilities with the use of DPI – the methods themselves are not transparent. «Who sets the keywords (which the search is based on)? Sometimes these are also everyday words such as «holidays». If a keyword is common, we're all affected when we communicate via the Web.»

Apart from the fact that quite a few participants at the round table discussions felt strongly about more transparency, many postcards also referred to the subject. «More transparency!» demands someone from Zurich, simply and concisely, and another person says at rather greater length and more dramatically: «More transparency about modern technological terror». It was a similar story in Grandson: "Transparency, transparency please. The public in general is being kept in ignorance about what is really done with these personal data", and in Ticino one person demands: "ethical and transparent use of this new technology".

The mixing of governmental and private sector actors and interest groups is also a thorn in the side for some people; any possible commercial use of data is a thorn in the flesh for many: "There's no transparency, the data end up in advertising. The challenge will be to create transparency and to find an ethical basis for regulation". Others put it in a similar way: "Separation of governmental and commercial concerns is not self-evident. The ethic is at a very low level. The German Länder buy bank data – so is that governmental or commercial? That's very dangerous". And finally, someone calls for «... all surveillance systems not to be permitted on the basis of area, and not at all for commercial reasons.»

All in all, many statements verify that the authorities in this country enjoy considerable confidence, and hardly anyone is afraid that they would use technical resources to the detriment of citizens. Participants do, however, also point out that totalitarian regimes tend to use powerful technical means against their own people. Consequently, specific surveillance technology can affect individuals in very different ways, depending on whose hands they are in. "I am aware that I'm being watched. In Switzerland that's not so bad, but in North Korea I'd be worried" is how someone sums up the situation.

4.5.3 The person is more than his or her data

From the point of view of participants in all language areas, DPI seriously encroaches on people's personal rights. The fact that their data can get into the wrong hands without them knowing is just one of a myriad of problems. No less delicate is the fact that the stolen data can result in false interpretations, which might possibly entail considerable disadvantages for those concerned. Accordingly, there is a fear in all three language areas that unjustified surveillance might take place and – based on misunderstandings and misinterpretations – innocent people might come under the scrutiny of state control. One person warns of an accompanying change in the understanding of the law: «Up to now the presumption of innocence has applied. With surveillance we are changing to one of general suspicion. Which should apply? That is an important fundamental question.»

Finally, a number of the participants in the various discussion rounds fear the social changes which surveillance technology such as DPI threatens to set off. The concern was thus repeatedly voiced that only well-off people could protect themselves from electronic stalking or engage competent lawyers to defend them against accusations. "If someone is tracked and doesn't have the financial means they can't defend themselves", as someone noted. Several participants take the view that a poorer education increases the risk that those concerned would not know how to obtain information about electronic

surveillance and possible countermeasures. DPI is anyway regarded as a tool which from various points of view encourages the multi-class society and may also be understood as a categorisation instrument: "Google adapts the answers to my searches to previous searches, which means that everything remains stored somewhere and I am placed in some pigeonhole or other, I am profiled and after a certain time I will be practically told in advance what my interests, likes and so on are".

4.5.4 The advantages should not offset the disadvantages

In all discussion rounds, participants also explored the issue of the advantages which they can identify with DPI. Defence against spam and computer viruses were referred to many times in all discussion rounds, as well as the fight against paedophilia. As discussed further above, the results of the quantitative survey nevertheless lead to the conclusion that many people do not rate these benefits of DPI very highly in respect of individual security on a PC.

Various people welcomed the fact that broadly based data control is also ideal for putting a stop to terrorists, but a number of people seemed doubtful. Several people also complained that there was no data to actually be able to measure how many attacks on national security had in fact been prevented thanks to DPI; successful and unsuccessful surveillance operations would not be assessed, according to the critics. Also, criminals would generally be technically very competent and are in a position to take measures against early detection: "The criminals are cleverer than we are, and they don't discuss by e-mail when they are planning the Tettamanti robbery". All things considered, measured against its success DPI is very expensive: "The number wrongdoers who are apprehended thanks to DPI, is extremely low and does not justify this widespread surveillance", as someone sums up this point of view. Geolocalisation by mobile phone: everyday benefits are undisputed.

4.6 Smartphone location tracking: clear advantages for daily life

Apart from DPI, smarphone location tracking also formed part of the SurPRISE debate. In Switzerland, mobile phone localisation is only permitted by court ruling as part of legal and police investigations – for instance, if it is a matter of solving a crime. The video which set the scene for the discussions referred both to localisation which can be undertaken using the communication from any mobile phone with radio stations, as well as localisation via the GPS satellite system, which is only possible with smartphones. Whereas localisation via radio cells cannot be separated from the functionality of the mobile phones, localisation via GPS is based primarily on various apps.

In the discussions participants often failed to say exactly which type of geolocalisation their vote referred to. Despite this minor lack of terminological precision it was still clear that in Switzerland – exactly as with DPI – geolocalisation does not meet with unreserved approval. In comparison to the average figure (of 58 percent) across all countries participating in SurPRISE, the statement that geolocalisation as a measure for protecting national security is welcomed achieved the very slightly lower score in Switzerland of 55 percent (see Figure 16: "Overall I support the adoption of Smartphone location tracking as a national security measure" (percentage)). Accordingly, geolocalisation could still win a small majority of participant votes. Nevertheless, over a quarter rejected the statement that geolocalisation should be welcomed as a tool for protecting national security. Compared with DPI, which in this country scores an approval rating of 47 percent and 34 percent for explicitly opposing votes, geolocalisation might yet win over somewhat wider range of people for itself. On this question, too, Switzerland is therefore in line with the views of the other participating countries which likewise mostly approve of mobile phone localisation. In Germany, uniquely, the reservations are so great that only a minority of just under one-third welcomed the use of geolocalisation as a security measure for the nation.

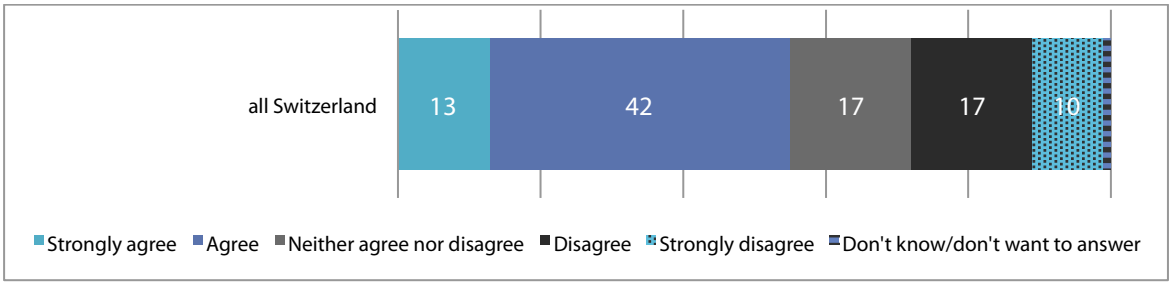

Figure 16: "Overall I support the adoption of Smartphone location tracking as a national security measure" (percentage)

The comparatively broad acceptance of geolocalisation could therefore be connected to the fact that its benefits are experienced directly in everyday life: «Very often it's practical. If you're looking for a bus, it show you where the next stop is. I need that sometimes », was one opinion. The fact that missing persons can be located, or people who are lost can find their bearings using the localisation function on their mobile phone, was also named as a definite advantage. Tracking is also practical for finding the lost mobile phone itself again, and in addition it can be used to track high-risk transports. Further useful applications for society are warnings of traffic congestion and traffic measurements, which could be used in urban and transport planning.

4.6.1 More transparent settings

Localisation technology not only shows tangible benefits, it also has an «institutional face»: users know who their provider is, so they can visualise who keeps their data and what purpose it is used for. Or, to put it another way: users have certain ideas about what happens behind the scenes and who is responsible for it. At least localisation via antennae appears to be a minor disadvantage which is recognised. «The mobile phone provider has all these data. The question is, whether I can just come and ask where your mobile is. That is the question », was basically the view of people in all parts of the country. A number also saw the administrative sense of the data collection: «They must also preserve it so that one can question and/or substantiate the bill. That doesn't seem that daft to me, these six months», added one person.

Several people agreed with the explicit comparison of DPI and geolocalisation, in that transparency is better in the case of localisation technology, and the influence potential greater. «It's a bit easier to exert influence with the mobile phone. One can also switch something off. Self-determination is greater than with DPI», was one comment. «Here at least legal regulation (at least) in Switzerland is possibly better than with DPI», added another person from Zurich. Several participants also referred to the possibility that any spies are easy to outwit, by handing one's own mobile phone to another person. "Geolocalisation reveals where you are, but not what you're doing", was how someone summed it up.

4.6.2 Countering the risks of localisation

Despite the obvious usefulness of mobile phone localisation, many people also mentioned disadvantages of the technology. They seemed particularly disturbed by the fact that private individuals could access data. «I don't want any adverts for chocolate appearing on my mobile», declared someone; like-minded statements were made in all discussion rounds. But government agencies also appear not to be above suspicion. A number of participants in all language regions were afraid that «There is the danger of monitoring political opponents, e.g. in demonstrations».

Social constraints and upheavals are another issue linked to geolocalisation which concerns the participants. The almost universal dependence on the mobile phone gave a number of people pause for thought, and in looking at localisation technology several people were afraid that map reading would disappear as a cultural technique. «Localisation is a disadvantage, because young people will no longer learn how to find their way around», as someone put it, and another person added that she was afraid of making herself look suspicious if she switched her mobile off so that she couldn't be tracked.

The lack of transparency was another reason for criticism with regard to geolocalisation – even though this was directed primarily at the applications («apps») which rely on localisation data, without that

being apparent to users. In this case, criticism was aimed at the often voluminous and confusing terms of use, which hardly anyone reads if they want to install an app quickly. Furthermore, in all discussion rounds people argued strongly that localisation technology should be deactivated on mobile phones as standard; it should only be switched on if the user had expressly agreed.

4.7 Who controls the technology

The quantitative survey did not just explore the views of citizens on surveillance tools, but also sought to track down the image of the actors who use these techniques. For Switzerland, the findings verify that in this country one is fairly heavily reliant on the authorities. Public security forces which would use DPI enjoy greater confidence in this country than the average for participating countries. One is also confident that they want to protect the interests of citizens as well as concerns of national security (see Figure 17: Security agencies which use DPI are trustworthy). Accordingly, 44 percent of people in Switzerland answered yes to the question whether authority-orientated agencies such as the police or customs, for whom DPI could be useful, were trustworthy; the average score achieved in this respect for all participating countries is 36. Only about 25 percent of Swiss participants disputed the credibility of the authorities – a much lower figure than the just under 35 percent on average for all participating countries. Nevertheless, it might also be worth bearing in mind the fact that almost one-third (actually 28 percent) fall into the undecided category «neither – nor». The finding cannot be readily interpreted: it could mean that those questioned find it difficult to assess the trustworthiness of the relevant institutions. It might, however, also be possible that the hypothetical nature of the question requires some effort; in any event a number of people among the public asked which authorities were involved, because in Switzerland official agencies are not permitted to use DPI. In any case participants in Switzerland are also very confident that the responsible agencies will not lose sight of the citizens' interests even if they use DPI to defend the security of the nation: 40 percent agree with the corresponding statement, compared with an average of 33 for all countries.

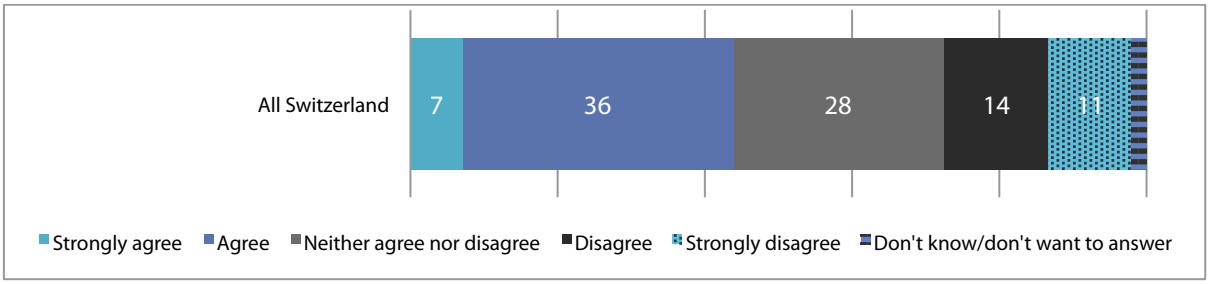

Figure 17: Security agencies which use DPI are trustworthy

Swiss participants are more sceptical than those from the surrounding states only with regard to the competence of the authorities. In Switzerland over 25 percent are of the view that, if they were using DPI the relevant offices and institutions would know what they were doing – compared to 27 percent on average for all participating countries.

Once again, when it comes to using geolocalisation via the smartphone Swiss authorities come off less badly than with the – assumed hypothetical – use of DPI. In this case a good majority of 57 percent of participants were of the view that trust is justified – compared to an average of 46 percent. In all other characteristics, too, such as competence, diligence towards the interests of citizens and foregoing the abuse of power, the Swiss rate «their» offices as better than is the case on average for all participating states. When it comes to the use of geolocalisation, the image of the security agencies is therefore better than is the case with DPI.

4.8 Recommendations - Doubts about the achievability of solutions

At the end of the events, the participants discussed possible solutions for toning down the disadvantages of surveillance technology and thereby reducing the sense of unease. In addition, the participants set out the essential points of the discussion that had taken place at their table. The list of the recommendations that emerged as a result is included in the annex to this report.

The concluding discussions about possible measures were characterised by a range of opinions, from mainly overtones of doubt as to the achievability of the proposals to very resigned undertones.

4.8.1 Agreements and laws

In all discussion rounds the call was made for effective legal safeguards. At the same time, however, doubt was also expressed in all round table discussions as to the achievability of this demand: firstly, because experience shows that legislation always lags behind the technology, and secondly, because the global flow of data through national legislation can be difficult to direct into the right channels. «I have no faith in the law, because a law always lags behind the technology. That's why the question is so difficult, how one wants to restrict it, to restrict it by law. And which instruments can be deployed for sanctioning purposes. One could compare that with human rights, which are also continuously abused without anything being done about it», is the view of one person from Zurich, for instance, and someone in Grandson is also convinced: *"Technology is advancing faster than politics, so it's useless to pass laws about technologies that are already obsolete when the law comes into force."* Similarly minded comments were also made in Lugano.

The different legal opinions and moral convictions around the world also fuel doubts about the enforceability of laws – to say nothing of divergent interests. "The community of all countries would have to impose a common legislation. That's virtually impossible", is how someone summed it up, and a person from Zurich thinks: "It needs a higher-level authority to enforce the [regulation] And what sort of authority would that be then, which can force every country to surrender a bit of its sovereignty?" Voices from Lugano are also rather pessimistic: "Even if we have one regulation, it won't apply in America." One person in Grandson considered that more stringent laws could also work to a country's detriment: "If Europe is more restrictive, the USA will profit from that and impose their economic power. I don't see how we can defend ourselves, because if our laws are stricter the USA will exploit that."

Against this background, a number of people in all three language-areas voice their support more for setting general ethical guidelines which establish respect for human beings and their privacy, and which maintain their validity irrespective of the latest technical developments.

Nevertheless there is a prevailing cautious optimism that not all surveillance technologies will evade a legal regulation quite as strongly. For a number of SurPRISE participants, one advantage of localisation with the smartphone actually lies in the fact that country-specific precautions seem achievable: «Here at least legal regulation is only more possible in Switzerland than is the case with DPI», was the view in Zurich, and similarly in Grandson.

4.8.2 Control and data integrity

Another major concern for citizens participating in SurPRISE was maintaining control over their data. «I'd like to know who controls the data, and what will require attention. The loss of control is disturbing », was how someone from Zurich summed up this position. Similar sentiments were also expressed in Grandson and Lugano. In this connection the call for stronger data protection was also made repeatedly. "If billions are ploughed into surveillance, then billions would also have to be invested in data protection", opined someone in Grandson. In Zurich, one discussion group even supported the idea of a global data protection commissioner.

In this case, technical precautions could also help to respond to the scepticism towards surveillance. «It would also have to be possible for data to be deleted. There is in fact also software where a message is only valid for a short time. But it would have to be technically possible to delete things», was one view from the Zurich discussion round. The call for a «digital eraser» which would ensure that data is not stored indefinitely was also expressed in the French and Italian regions of Switzerland. «It would be key

for the trust issue to have copyright as sender. So you can specify if something should be deleted or amended. That would be really key», was how another person summed up her thoughts. Only a single voice referred to possible negative implications which could be linked to the deletion of information: «Deleting can also be tricky – because victims of abuse often leave it very late to report anything », someone in Grandson stated.

4.8.3 Transparency and evaluation

Also closely linked with the wish for control is the desire for transparency. «If you know the source, you can follow what's going on. But it's because of the lack of transparency that one can't follow what's happening to us." There were even some isolated calls for all-embracing transparency in the sense of a complete abandonment of secrecy and privacy – because if everything is open, underhand dealings would hardly be able to gain any foothold, one person was convinced: «The problem is anonymity. We're discussing data protection because there's no transparency about senders. Anonymity is the problem. One solution would be that the author would have to be known. Everyone who logs on would have to identify themselves. Then the technology could trace who has committed what abuse. The law is ineffective for countering this problem».

Various participants in all three discussion rounds also point to the fact that it is not only with regard to the use of DPI and localisation technology that there is a lack of reliable information; there is also no verification of success. One person in Zurich made the point that «The secret service says that if nothing's happening, that's because we have been monitored so well. And if something has happened, they say that one must monitor more». "One would have to have statistics to know what has been prevented because of surveillance", someone else demanded. There was, however, some doubt that the authorities would heed the call for evaluation, as one person presented the situation: «The interests situation is a problem. Many people have an interest in remaining anonymous. Including the state if a secret service does something. The total transparency approach is therefore probably unachievable. What's behind it, ultimately, is power. If you have information about somebody, you have power. And that's what they want. What they don't want is for everyone to have a level playing field».

4.8.4 Individually adapted behaviour and consumer power

Because they expect little from regulatory guidelines, a number of participants are relying more on the personal responsibility of every individual. «In any event, at individual level one can conceivably mitigate the consequences. And one can do that by explaining things, so that people know what will be read and stored», commented various people in Grandson and Zurich, while someone from Lugano was very much in favour of developing indiscreet Web applications or warnings on smartphones, comparable with the off-putting warnings on cigarette packets: "Users should always know the risks. One could warn them: your mail could be read / your data may be store.", was his suggestion for a warning text.

In this connection, several participants also referred to customers' market power. Someone recalled that in the end even Facebook had improved data protection, when young people were increasingly staying away. «Because we are smartphone users, we are a consumer group. Accordingly, one might say, we also have communal power. If we could join forces and agree. One can also NOT select certain apps which pass on data if one knows that», thought one person. Not everyone was able to share this optimism: «It is always the same big names behind the interesting apps. As far as customer power is concerned, I am rather sceptical, because the providers can hardly be played off against each other», said someone else in the same discussion round. But everyone agreed that terms of business and use should be easier to understand and more user friendly.

On several occasions reference was also made to the possibility that personal electronic communication can also be disguised by an appropriate choice of language and terminology. «Everyone has to start with themselves and take care. And everyone must encrypt, encode their own language», commented someone. Another person referred to the technical means of self-protection, although she herself qualified the prospects of success for this approach: "One must encrypt –but people don't want that, because that's like spying". Nevertheless, voices were also raised by those for whom it is precisely the changes in behaviour due to electronic surveillance which involve the biggest social risks: «That's my main concern. If everyone thinks they would have to be very careful in expressing themselves, that

means losing an awful lot of liveliness and trust. If we are mistrustful of each other, the question is what's happening to our souls», was how someone brought the point home.

The results of the quantitative survey confirm that surveillance technologies most probably impact on people's behaviour (see Table 9: Active avoidance of technology). In Switzerland, 44 percent of those participating in SurPRISE indicated that they want to behave differently than before because of DPI – compared to 54 percent who could not imagine that. Here there are significant differences apparent between the language areas, in that in German-speaking Switzerland in particular 57 percent consider a change of behaviour for online activities (compared to 36 percent who do not). In Ticino 45 percent try out appropriate precautionary measures (compared to 60 percent who continued to behave as before). Finally, in French-speaking Switzerland, 38 consider making changes to their surfing behaviour (compared to 60 percent who stick to what they are used to). In the case of the smartphone, the tendency is to change one's own behaviour is much lower. Only 25 percent declared that they would give up their mobile phone completely or wished to change their behaviour so as not to be tracked. However, 69 percent of participants have no intention of changing their behaviour patterns. These values are comparable with the average figures for all countries participating in SurPRISE. Nevertheless, here too significant differences are in evidence within Switzerland: this time it is the participants from French-speaking Switzerland, 31 percent of whom are most likely to consider changing the way they act. Out of the people from Ticino, 25 percent would consider appropriate changes to their behaviour, while in German-speaking Switzerland the figure is just 13 percent.

Deep Packet Inspection *(N=248)*		smartphone location tracking (SLT) *(N=248)*	
Percentages			
I would not go online because of DPI	1	I would not use a smartphone because of SLT	3
I would avoid going online because of DPI	4	I would avoid using a smartphone because of SLT	5
I would change how I behave online because of DPI	40	I would change how I behave because of SLT	17
I do not think I would change my behaviour online	34	I do not think I would change my behaviour because of SLT	44
I would definitely not change my behaviour online	18	I would definitely not change my behaviour because of SLT	25
NA	3	NA	6
Total	100	Total	100

Table 9: Active avoidance of technology

In fact, the discussions suggested that subtle changes are occurring in people's behaviour. Several people indicate that the need for control over their own data is leading to established information channels drying up. Many people, for example, are no longer listed in the official telephone directory of Swisscom. «It's appalling how many people move home without making their data public. They don't want any adverts, any phone calls – there's a perceptible change in society. One drops into anonymity, one can no longer find people. They have four or five e-mail addresses and several mobile phones, but one can no longer find them», observed one person, and while someone else was apparently astonished about the discrepancy between data protection, which often makes it harder to obtain details of a person's address and to gain free access to information on the Internet. «I'm astonished by the mismatch between the application of the laws on data protection, (for example when one is looking for someone's address and when it's very difficult to get it) and all the data which we have free access to on

the Internet". In this respect, several participants suggested that the need to delete personal data from established sources was due to a sense of unease at constantly feeling publically exposed.

4.8.5 Education and information

The need for control and transparency, as well as the concern to be able to adapt one's own behaviour, matches the desire for education and information. Particularly with regard to the younger generation, who in the view of a number of participants often handle electronic media in an overly uninhibited and careless way, the call for clarification is loud and clear: "I think that sensitisation is very important; the individual must know what he's doing", as one person put it, while another thought: «I was badly informed before, and got explanations from the brochure. That alone is already important – that one knows that it's done, that one also knows who does it and how deep it goes. This information would be the first thing that one would have to ask for». Corresponding demands were also made at school "Schools would have to make people aware of these issues, it would take whole lesson dedicated to it. There would also need to be classes for adults".

4.8.6 Address the causes of security threats

Although the declared subject of the SurPRISE discussions was surveillance technology, there were a number of participants in all discussion rounds who observed that there is more to life than technology and that ultimately it is all of us – society – who decide how technical applications are used and what implications that will have for the community. From this perspective, the use of surveillance technology brings out underlying uncertainties which are attributable to global disparities and injustices. This standpoint is represented by the following statement: "Technology is not the best solution for enhancing security. It is rather a matter of sharing wealth and education out better. It is much more beneficial to invest in peace building than in security."

Seen in this light, security problems can hardly be resolved technically – in any case, not if the aim is merely to treat the symptoms. «There is a huge number of people on earth, and we think that surveillance, or rather security, will save us. That is a choice for society. But one ought perhaps to have an alternative choice as well". Representative of like-minded statements is a quote from a postcard written by someone in Zurich: «Feeling safe and secure does NOT come from advanced technology! The major security problems must be tackled on a MUCH broader basis: poverty, migration flows, education for all girls/children. Only when the EARLIEST RELATIONSHIPS are stable and loving for all children on this planet can a GLOBAL sense of primal trust develop.»

5 Conclusions

In the run-up to the discussion events, the partners in the SurPRISE project, working together internationally, developed a series of hypotheses on the factors which might characterise people's attitude to surveillance, privacy and security. Viewed overall, the Swiss sample confirmed many of the assumptions made in this respect.

One of the central hypotheses assumes that persons who feel personally secure have little sympathy for surveillance technologies. The results of the surveys and discussions in Switzerland affirm this link: people in this country feel very secure, or at least much more secure than the average for all participating countries. At the same time, opposition in this country to security technologies in general, as well as DPI and – to a rather lesser extent – geolocalisation via a smartphone is relatively strong. In light of this, the assumed connection between a strong sense of personal security and scepticism towards surveillance technologies is confirmed. There is even evidence of this correlation within Switzerland: in Ticino, where the sense of personal security appears to be least well marked, reservations about security technology are smallest. In Zurich however, where interviewees feel most secure, acceptance of security technology is lowest.

The central working hypothesis, whereby persons who are worried about their privacy are particularly strongly opposed to surveillance technologies, is likewise confirmed by the Swiss results. For it is in German-speaking Switzerland, where worries about privacy are most pronounced, that opposition to surveillance is strongest. Conversely, opposition to instruments of state supervision and control is weakest in Ticino, where concern about privacy is, in comparative terms, least.

Another assumption presupposes that the image of institutions influences the population's attitude to technical surveillance. The more credible, competent and attentive to their citizens the authorities seem to be, the more able the population is to embrace surveillance technology – that is the assumption. It is, however, belied by the results from Switzerland. The authorities here score better marks than the average for all participating countries, and indeed both in terms of credibility and also of their consideration for the citizens. Nevertheless, in this country people cannot embrace surveillance – even if it is practised by an authority perceived as benevolent. The sense of personal security therefore seems to outweigh trust in the authorities who use surveillance technologies.

However, it seems obvious to assume a connection between the two variables «sense of security» and «perception of authorities». The fact that many people feel secure and at home in this country could be linked to a governmental organisation which by and large is perceived as efficient, credible and considerate. In such an environment, technical surveillance is regarded at best as superfluous and at worst as threatening, because it is a reminder of global interdependence, something people are not entirely able to escape from, even in the comfort of their homes.

Don't jeopardise trust

The results of both the quantitative surveys and the discussions underline how important it is that surveillance technologies should be used in a reasonable way and within a clearly defined legal framework, so that they can comply with their right to privacy. Transparency here is absolutely essential: people want to know what data are being collected, who is responsible for them and what purposes they are intended for.

In Switzerland, where threats to security are regarded less seriously than in other countries, intensive surveillance measures which infiltrate privacy too much rapidly come up against considerable opposition. There is therefore also a risk that the authorities, which currently enjoy a good reputation in this country, will gamble away their trust capital.

That is because various statements from the discussions prove that the «files scandal» of the late 1980s has certainly not been forgotten. The Federal Council has restored the reputation of the authority by reorganising the news services and setting up a strict legal framework. Preserving this restored trust in the security authorities is an extremely challenging task, in that at a time of rapid technical change and changeable levels of threat it is important to find a balance between protecting national security and preserving privacy. The present arguments over the revision of the revision of the Federal Law on the

surveillance of correspondence by post and telecommunications (BÜPF) prove that there is considerable potential for conflict inherent in the use of security technologies.

Against this background, it is therefore all the more important to strengthen data protection and to equip the agencies responsible for it with the necessary resources to be able to carry out their task. A central concern of citizens would therefore be accommodated: To maintain control over their own data.

6 Bibliography

Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweizvom 23 Juni 2010
(http://www.news.admin.ch/NSBSubscriber/message/attachments/19697.pdf)

Crédit Suisse, 2013. What concerns the Swiss? What is important to them?, 1/2013
(https://publications.credit-suisse.com/index.cfm/publikationen-shop/worry-barometer/2013-what-concerns-the-swiss-what-is-important-to-them/)

Federal Intelligence Service FIS, 2014. Switzerland's security : Situation report 2014, Berne
(http://www.vbs.admin.ch/internet/vbs/en/home/documentation/publication/snd_publ.parsys.75250.downloadList.29258.DownloadFile.tmp/ndbsicherheitschweiz2014webe.pdf)

Rapport du Conseil fédéral sur l'évaluation de la loi fédérale sur la protection des données du 9 décembre 2011
(http://www.admin.ch/opc/fr/federal-gazette/2012/255.pdf)

Rudin Beat 2009. Die datenschutzrechtliche Umsetzung von Schengen in den Kantonen, in: Breitenmoser / Gless / Lagodny (Hrsg.), Schengen in der Praxis, Zurich/St. Gallen, 213 – 255.

Szvircsev Tresch, Tibor et al. 2013. Sicherheit 2013. Aussen-, Sicherheits- und Verteidigungspolitische Meinungsbildung im Trend, Center for Security Studies und Militärakademie, ETH Zurich.

The World Internet Project, International Report 2012 (fourth edition), USC Annenberg School Center for the Digital Future

Quelle: STATPOP, Bundesamt für Statistik:
http://www.bfs.admin.ch/bfs/portal/de/index/themen/01/02/blank/key/alter/nach_staatsangehoerigkeit.html

7 List of Figures

8 List of Tables

9 List of Abbreviations

Abbreviation	Definition
BÜPF	Bundesgesetz und die Verordnung betreffend die Überwachung des Post- und Fernmeldeverkehrs („Federal Law on the surveillance of correspondence by post and telecommunications")
CCTV	Closed circuit television
CISA	Federal Act on Responsibilities in the Area of the Civilian intelligence Services
DPI	Deep Package Inspection
EU	European Union
FDPIC	Federal Data Protection and Information Commissioner
FIS	Federal Intelligence Service
ISA	Federal Act on Measures to Safeguard Internal Security
IT	Information Technology
NGO	Non Governmental Organisation
SLT	Smartphone Location Tracking
SOST	Surveillance-oriented security technology
SSCPT	Service chargé de la surveillance de la correspondance par poste et télécommunication
UDC	Unione Democratica di Centro ("Nationalist party")
UNO	United Nations Organization
WIP	World Internet Project

10 Annex

10.1 Table recommendations

Template[13]

Recommendations – content[14]*: Zurich 08.03.2014*

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?
Data recording must be transparent, controlled and definitively regulated (applies to all institutions which collect data).	Using technologies for security with maximum possible preservation of privacy, no data obtained without consent. Lack of transparency about who stores, uses and passes on data. Disparity with other sectors regarding privacy: e.g. organ donation (no data obtained without consent).	• Clear catalogue of criteria which defines who can collect and use which data for a specific purpose. • Use better encryption technologies (firewall). • Development of alternative security technologies. Tackle the root causes of security risks, prevention.

[13] 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 (The recommendation sheet was translated in French, Italian and German. However, here only the image of the German template is shown.

[14] Translated from German

Protect privacy in the digital sector as well.	Analyse the network of laws more accurately. Accountability for data.	Make it more difficult for firms to change terms of use. A strong state data protection authority.
There is no discernible transparency about when, where and why which data is collected about us	At the level of society, dealings with DPI result in there no longer being any presumption of innocence. Any behaviour can be wrongly interpreted.	Greater transparency is required, and providers must actively inform their customers about everywhere they are registered, and/or which data are stored about them. It must be possible to delete data after a certain length of time. What is called for is for citizens in all age groups to be actively informed and sensitised about the risks and dangers of electronic media. Media competence should be actively conveyed. Citizens should know how they can defend themselves and to whom they can turn.
Transparency through information.	Lack of transparency and loss of control for individuals.	More resources for education and research which should benefit citizens in protecting their privacy. Creation of universally applicable standards within a charter to be drawn up internationally. Creation of a supreme authority to supervise and maintain these standards. Basic right to view personal data.
Create preconditions for transparency.	Mistrust, naivety, ignorance, underestimation regarding the collection and use of data.	• Create strict legal guidelines. • Better controls/control bodies (control of control). • Create uniform preconditions nationally/in Europe. • Increase awareness among the population by instruction. Ensure prevention of manipulation of data.
Protection of privacy	Citizens have too few opportunities to regulate the use of their data. The State is taking too passive a role in protecting its citizens.	It is a duty of the State to adopt an active role in protecting the storage of citizens' data, and as far as possible to anonymise and protect. Commercial and private use in particular must be prohibited. The State should formulate clear and enforceable legislation
Better protection of privacy through more transparency: opportunities for information. Separation of security and commerce.	• Misuse of data and thus lack of security. • Legislation is lagging behind because of the very rapid development of new media.	• Passing on of data must not be encoded in the GTCs. • Users must be able to determine which data can be circulated for commercial use. • CH providers must completely delete data after a certain time. • The Federal Government has an obligation to support schools in raising awareness of new media and at the same time of course the entire population.
Inform, sensitise, autonomisation	Legislation is not keeping pace with technological change. Tension among	Information campaign by authorities, schools, media and specialist units. Political conditions to strengthen users by calling

	users between curiosity and risk. Non-estimable consequences of technology determinism	for "Privacy Enhancing Technologies", "Opt-In" models and finding a balance between security policy – economic – and personality-relevant points of view.
"Anyone who surrenders their freedom for extra security ends up losing both."	We are unconvinced by the benefits of the new technologies in respect of security	Human rights, data protection and transparency must be given higher priority than satisfying security needs.
More transparency regarding our privacy	Lack of trust in society/institutions	Self-determination regarding the use of our data, handling the technology. Change in society must be countered with prevention/cooperation. Resolve together.
-	Only partial use should be made of DPI. The endpoint of the data transfer should be protected above all else.	Strict legal framework conditions for using DPI, which guarantee that • only a government authority uses DPI • this authority is supervised by a political institution.
Global binding guidelines on the protection of privacy, focussing on information and communications technology.	• We can no longer resolve the problem of protecting privacy from "modern" technologies on a purely national basis. • International networking of technology (today and in the future).	• Formulation of a charter • Global data protection officer • Setting up a tribunal similar to the UNO war crimes tribunal • For Switzerland: Create framework conditions for national Intranet (CH as SME), to guarantee protection against international data access (e.g. by Google): Intranet where national legislation is executed, because there is no "data looping" abroad. (Comment: No censorship, 2 networks 1x CH Intranet, 1x www = option for citizens)
Creation of legal bases	• Uncertainty about who is monitored for how long and why. • Unclear which data can be collected from whom. • Unfamiliarity with surveillance equipment: which ones exist on the market and what can they be used for. • How/to what extent are basic constitutional rights put at risk.	• Basic rights regarding privacy must be guaranteed. • Transparency about using and passing on of data. • Guarantee independent control through competent bodies. • User friendly regulation/info of terms of use → enable consumers to control their own data usage. • Data deletion facility: Who decides on the default setting. Viewing opportunities

Recommendations – content[15]: Grandson 22.03.2014

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?
Creation of a charter or quality label which guarantees basic rights on the internet	Invasion of privacy, lack of transparency about how data are used, lack of bases for decision making. Especially with applications such as Facebook, Twitter, e-mail etc.	Websites should undertake to respect a charter. In return they will receive a quality label that is managed by an organisation – already existing or to be set up – that is international, independent and trustworthy. This charter will cover the following points and requirements in particular: • Continuous information on technological and legal developments Transparent use of data. Maximum permitted time frame for using the data (restriction)Ban on amending content (list incomplete)
We appreciate the new technologies, but have some concerns regarding the protection of privacy.	Lack of transparency when using the data. The data are not only used to protect users	More emphasis on training and education for all age and population groups. Standardisation of the terms of use
DPI and geolocalisation must be regulated at European level in such a way that individual liberty is respected.	Users/consumers must give their full consent.	Create legal bases, set up a control body which monitors individual liberty in each state, sensitise and inform the population.
Ethics that guarantee democratic debate.	Respect for human rights (religious freedom, political, sexual freedom, respect for privacy) is not always guaranteed, lack of public debate, opacity.	Access to and use of stored data must be transparent, and it must be stored under democratic control and in compliance with human rights. Our request: create legal bases (at national and international level).
Creation of a Europe-wide legal basis which respects the basic rights of the individual.	Absence of clear legislation. Pace of development. Lack of coordination. Globalisation of the network.	Citizens should be informed about what results could be achieved by the use of security technologies. Information/education in compulsory education. Private firms which use security technologies should be made to adhere to strict framework conditions, especially regarding terms of use
More frequent and more comprehensive consultation with citizens (on important issues such as that discussed here).	The legal vacuum regarding DPI and geolocalisation. The inadequacy of the information available to DPI, especially the lack of knowledge of young people.	Create national or international laws. The use and evaluation of DPI must be restricted, with the exception of legal issues and issues of national security. Better information for citizens regarding these technologies. An ethics committee for the IT sector.
Strengthen the current legal basis so that the protection of private life against the use	Technological development goes hand in hand with a loss of control	Increase the independence of consumers (widen the offering). Make collection of data more difficult by tightening up the

[15] Translated from French

of these technologies (in Switzerland and at European level) becomes priority.	over the instruments and the data. It happens at the expense of private life. Dependency of consumers on just a couple of providers (lack of alternatives).	law. Increase information and education to protect the private lives of users. Clear commitment to basic principles which define the right to a private life (also the right to be forgotten, i.e. the right to delete certain data must be part of this).
Protection of privacy must take precedence if it is a matter of maintaining democracy and basic rights.	The emergence of new technologies brings with it opportunities and risks. But people lack the necessary knowledge and the resources to adapt to these technologies and to make informed decisions.	Creation of a legislative framework that should include the following points: • Duty to inform, to educate and to instruct. • Duty of transparent disclosure as to who uses which data for what purpose. • Duty to determine precisely the preconditions under which collected data can be used by third parties. • Restriction and control of the use of personal data.
Strict conditions of use for data that have been collected by DPI and geolocalisation.	DPI : Too many private and commercial actors have access to data. Geolocalisation: user has no freedom of choice (activation, deactivation)	DPI: Creation of a legislative framework which restricts the use of DPI to problems of state security, under the supervision of the judiciary and Parliament. Ban on use for commercial and private purposes. Geolocalisation: It must be clearly evident in which cases the general terms of use provide for the automatic activation of positioning or the passing on of data to third parties. Data must not be allowed to be passed on and it must always be possible for the consent of the user to be cancelled. Generally: All citizens must be able to view their own data.
handling must be clearly defined. Guarantee the right to preserve privacy, i.e. the right to information, the right to give one's consent and to be free to choose.	We are doubtful about the sales pitch from «security»: What security? Who for? Why? The general public is being left in the dark about what is actually done with these personal data.	Who controls whom? Why?
Lack of transparency: It is essential to have clear and transparent information about how the collected data are used.	-	Creation of a European network and an ethics charter for data usage.
The need to increase transparency and tighten controls on how the stored data are used.	Concern and doubts regarding the use of these data and the possibility that they will be used and analysed for purposes other than the preservation of state security (commerce, health data, human resources).	The current data protection act should be appropriately extended. A national and European control body should be created. Prevention and education programmes must be intensified. European autonomy over the USA should be promoted.

Criminality is caused by a lack of education and by an unfair distribution of goods, which lead to a sense of insecurity.	Technology is not the best method of increasing security.	To increase security the first priority must not be tracking criminals. It is more important to deploy the necessary resources so that there are fewer criminals: Reduce prosperity gaps, improve education. Prevention and vision, and greater transparency are called for. Peace work offers more than security policies. Peace building.

Recommendations – content[16]: Lugano 29.03.2014

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?
Information, transparency, common legal bases, prevention, dependency	- Information: Awareness and knowledge of the advantages and disadvantages of the means employed. - Transparency: Users are absolutely uninformed about how their data are used. - Legal bases: There are no internationally applicable laws and standards. - Prevention: Too little is known about the extent of data mining.	- Using laws that apply to everyone and that all nations have to comply with. - Information and clarification about the extent of the data and about the technological potential of the means employed, especially for minors. (school subject) - Users must have the right to know how information relating to them will be used, and they must have the right to receive feedback on it. - "Ticket" for the Smartphone. - Alternative ways to protect national security must be actively sought. - Re-socialisation programme and withdrawal programme for addicted Smartphone users.
Limitation of privacy in the name of an allegedly greater common security.	The so-called «need» to increase security	Clearer legal bases (DPI and geolocalisation) Clarification for citizens/users IT skills training for citizens and also for inspection bodies Deployment of a control body with precisely defined area of authority
We ask for clear and unambiguous legal standards.	We are concerned that the use of these technological tools will not be managed transparently.	We ask that each user of such technologies must expressly and compulsorily give their consent to the use and reuse of their personal data. There is a need for clear, international and globally valid laws for transparent use; circulation of data must be limited and after a clearly defined period of time they must be deleted. Strict penalties for breaching the privacy of individuals and society. Supervising the supervisors.
Clear rules for reasonable use of security technologies.	Preventing misuse in respect of personal rights	Creation of a neutral international organisation to oversee technological development and guarantee free access to independent information. There must also be greater transparency about who collects and keeps sensitive data.

[16] Translated from Italian

Rules must be created that apply globally (Europe and beyond) to regulate how personal data that has been obtained and collected by security technologies may be used, and also critically question the benefits and effectiveness of their use.	• These technologies are very intrusive, and it is impossible to control who uses them and how. • The problems (terrorism) that might be solved as a result of these technologies are presented to us as being more serious than they actually are. The question arises as to whether it is really necessary to use them. There is doubt about the actual effectiveness of these technologies. Alternative solutions (the human factor) would be preferable here	• Legislation/regulation at global level (on a large scale) which protect privacy in connection with the use of these technologies and the data obtained by them • A clear estimation of the actual need to use these technologies. Realistic evaluation of the threat situation and of the real risks, and appropriately discreet use of security technologies. Alternatives should be sought and in the security sector greater value should be placed on the human factor (investigating authorities) than on the technology. The population must be correctly informed about these technologies, their use and risks, starting from school age. With this information they should have the ability to protect themselves against certain risks and to be fully aware when handling these technologies.
Greater awareness and higher level of protection with help from politicians	-	Make sure that the instruction given to the whole population does place greater value on technological aspects than on social aspects and also takes account of the risks. There must be clear and effective sanctions for all those who collect or use personal data illegally.
Create laws and regulations. But also greater transparency.	There is a lack of clear information on the risks taken by users of these technologies. At the same time the existing legal bases are inadequate or completely absent, and legislation must be harmonised at both national and international level.	Create laws and independent control bodies. Show who administers the services (internet) and clearly establish what are their duties and responsibilities. Users must be informed at all times and in a transparent way of the risks and of their rights. The technology should be independent of the agency which uses it. Users should be able to determine when and how violations of their rights and especially of their privacy are permissible.
Transparency, information, education	Lack of knowledge about how data are gathered, managed and analysed, and what end use they are intended for.	Transparency: Simplification of the legal provisions (ITU) regarding new technologies. Make public details of who uses data. Information: Fuller and more frequent information by means of different communication channels. Education: Education and instruction in schools, sensitisation and introduction of a class dedicated to one of these topics, and also courses for adults.

Personal rights and privacy are inviolable.	The goals pursued with these technologies are in no way proportionate to the breaches of privacy and of individual liberty that occur as a result.	We call on politicians to work together for a clear regulation which sets out precisely how the use of DPI and mobile positioning is to be managed, controlled and if necessary limited so that the right to privacy is not violated.
Improve information to make users more aware of the implications of using these technologies	We note that users' data are used for purposes that constitute a breach of privacy, or even an act of aggression.	We ask political groups for: 1) Clarification of the risks of using telematics to be a fixed element of school lessons Equipment manufacturers and service providers must be compelled to inform consumers briefly and clearly about the risks they incur with regard to their personal security.
Missing information, lack of protection from misuse of these technologies. Urgent need for better clarification of which technologies are already in use.	Threat to privacy. Lack of awareness about what use implies, espionage, commercialisation, unlawful use of personal data.	Sensitisation campaign for all age groups. Joint European legal bases and standards, strict penalties in case of abuse, transparently made obligation to request consent (privacy by design). Personal data must be managed by the State, an opt-in must be obligatory for commercial purposes.
Information and education even during childhood, so that everything connected with surveillance, security and privacy is made transparent.	Complex subject which affects everyone and which must be better explained and more clearly regulated at international level.	1a) Information and education on the subject from commencement of schooling 1b) Information of the population by the data protection authorities on security technologies in a continuous and accessible way (possibility of exchange, to ask questions). 2) Harmonisation of the international rules by institutions such as the UNO or the ITU, which are already based in Switzerland. 3) Equipment manufacturers must be placed under obligation to give users the opportunity to switch certain surveillance mechanisms on and off.

10.2 Postcards

Template