"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 6.2 – Citizen Summits on Privacy, Security and Surveillance: Country report Denmark

Lead Beneficiary: DBT

Author(s): Jacob Skjødt Nielsen (DBT)

Due Date: June 2014

Submission Date: December 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

About SurPRISE

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

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

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

This report is part of WP6, it describes and analyses the Citizen Summit held in Denmark.

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

Executive Summary

This report presents the results of the Danish citizen's summit held in Aarhus on 18th January, 2014, as part of the pan-European SurPRISE project, being conducted in nine European countries. The analysis is based on exploration of the empirical data gathered during the summit. In order to best accord with the format of the participatory process, a mixed-methods approach is utilized combining the data gathered from a pre-defined survey and notes about and outcomes of three thematic group discussion rounds conducted at the summit. The purpose of the participatory event was to investigate how Danish citizens perceive the interrelationship between privacy, security and surveillance in relation to the deployment of surveillance oriented security technologies (SOSTs). The two SOSTs being scrutinized in depth at the summit were smart CCTV and smartphone location tracking (SLT).

In order to set the scene for the analysis and to account for any potential coherence between summit results and national peculiarities, the report starts with review of Danish socio-cultural history as well as national domestic developments in legislation. After this, a description of process design at the Danish summit, including structure of the citizen panel, is presented. Section 4 is comprised of the analysis of the empirical data and presents the results of this, providing deeper insight into the Danish participants' perceptions of privacy, security and surveillance. Further, this section also contains the recommendations to policy makers, developed in cooperation between the participants at each table. The final section comprises some concluding remarks.

The Danish society has been habituated to public registration for many years through church books and later the central person register. In the course of the past 15 years, Denmark has been faced with changes in global geopolitical movements, particularly the terror attacks in the early years of the new millennium, prompting legislative and institutional adaption. Faced with this, Denmark, as other countries, has increasingly seen surveillances and registration measures being implemented by security agencies in order to ensure national security, creating tensions between privacy and security.

The results of the analysis shows that, despite the participants generally feeling safe in their daily lives and in Denmark, they largely supported the implementation of SOSTs by security services and that SOSTs in general, and the two dealt with in depth, were perceived to be both appropriate, efficient and capable of ensuring national security. Further, most participants considered the security agencies employing such SOSTs to be both trustworthy, competent, concerned about citizens' welfare and not abusing their power. From the table discussions it was evident that it was rather data collection performed by private actors that seemed to concern the participants. Both smart CCTV and SLT were considered to be intrusive, and in both cases the majority of the participants did not agree that the benefits of them outweighed the intrusiveness. Despite this, the majority still supported the routine implementation of both SOSTs, and few were willing to challenge the use of SOSTs while most wanted to seek information about how to protect their privacy, and not many believed that they would change their behaviour because of either SOST.

This does not mean that the participants considered the implementation of such SOSTs to be a matter of triviality. Quite contrary, most voiced concerns about the consequences of SOSTs, and the results from the survey showed that most were concerned how SOSTs would affect privacy and human rights. Many voiced concerns about the unknown extent of data collection, both on the part of public and private actors and this was for many a primary concern. Again, this was substantiated by the survey, showing that many were concerned that too much information was collected about them and that they were concerned what the data was used for and who had access to it. The participants felt that legislation was too opaque and that they were disempowered by incomprehensible regulations and 'terms and agreements' of private service providers, which in turn made many worry about function creep, especially in terms of smartphone applications. The survey also showed that a large majority wanted alternative approaches to security, that do not involve SOSTs, to be given higher priority, and that they feared the future development of both smart CCTV and SLT.

The participants generally considered SLT to be substantially more controversial than smart CCTV in almost all aspects, and while they were considered fairly equally efficient and capable of ensuring national security, it is still noteworthy that the support for implementation of the two was fairly similar.

The recommendations were marked by the participants being ok with government security agencies employing SOSTs, as long as that does not result in a trade-off between security and privacy, but they also wanted non-technological solutions to be given higher priority, for instance social efforts. Apart from that, the recommendations can generally be categorized in three types: empowerment through information and education; surveillance ombudsman; and, transparent legislation. The participants generally wanted greater dissemination of information about how security agencies are employing SOSTs and what they are legally allowed to do, as well as what private actors are allowed to. This dissemination should be conducted efficiently through primary school education and public information campaigns across multiple media. Further, the participants wanted a 'surveillance ombudsman' who could represent the citizens' interests and to which it should be possible to file complaints about rights violations and abusive surveillance. Lastly, and in continuation of the other two, the participants wanted transparent legislation, understandable to regular citizens, quickly and easily available and comprehensible. This legislation should set out the rules for who are allowed to do what and under what circumstances, and what is the collected data used for. Further they wanted to disallow function creep, or at least make it clear that it is taking place. The legislation should be anchored in enforceable sanctions and be in mutuality with the surveillance ombudsman.

Summing up, the participants were calling for empowerment of Danish citizens through information dissemination and education, a 'surveillance ombudsman' and an improved transparent legislation.

In total, the results from the Danish citizen summit can help show how the interrelation between surveillance, privacy and security is seen from the citizens perspective, which in turn can create essential input to policy decisions and those who make them, assuring that the actions taken, at least take into account, the views of the citizens who are affected by the same actions.

1 Introduction

The debate concerning privacy, security and surveillance is by no means a new one; it has long been the subject of heated debates in politics, media and academia, but a coherent, extensive investigation into the general public opinion of laymen has not previously been conducted in Europe. In recent years the technological advances and revelations about (c)overt government indiscriminate mass-surveillance has again prompted widespread debate about surveillance and the trade-off between privacy and security, making a pan-European investigation, as the SurPRISE project, all the more relevant and necessary. Both to let ordinary laymen have their voices heard and to extensively analyse what 'the public opinion' on the matter is. In order to carry out this analysis, the SurPRISE citizen summits, undertaken in 9 countries, let citizens voice their perceptions about the trichotomy of surveillance, privacy and security.

Objectives of this report

In this report, the results of the Danish SurPRISE citizens' summit, held in Aarhus, are presented and analysed. In order to provide a fair, holistic representation of the participants' opinions, the analysis is the result of a mixed methods framework combining empirical data gathered using quantitative and qualitative methods. To generate a factual and descriptive big picture of their opinions, the participants completed a quantitative survey, developed in the SurPRISE consortium and employed in all the citizens' summits. These also allow for easier comparison of results across countries, through homogeneity of methodology and result format, as well as ease of generalizability. For a more in-depth understanding of what underlies these results and to give participants a chance of elaborating on the opinions expressed in the quantitative survey, three discussion rounds were conducted at the tables, with each table focusing on the following surveillance oriented security technologies (SOST): Smart-CCTV and smartphone location tracking (SLT).

In Section 2, a short description of the Danish country profile is followed by an account of major security policies and strategies, major privacy issues and an account of the public discourses concerning SOST and related practices, setting the scene for understanding the context of the citizens' summit. Section 3 describes the design of the participatory process, briefly the organizational setting, the structure of the citizen panel, and briefly some reactions to the process offered by the participants after the event. In Section 4, the results from the citizens' summit in Aarhus are gathered, compared and analysed, and the results are presented, and the citizens' recommendations are presented. The concluding section summarizes the major findings and offers some concluding remarks.

2 Privacy, security and surveillance in the national context

In this section, a brief country profile provides background information for a general introduction to how the geopolitical developments of the early 21st century lead to substantial changes in Danish security policy and strategies. This is followed by a description of the major privacy issues relevant to Denmark and an account of the Danish discourse on security oriented surveillance technologies (SOSTs) and related practices.

2.1 General national context/ country profile of Denmark

Denmark is a sovereign state located in the northern part of Europe, in the geographic region of Scandinavia. The area of Denmark covers 43.098 square kilometers, and has a population of 5,584,758, with a population density of 126.4 per square kilometer.

The form of state is unitary constitutional monarchy, which was established by The Constitution of Denmark in 1849. The purpose was to reduce the power of the monarch, and it therefore marks a transition from absolute monarchy to the current trichotomous separation of powers into the legislative, the executive and the juridical branch. The Constitution has been subject to four amendments and the current act is from 1953. The first amendment occurred in 1866, as a consequence of loss of territory, making the constitution then in force, obsolete, and was thus a correction for this condition. The second amendment, in 1915, gave voting rights to women and servants. Moreover, it entailed that future amendments would require a popular vote to be held, in which at least 45% of the electorate would need to vote in favour of an amendment. The constitutional amendment of 1920, was a consequence of the Reunification, which meant that the northern part of the Duchy of Slesvig once again came under Danish fiefdom. Hitherto the fourth amendment of the constitution in 1953, the Danish political system had been bicameral, consisting of a 'Landsting', with limited eligibility and a more democratically elected and eligible 'Folketing', but with the fourth amendment the Landsting was abolished. The 1953 amendment also entailed a de jure implementation of the parliamentary principle, which had been de facto adopted since the System Change of 1901.

The form of government is organized in parliamentary democracy, subject to the negative parliamentary principle, meaning that no government can be appointed or remain in power if a majority of the parliament opposes this. Furthermore, it is organized in a multi-party structure, where several political parties can be, and often are, represented in Parliament at any one time, and currently 8 parties are represented in the parliament. This is because a party only needs 2% of the votes in an election to be represented. This means that minority administrations, where the governing parties don't have parliamentary majority in themselves, but are dependent on support from other parties, the government's so-called parliamentary basis, are both possible and common. The Danish political system is therefore often characterized as driven by consensus decisions, often across the political spectrum.

Since World War 2 Danish society has developed a, so-called, universal welfare state, based on the principle of equal opportunities for all. The welfare state is also based on the idea of public responsibility for individuals unable to obtain a certain level of material and immaterial well-being; both economic and social security. This includes a minimum of level of education, a minimum of prosperity, and the citizens' accessibility to art and culture. This means that the state offers a number of free services, for instance the health care and educational system. To ensure this free universal access, the taxation system is one of progressive taxation, where, the more you earn, the higher you are taxed off your last earned income, resulting in a relatively high taxation level.

It has been asserted by a number of scholars, that a reason for the Danish economic success experienced through the past 50 years, is largely ascribed to a great social and cultural homogeneity.[2] This, some scholars assert, has been key in the solidary system of redistribution and the widely hailed unemployment system, known as 'flexicurity'. Flexible, because it is easy to hire and fire people, secure because

[2] E.g. Iversen & Andersen, in Fellman, 2008; or Campell & Hall, 2006.

unemployment benefits are relatively high and unemployed people are offered training courses and seminars to strengthen their professional profile while unemployed.

Denmark has a mixed market economy, ranking 10th in the world in nominal GDP per capita. Denmark ranks highest in the world for workers' rights. It has the fourth highest ratio of tertiary degree holders in the world. Denmark has the world's lowest level of income inequality, according to the World Bank Gini (percentage) and the world's highest minimum wage, according to the IMF.

In 1945 Denmark became a founding member of UN, in 1949 Denmark entered NATO, in 1973 EEC and finally in 1993 the EU.

Civil registration

Denmark is a highly registered society. Close to everything imaginable is being registered and stored in large databases, making it possible to monitor every corner of the Danish society and intervene with rules and remedies if something develops in an undesirable direction.[3]

The history for civil registration is more than 350 years old.[4] For comparison, it should be mentioned that Iceland has a more than 1000 year old history with extensive registration of citizens. Denmark and Iceland have throughout history had a close relationship since Iceland was part of the Danish kingdom for over 500 years. Today the Danish state has a comprehensive knowledge about its citizens; where they live, whether they are married, how much they earn, etc. Until 1968 this kind of registration was decentralized. It was the churches and later also the municipalities that had information about the citizens, and the state had to settle for seldom performed population censuses. In the 1960's, due to the increasing development in IT, it was decided to create a central register with information about every citizen. In 1968 the Civil Registration System (Det Centrale Personregister, CPR) was created.[5] In the system there is information about the citizens' name, address, place of birth, membership of the Danish National Church, information about the parents, income, taxes due etc. The reason for creating the central register was the introduction of the retention tax, where comprehensive information about the citizen is necessary.[6] Since 2004, the majority of civil registrations were made electronically.[7] As part of the civil registration system each citizen has a personal identification number in the system.[8] The information from the register is especially used by the state due to the register's extensive collection of information about each citizen. The civil registration number is a key to facts about the citizen - and the number is widely used as a means of identification in telephone transactions with banks or medical services or submitting a tax return.[9]

When the personal numbers where created it was expected that it was going to be a crucial part of the citizens' everyday life, and it has effectively connected the citizens to the public sector, and is also widely used by private registers. The personal numbers has also been essential in enabling a number of research projects. The registration system and the personal number are considered a great success and have been exported to other countries.[10]

2.2 Major security policy and strategies

Denmark has a long history of registration of citizens which provides for both a population accustomed to being registered and a framework from which to build a surveillance system, and with 78% of Danes using the internet on a daily basis and 55% of Danes between the ages of 16 and 74 using smartphones daily,[11] the foundation is laid out for establishing a wide-ranging and efficient system of surveillance and registration of the citizens. A combination of social coherence, trust in the public sector and few breaches

[3] Lauritsen, 2011b.
[4] Personregistrering.dk, 2012.
[5] Personregistrering.dk, 2012.
[6] Lauritsen, 2011b.
[7] Personregistrering.dk, 2012.
[8] Lauritsen, 2011b.
[9] Personregistrering.dk, 2012.
[10] Lauritsen, 2011b.
[11] Danske Medier, 2012

of trust, the Danes are generally positive towards the surveillance mechanisms utilized by the state apparatus.

A change in Danish foreign politics

The Danish security policies and strategies have in many senses been influenced by the major geopolitical developments in the new millennium, namely the terror attacks of 2001, 2003, 2004 and 2005, in New York and Washington, Istanbul, Madrid and London, respectively. It has meant a change from considering Danish security policies and strategies to be domestic in scope. With the terror organizations attacking western countries at home, the scope was expanded to involve considerations of international developments and conditions; a perceived need to conduct activist foreign politics in order to ensure national security was adopted by the Danish government, with Danish military involvement in the offensive military campaigns in Afghanistan and Iraq, and less significantly, in Libya. In this way, the national security policy became linked to an active foreign policy of military engagement. This strategy was adopted in order to counter future terror attacks by acting as deterrent for potential recruits of these organizations, to disrupt boot camps for would-be terrorists and in order to weaken the central organization of the Al-Qaeda network. This was seen as a means of weakening the militant, Islamist Al-Qaeda organization. By military engagement in the region that was conceived of as harbouring the central members and acting as training grounds for new members, the Western strategy was to replace the Afghan Taliban regime supporting Al-Qaeda, and thus ensure that this region would no longer serve as a safe haven to the terrorist network.

This war on terror sought to quench terrorist organizations throughout the world by showing that terror will not be tolerated, and terrorist groups will be hunted down, but a study on Britain's military operations, by the Royal United Services Institute (RUSI), concludes that "[f]ar from reducing international terrorism … the 2003 invasion [of Iraq] had the effect of promoting it"[12], and a result of the activist foreign policy was that Denmark was put on the world map for the Muslim terrorist groups.

In an assessment made by the Danish Defence Intelligence Service (Forsvarets Efterretningstjeneste (FE)) and Danish Security and Intelligence Service (Politiets Efterretningstjeneste (PET)), the risk level of terror attacks on Western countries has been heightened since the attacks on September 11th 2001. The threat to Denmark has been further heightened as a consequence of the Danish military engagement in Afghanistan and Iraq, and even more by the Muhammad caricatures brought by Jyllands-Posten in 2005. Thus the risk of terror attacks against Danish and foreign targets in Denmark, as well as Danish targets abroad are been heightened.[13].

The Reality of the Threat

The heightened sense of a threat to Denmark was not based on figments of imagination, and the reality of the new millennium's terror threat has been made very real by a number of instances were terror attacks have been averted. In 2009, David Coleman Headley was arrested in Chicago International Airport with a ticket for Copenhagen. He was charged with and pleaded guilty to planning a terror attack against the newspaper that printed the Muhammad caricatures, Morgenavisen Jyllands-Posten. He had previously planned the terror attack in Mumbai in 2008, killing 188 people, and he had been on reconnaissance visits to the newspaper's offices in Copenhagen and Aarhus. In 2010 Lors Dukaev, a Dutch man with Bosnian roots, accidentally detonated the bomb, he had intended for Morgenavisen Jyllands-Posten, in the bathroom of his hotel room. A third instance, was in 2010, when a group of four male extremist Muslims were arrested for planning and intending to enter JP / Politikens Hus (affiliated with Jyllands-Posten) during an annual award show and kill as many as possible with the machine gun and 9mm gun, in their possession when apprehended.[14]

[12] RUSI 2014, in Norton-Taylor, 2014.
[13] Den tværministerielle arbejdsgruppe om terrorbekæmpelse, 2005.
[14] Ritzau, 2014.

Fear of terror and national security legislation of increased surveillance

The terror attacks of 9/11 2001, changed the approach taken to security policies and strategies pursued in Danish domestic politics. The terror attacks in New York, Madrid and London created awareness that the threat of terrorism on Danish soil or Danish interests was no longer an abstract potential, but a concrete risk. This new realization prompted politicians to react, and in the 13 years since the attacks on the World Trade Centre, the Danish politicians have taken a range of initiatives to counter terrorism, with a particular focus on increasing the authority of the intelligence services to conduct surveillance in order to reduce crime and reveal terrorist suspects.[15]

These legislations have variously been described as giving in on hard won civil and human rights by diluting them, and on the other hand, as being necessary to ensure public security and prevent terror attacks, but generally they can be described as classic conservative approaches to ensure security, focusing on stricter penalties for offences and expansion of the authority of police and intelligence services. This type of security strategy was pursued by the centre-right government in office from 2001 to 2011 and its successor, the current centre-left government. Here a number of the legislative implementations central to the counterterrorism efforts are presented.

Denmark was one of the first countries to meet and implement the UN and EU's framework directives on counter-terrorism. While other European countries, like Sweden and Norway, waited to implement the European requirements, Denmark was very quick to meet the requirements to the letter,[16] by means of Law nr. 378 of 6th June, 2002, also known as the Antiterrorism Package (Antiterrorpakken). This was a direct political reaction to the events of September 11th 2001, and so was influenced by these events. Prior to the implementation of the Antiterrorism Package there was no specific antiterrorism law in Denmark, but instead there was section 114. The new law package was composed of amendments to the Danish penal law, the law on administration of justice, the extrication law and law on foreigners. The existing paragraph 114 was significantly tightened by the new laws, by extending the penalty for violating the paragraph from 6 years to lifetime and widening the scope of interpretation of what constituted "terrorism" or "terrorist activity". Further, any support, economic as well as expressed, for terrorist organizations was criminalized, the police were given wider access to secret searches and confiscations, telecom companies were enjoined to log their users' traffic data, both internet and telecommunication traffic, and retain the data for a year. This only included the traffic data; the content of the communication was not logged.[17]

This was by many, considered to be the domestic legislative part of 'The War on Terror', introduced by politicians to show that they were active and capable of ensuring public security.[18]

In 2004, the Police Law (Politiloven) was amended, to allow police officers the use of administrative deprivation of freedom for up to 6 hours without having to create a case or report. This was expanded in the 2009 loutpackage ('Lømmelpakken'), which provided for administrative deprivation of freedom for up to 12 hours.

In 2006, the Danish government implemented two central antiterrorism legislations. One was the implementation of the Data Retention Directive from the EU, which meant that telecommunications companies were enjoined to retain all internet and cell phone activity of their customers in a database, which the police and intelligence services could be granted access to upon request. The Danish implementation of this went further than demanded by the directive, which only required for the data to be stored up to one year[19]. If special conditions provide for it, the police and intelligence services can conduct surveillance without a warrant, in which case they must inform the courts within 24 hours. The Data Retention directive was implemented as part of the second antiterrorism legislative implementation that year, the Terrorism Package II (Terrorpakken 2). In practice, the consequences of the second antiterrorism package was that The Danish Security and Intelligence Service (PET) was given authority to gather information from other public authorities regardless off the nature of that information and without

[15] Mortensen & Valeur, 2009.
[16] Stampe, 2010.
[17] Fenger-Grøndahl, 2013.
[18] Fenger-Grøndahl, 2013.
[19] This directive was repealed in May 2014, by the European Court of Justice. (Eurpean Court of Justice, 2014) See below for further information.

an assessment of the necessity of the information. PET was empowered to share this information with FE. The police only needs one warrant to tap all the phones and email accounts, a suspect attains. The police was also given authority to disrupt or cut off all radio- and telecommunication in an area in order to prevent terrorist activities, and are, further, given authority to use public authorities', as well as, private individuals' and organisations' CCTV surveillance and to pose demands to the quality of the surveillance.[20] Finally, airline companies were required to retain lists of all passengers and crewmembers for all flights for a year, which the intelligence services and police can access without a warrant.[21]

The law on CCTV surveillance was revised in 2008 and in 2011. The first revision provided for increased use of CCTV surveillance in public spaces and granted the police mandate to use this in investigations.[22] In the 2011 revision the municipalities were allowed, after discussion with the police and in order to promote security, to conduct CCTV surveillance in public streets with general public access.[23]

In summary it can be said that the laws securing the right to privacy have thereby been reduced significantly in Denmark. In a comparative analysis from Privacy International from 2008 Denmark received a record-breaking score and was characterized as an "Extensive Surveillance Society".[24]

2.3 Major privacy issues

The Danish Constitution of 1953 contains two provisions relating to privacy and, indirectly, to data protection. Section 71 provides for the inviolability of personal liberty. Section 72, the pivotal constitutional section in terms of privacy, states: "The dwelling shall be inviolable. House searching, seizure, and examination of letters and other papers as well as any breach of the secrecy to be observed in postal, telegraph, and telephone matters shall take place only under a judicial order unless particular exception is warranted by Statute." Section 72 also applies to all kinds of telecommunication and electronic data. The intended extent of the law has been widely discussed and whether the current practice is in line with the initial intention of this section of the constitution[25]. It has been established, though, that the lofty and idealistic first phrase of the section did not equate it to the British idea of 'my home is my castle'. Rather it was a way of giving the greatest protection against 'real violations' of privacy, since any infringement would require legal authority.[26] In many ways, the Danish interpretation of section 72 has historically often been similar to the British notion of the sovereignty of the home, which has been instrumental in shaping the Danish conception of privacy and the law on it. Nonetheless, as of 2013, there were 240 exceptions from this section, which has made some critics argue that it is an alibi of a law, which has little real effect because there are so many provisions that circumvent it. Perforated or not, the legislation provides for protection of the citizens' privacy and rights, and conditions violations on other constitutional provisions. The European Convention on Human Rights (ECHR) was ratified in 1953 and was formally incorporated into Danish law in 1992.[27]

Critique of the Measures of the War on Terror

The first Antiterrorism Package was heavily criticised for being treated as a matter of urgency, and consequently not properly worked through. The same critics point out that it was very influenced by being developed in the aftermath of the 9/11 attacks, and thus subject to hysterical rhetoric and politicians more concerned with proving that they were capable and doing something, than with doing something properly.[28] This haste also had the result that it was impossible to include the public sufficiently in drawing up the legislation, and not even the Committee of Justice felt that they had sufficient time or opportunity to question the contents. As was pointed out, the Danish legislation was implemented much earlier than

[20] Fenger-Grøndahl, 2013.
[21] Privacy International, 2011.
[22] Justitsministeriet og Datatilsynet, 2008.
[23] Justitsministeriet, 2011.
[24] Mortensen & Valeur, 2009.
[25] E.g. Berlingske mener, 2013; Kamil, 2012.
[26] Wendel-Hansen, 2013.
[27] Privacy International, 2011.
[28] Fenger-Grøndahl, 2008

both the Norwegian and Swedish, which indicates that the situation potentially did not call for such hurried course of action. Further, these legislations were justified by UN and EU framework directives, but it went beyond these, e.g. in the implementation of data retention. The Antiterrorism Package was subject to a range of criticisms. Some experts asserted that determining whether an organization can be considered a terrorist organization is fundamentally a political question with many grey areas. This is to some extend exemplified in a current situation, where members of an organization are being charged with supporting the PKK (the Kurdistan Worker's Party), while, at the same time, the Danish government is supporting the PKK's fight against Islamic State in Syria.[29]

The second Antiterrorism Package was implemented because the Danish intelligence services considered the threat to Danish interests to still be relatively high. This background has prompted some to argue that the legislation constituted a victory for the terror organizations behind the attacks on western soil in the early 00's.[30] The second Antiterrorism Package was received with criticism from many fronts, all of which had in common that the package was considered to move Denmark towards a surveillance society.[31] In more practical terms, it was criticized for imposing huge economic costs on telecommunications companies because of the data retention. Already before the data retention directive was implemented it was also widely criticized for violating privacy rights and for being an inefficient tool for investigations. It was inferred that the directive can be seen as making all citizens de facto suspects, and thereby voiding the principle of being innocent until proven otherwise.[32]

The Danish Data Protection Agency

The Danish Data Protection Agency (Datatilsynet*)* is an independent public body consisting of a council and a secretariat. The Minister of Justice appoints the members of the council. According to the Act on Processing of Personal Data the Data Protection Agency shall act with complete independence in executing the functions entrusted to it. Neither the Ministry of Justice nor any other public body has instructive authority over the Data Protection Agency, but the agency is attached to the Ministry of Justice regarding recruitment of staff and budgetary issues. Furthermore, the Minister of Justice appoints the members of the data council.[33] The agency supervises registries established by public authorities and private enterprises in Denmark, and ensures that the conditions for registration, disclosure, and storage of data on individuals are complied with. It mainly deals with specific cases based on inquiries from public authorities or private individuals, or cases taken up by the agency on its own initiative. Staff of the agency is allowed to enter any premise where a file is operated without a court order. The Act on Processing of Personal Data states that the agency shall see to it that that the processing of personal data is carried out in compliance with the provisions of Act and that any regulations issued are in accordance with the Act. The agency also has competence to conduct unannounced inspections. Decisions made by the agency are final and may not be appealed to any other administrative body. They may, however, be brought before the courts.[34]

In recent years there has been a shift in terms of what information is collected and what is traceable to persons. The citizens are monitored and registered in an increasing number of contexts. At the same time, increasingly, the information is available for a wider and broader audience. In international comparisons, Denmark is no longer among the pioneering countries that respect the basic human right: the protection of privacy. According to Privacy International, Denmark was in 2005 less able to protect privacy than countries such as Germany, Austria, Poland, France and Italy. Denmark is in category with countries such as Israel, Spain, Argentina and Sweden.[35] And the situation has deteriorated since 2005.[36] In addition, the increasing digital surveillance and registration have not resulted in a corresponding strengthening of The Data Protection Agency. Instead the authority has to lift an increasing number of tasks. As an example of

[29] Fenger-Grøndahl, 2008.
[30] Mchangama, 2009.
[31] Fenger-Grøndahl, 2013.
[32] Ibid.
[33] Privacy International, 2011.
[34] Ibid.
[35] Ibid.
[36] Togsverd, 2007.

The Data Protection Agency's ability to control the compliance of the Privacy Act it may be noted that in the period 2000-2003 there was annually completed an average of 70 inspections. Today there are reportedly 3600 data responsible and professionals dealing with data, which means that the Data Protection Agency can only inspect these every 51st years.[37] Another example is that the agency's number of employees has only increased by roughly 20%, whereas the number of cases has increased 73%.

The Data Protection Agency cannot engage with guidance in relation to the parties that may have an interest in it, just as the international work must be low priority. The agency is unable to assist in assessments of new technologies,[38] for instance, the agency refused The Danish Consumer Council's call to assess Facebook's user policy.[39] Finally, there is no guarantee that the quality of The Data Protection Agency's studies is sufficiently thorough.[40]

Generally there is not much focus on privacy when new initiatives are taken in Denmark.[41] The Danish strategy for digitalisation "The Digital Path to Future Welfare" was first presented as a plan to improve efficiency, and sat the scene to merge information and establish new systems without regard to privacy.[42] After pressure from the Digital Taskforce (a unit in the Ministry of Finance), a cross-sectorial working group was appointed to create a template for privacy impact assessment.[43]

In 2011, The National IT and Telecom Agency (IT- og Telestyrelsen), was shut down by the newly elected government. The agency's role was to fulfil tasks in information and communications under the Ministry of Science, Technology and Innovation. The agency worked to increase IT security and to promote citizens' use of IT and to support the development of Danish telecommunications industry and to ensure public communication and education. Its operations have been divided between the Ministry of Business and Growth, the Ministry of Defence, the Ministry of Finance and the Ministry of Internal Affairs.[44] The closure has been criticized as being another step towards less control with securing privacy.[45]

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

NemID

Among the Danish citizens the central register and the personal numbers are generally accepted and very few perceive the system as problematic.[46] Most Danes are aware that the personal numbers contain information that principally can be abused. But in general the Danes do not mind that the state has access to personal information about them. There is a general trust that the information is being managed with caution, and one could say that the general perception is that the submitting of personal information is an essential part of maintaining an efficient welfare state with health care, social services, etc.[47]

There are examples indicating that information from the civil registration system and the personal numbers are not always being handled with the necessary caution. Occasionally, education institutes or municipalities unwittingly leak personal numbers on webpages. This is illegal and they receive strong reprimands. But it is not difficult to find a person's personal number because it is written in letters from the tax service or other official services. There are examples of people, having their personal numbers

[37] Togsverd, 2007; Justitsministeriet, 2003.
[38] Togsverd, 2007.
[39] Mortensen & Valeur, 2009.
[40] Togsverd, 2007.
[41] Mortensen & Valeurm 2009.
[42] The Danish Government et al., 2011.
[43] Mortensen & Valeur, 2009.
[44] Den Store Danske, 2011.
[45] Elkær, 2011.
[46] In 2014 two major scandals concerning leakages of sensitive information saw the light of day. Though, both are fundamentally and principally important, they were revealed after the citizen summit, and are thus not considered here, as they had no influence on the participants at the time of the summit.
[47] Lauritsen, 2011b

intercepted, and consequently have been exposed to identity theft. Using personal numbers, some criminals have succeeded in buying a car or getting a loan in another person's name.[48]

In 2010 the CPR-register was correlated with NemID, which is a single login to all online public services and a number of other services. NemID works as a universal key, to the bank, the municipality's online self-service, to the annual statement from the taxation agency, SKAT, to the insurance, etc. NemID consists of a user ID, a password and a code card with single-use codes.[49]

The security of NemID is being criticized as being too weak and there is a risk that businesses and governments can pry into people's private data. IT-Political Association of Denmark *(IT-Politisk Forening*) thinks that there are problems with the administrative structure of NemID and that the safety of NemID's software is outdated. At the same time, the association is strongly skeptical about the system, because NemID can potentially be used by service providers to gain access to users' computers. The association claims that it is a problem that NemID is based on a Java applet. Principally this makes it possible for the state and the banks to run programs on users' computers and pry into personal matters. DanID, the supplier of NemID, has previously denied that it was possible for service providers to "perform functionality on the user's computers", but the IT-Political Association has on their website documented how easy it is to get access to users' hard drives via a Java applet. Another appeal is NemID's vulnerability to man-in-the-middle attacks, where a criminal creates a fake web page where a user enters his codes. There have already been several such attacks. The attacks have so far only been on banks, but it might as well have been attacks on public services. The association claims that there are serious errors in the system's design that makes NemID a paradise for criminals, curious businesses and governments.[50] But in general the critique of the central register, the personal numbers and NemID is rarely about whether the Danes are in favor of the registration or not. Generally the criticism is directed at how the system can be designed best possible, but rarely on the systems' raison d'être. The extensive registration is a cornerstone of the Danish welfare state.[51]

In late 2013, it was discovered through a Swedish court case, that CSC, a company whose serves hosted a number of the Danish police force's highly sensitive material, including criminal records, Schengen extraditions and more, had been hacked through more than 4 months. Ex post investigations have shown serious shortcomings of the security mechanisms of these systems, among other things it was found that it is impossible to determine whether these registers have been tampered with.[52] [53]

The role of privacy, security and surveillance issues in Denmark

According to Special Eurobarometer 371 survey titled *Internal Security* from 2011, Danes are comparatively, not very worried about security. Compared to other EU countries, Denmark has the fewest people worried or very worried about EU border insecurity (59%), natural and man-made disasters (61%), Terrorism (81%), and second fewest worried about cybercrime (74%). Furthermore the Danish population seems to be among those most content with the current level at which the security challenges are being faced domestically.[54] Despite being comparatively lower than in other EU countries, it doesn't change the fact that the majority of the population is still worried about these security threats.

Denmark has the world's highest concentration of CCTV cameras per inhabitant. With one camera per fifteen inhabitants, approximately 350.000 cameras, Denmark now has more cameras per inhabitant than England, which previously had been known as having the world's highest concentration.[55] This figure is

[48] Ibid.
[49] Nemid.dk, 2012.
[50] Rådet for Større IT Sikkerhed, 2012.
[51] Lauritsen, 2011b.
[52] Version2, 2014.
[53] The full extent of this case was not known to the public until after the citizen summit, so it will not be dealt with further.
[54] Eurobarometer 371, 2011.
[55] Davidsen-Nielsen, 2011.

subject to some uncertainty and may vary by plus/minus 50,000,[56] but the general picture is clear: Denmark is today a highly monitored country.

Today surveillance is much more than only CCTV. It is also logging and social media. The traditional and enclosed surveillance from places like airports has seeped out to the rest of society without this development being significantly questioned, maybe because it creates a heightened sense of security.[57]

In the public debates the perception and attitude towards surveillance has changed over time and today it is in Denmark generally much more accepted than previously. A "bigbrother" society is not as big a fear as it once was. Surveillance is in the broad public considered acceptable when it is used in preventing and solving crimes, but not when it comes too close to the private sphere; near the home or at the workplace.[58]

An explanation of why the increasing surveillance is not being debated more these years can be found in Denmark's historical background, as there are no traumatic historical precedents concerning comprehensive surveillance and repression as in many other European countries. In general the Danes have a large degree of social trust and confidence in the state and its institutions.[59]

Shift in attitudes

There can be identified a shift in the Danish citizens' and in the authorities' attitude toward surveillance. One can claim that it is both a matter of habituation and a greater understanding of an era of international terrorism. It is also a question of different generations. When we look at people's attitude to the registers there has been a lessening of concern. Young people are not as concerned about protecting privacy as older generations. The concern about surveillance in the form of civil registration numbers and the like is declining.[60]

This means that the authorities have increased abilities to control and monitor society, while the citizens are very active in uploading personal information about themselves on Facebook and other social media. More than three million Danes, of a population of 5.5 million, have a profile on Facebook.[61] The number of users continues to increase and so does the activity in Facebook. 72 % of the users are logging on to Facebook every day.[62] It is also worth mentioning that 61 % of Danish adults have a smartphone.[63] With a smartphone it is very easy to upload information about where you are and what you are doing. By doing so, the Danes are voluntarily sharing personal data to everyone interested, and are therefore, wittingly or not, actively contributing to the extensive surveillance.

Looking at Eurobarometer's surveys we can observe some of the general trends in the public opinion as stated earlier. Danes have a strong trust in public institutions and the same trust can be observed when looking at the population's attitude to cyber security.[64] Danes are not very concerned about disclosing personal information online compared to the rest of the European member states, and Danes have a strong trust that their online personal information is kept secure by websites and by public authorities. Respondents in Denmark (90%) are also very likely to say that they are confident doing online banking or buying things online, which strongly indicates trust in the institutions.[65]

This high degree of trust that the intelligence services and the public institutions do not abuse the authority that they are given in monitoring the public is also reflected in the public discourses regarding SOSTs, privacy and security. Danes in general, trust that public institutions and intelligence services are operating to serve the greater good and ensure public and state security, and that they are given the authority that is necessary to fulfil their task, and nothing more, and that they can be trusted to do this job without abusing

[56] Dr.dk, 2011.
[57] Lauritsen, 2011a.
[58] Ibid.
[59] Dinesen & Sønderskov, 2012.
[60] Ibid.
[61] Friis, 2012.
[62] Ibid.
[63] Kildebogaard, 2012.
[64] Dinesen & Sønderskov, 2012.
[65] TNS Opinion and Social, 2012.

their authority. For this reason, debates about privacy and SOSTs are strikingly limited and infrequent in Danish media.

The disclosures Snowden led to a short-lived debate about in what fashion Denmark was affected by this surveillance and whether the Danish government had been cognizant of the extensive surveillance and maybe had even cooperated in it. Disclosed documents from Snowden revealed that Denmark was included in the second highest tier of intelligence surveillance cooperation partners for the NSA, the so-called '9 eyes'- group, that, besides Denmark, consists of France, Holland and Norway, as well as the '5 eyes'-group consisting of Australia, Canada Great Britain, New Zealand and, of course, the USA. According to experts a categorization like this, indicates that Denmark has been cooperating intensively with American intelligence services and exchanging information. Despite the gravity of these revelations, they have not instigated a great public outcry demanding protection of the citizens' civil rights.

The following section will focus on three of the SOSTs that have received attention in the Danish public debate, and is primarily informed by three different surveys; one survey from the Eurobarometer on cyber security, one Danish survey done by the research company AC Nielsen AIM and one survey by the Danish Board of Technology (DBT), conducted in lieu of the PRISE project.[66] The Eurobarometer survey can mainly be used to identify some of the same tendencies as mentioned earlier in this national feedback, where the two Danish surveys can be used to illustrate the public opinion on different surveillance technologies.

CCTV

In Denmark, CCTV is widely considered to be an effective surveillance and crime-fighting tool. Evidence of this conception can be seen in the record amount of CCTV cameras in use in Denmark, with one camera per fifteen citizens,[67] and a projected development of up to 50.000 new cameras a year.[68] Some people are raising concerns that the effectiveness makes the cameras dangerous because they promote an Orwellian, panoptic surveillance society of behavioural self-correction. When looking at the academic research the conclusion is, that while CCTV can be used in some situations, it is overall not an effective tool to prevent crime[69].

There are three recurrent arguments for using CCTV in Denmark. The first argument is that CCTV prevents crime; CCTVs are considered to have a deterring effect, so people intending or considering criminal activity, reconsider and decide against it. The second is that CCTV is increasing the citizens' level and feeling of security; one do not have to fear assaults or robberies. The third argument is that CCTV is efficient in the police's investigative work. Although these presumptions seem obvious, there are reasons to doubt if these arguments are valid when looking at the existing academic research. At the same time it is unfortunate that much of the public debate focus on CCTV's positive effect on crime.[70]

There is no Danish research on this field that can confirm or invalidate that CCTV in public spaces has a preventive effect on crime, so researchers are looking at research from other countries. Unfortunately the results from this material do not give a clear conclusion. In attempt to solve this problem with varying conclusions researchers are doing meta-surveys. The idea is to collect the different conclusions from a number of surveys and on basis of that assess whether it is likely that CCTV will prevent crime in different situations. On that basis it seems that CCTV is effective on parking lots. In return CCTV has very little or no effect when it comes to dangerous crime such as violence. It is especially the violent crime the politicians and the police are trying to prevent by installing more cameras.[71] Many cameras are being put up and installed in problematic neighbourhoods and social housings to reduce vandalism, robberies and assaults.

[66] Though this data was gathered with a slightly different purpose, they still make up the only available data on public opinion regarding data retention and biometrics.
[67] Davidsen-Nielsen, 2011.
[68] Sikkerhedsbranchen, 2009.
[69] Lauritsen, 2011b.
[70] Ibid.
[71] Justitsministeriets Forskningsenhed, 2006.

Again there is no clear evidence whether the cameras alone are leading to a decline in the level of crimes, because much else than CCTV is being done in these neighbourhoods to prevent crime.[72]

The main pedestrian zone in the centre of Copenhagen is one place in Denmark with a comprehensive CCTV surveillance. Many of the cameras were installed in 2008, immediately after a young man was killed only because he would not give his hat to the perpetrators. Naturally the killing received a lot of media attention and the politicians were prompted to answer how they would prevent similar incidents in the future. The then Minister of Justice believed (as many other politicians and a big part of the population) that more cameras would prevent further incidents like this, in spite of the fact that the killing had actually been monitored on CCTV, which obviously did not have a preventive effect in this case.[73]

In the research there has been less focus on CCTV's effect on the citizens' feeling of security. But surveys show that there is no clear evidence that more cameras create more feeling of security. It is possible that CCTV creates a feeling of security, but more cameras can also create a feeling of insecurity. There are different examples where the CCTV has increased the feeling of security, but there are also examples where CCTV has increased the feeling of insecurity. That could be if the cameras are not being perceived as protecting but as a signal showing that the area is insecure.[74]

In the public debate CCTV is portrayed as very efficient in investigative police work. A reason for this is that CCTV footage is often shown in the media and it is always of a good quality. If there is nothing to see on the footage there is no reason for the police to show them in the media and the public is hereby only shown cases where CCTV is effective.

Smart CCTV footage is often considered to be of potential benefit to police investigations. The police know that smart CCTV does not constitute a miracle cure, but, rather, it is another 'tool in the toolbox' and sometimes it can make the difference between a solved and an unsolved case. But many examples exist where the police have not been able to use the CCTV in the investigation because the quality is insufficient or the crime is not captured on the camera. It is therefore not possible to conclude whether CCTV is increasing the efficiency of the police work. The utility of the footage depends on the effort put into using it by the police, which, moreover, depends on the crime in question.[75] In minor cases the police will not use many resources in using unclear photos from CCTV, but in important cases they will put effort into using all available clues.

Public opinion on CCTV

According to an opinion poll made in 2009, 85% of Danes disagree that there is too much CCTV surveillance, while 80% are recorded as opining that CCTV surveillance creates peace of mind.[76] The same tendencies can be found in the survey by the research company AC Nielsen AIM. The survey, investigating public attitudes to CCTV and related laws, was commissioned by The Danish Crime Prevention Council (Det Kriminalpræventive Råd), The Danish Bankers Association (Finansrådet), The Financial Services Union Denmark (Finansforbundet) and The Danish Trade Organisation for Safety and Security (SikkerhedsBranchen) prior to the amendment of the act on CCTV surveillance. Another objective was to describe the development of Danish attitudes to CCTV. The results of the survey were therefore compared to the results of a similar survey conducted by Gallup for the Danish Crime Prevention Council in 1999.[77]

In general the Danes are very positive about CCTV, and it has become an accepted part of society, and the development with an increasing number of cameras is not something Danes are very worried about. As much as 97 % of the population is generally in favour of CCTV in one or more locations. Most are positive, because they believe that CCTV prevents crime. For many people - especially women - CCTV also helps provide a feeling of safety.[78] There are no reservations when it comes to surveillance in places such as banks, post offices, petrol stations and shops, but almost all (90 percent) are pleased that signposting is

[72] Lauritsen, 2011b.
[73] Lauritsen, 2011b.
[74] Lauritsen, 2001b.
[75] Lauritsen, 2011b.
[76] Bjerregaard, 2009.
[77] Det Kriminalpræventive Råd, 2005.
[78] Ibid.

required in areas that are monitored by CCTV. The closer to the private sphere, such as the apartment block, entryway and home, the attitude towards CCTV is more sceptical. The dominant reason for people's negative attitude towards this type of CCTV is that it infringes privacy. Moreover, most are negatively disposed towards CCTV in places where you are "partially undressed", for example in swimming pools and locker rooms. Many do not like to be monitored at the workplace. A smaller proportion (16 percent) indicates that they fear abuse of the recordings. "The Surveillance Society", which has previously been the spectre of debate, is not people's primary fear.[79]

There are differences in the approach to CCTV depending on age and education. The elderly are typically more positive than the younger, and people with shorter educations are more positive than people with higher education. When asking whether people think that companies and shops should be allowed to install CCTV - and if they are allowed to save the recordings - the general picture is more mixed. Half of the population believes that companies and shops should apply for permission to monitor their own outdoor areas, whereas the other half believes that it is okay to allow companies and shops to monitor and store the recordings. The current legislation states that private companies and organizations are not allowed to conduct video surveillance in areas of general traffic, but they are allowed to monitor facades, entrances, fenced areas or similar, provided that the recordings are not stored.[80]

We cannot talk about a dramatic shift in public attitudes between 1999 and 2005. Compared to 1999, there was a slight decrease in the proportion of people positive towards CCTV near the home, while there was a slight increase in the proportion of people positive about CCTV at the workplace and in the changing- and fitting rooms. There was a decrease in the number of people that were positive towards CCTV at train stations. The majority of Danes were still negative towards CCTV in public toilets, but the proportion of positive rose from 20 to 28 per cent.[81]

Biometrics

In the public sector, biometrics is today being used by the police (DNA records, registration of fingerprints) and the passport-issuing authorities (digital photos and fingerprints) and integrating biometric security solutions into a future citizen card has been considered. The Danish National Police started issuing electronic passports in October 2006. These new, secure e-Passports feature a polycarbonate data page containing a contactless microprocessor chip running the highly secure operating system. The chip not only features the information identity already laser-engraved on the first page, but also contains the passport holder's digitized photograph.[82] Furthermore there are plans about storing retina scans in Danish passport as well. The timing of the introduction of the new passport is yet to be determined. The plans about introducing a biometric citizen cards, where a number of features (such as including social security card, driver's license, credit card and digital signature) are combined in one card, has so far been postponed because it is currently too expensive. Once prices reach a more affordable level, implementation of these, more secure and thus preferable, biometric citizens' cards will be one step closer to realization.[83]

It is particularly the private sector that has implemented biometrics in several areas, both to monitor and register employees and customers. In several industries biometric data is increasingly used identify customers or employees. The biometric technologies are here being used in relation to payment and for physical and logical access control, such as access to computers, databases or specific applications. The Danish Data Protection Agency has given the discotheque Crazy Daisy permission to register their costumers' fingerprints (with their consent) to facilitate their access. The hospitality industry is working on a nationwide 'bully register' based on biometric identification. A biometric citizen card could be used for much more than exchange of information between citizens and the state, it could also give access to online banking, function as debit cards, as key card to work places and as transport ticket.[84]

[79] Ibid.
[80] Ibid.
[81] Ibid.
[82] Privacy International, 2011.
[83] Teknologirådet, 2010.
[84] Ibid.

At a interview meeting, conducted in 2006, the use of biometrics for controlling access divided the participants, about security technologies and privacy, into two groups.[85] Approximately 40 percent of the participants would not feel comfortable, if any kind of biometrics was used, while the rest felt comfortable about the use of retina, fingerprint and, to a lesser extent, facial recognition.

When the technology is connected to specific situations and places it became more acceptable to the participants. The questionnaire reveals that a majority of the participants could accept the use of biometrics in airport and border control (approx. 60 per cent of the participants). While a minority of approximately a quarter of the participants would accept biometrics in banks, bus and train stations, sports arenas and stores.[86]

Another possibility with biometrics is registration of biometric data in a central database as a step to fight crime. The citizens were divided into two almost even groups of for and against such a register. The group discussions indicated that the thought of a DNA-register was quite unfamiliar to the participants, even though such a register is in existence today.[87]

Data retention[88]

Fear of terror has influenced Danish legislation and surveillance since the attacks on the New York World Trade Center in 2001. Most important is the previously mentioned Antiterrorism Package and the Data Retention Directive. The Data Retention Directive was introduced to give the police and intelligence services more tools to prevent terrorist attacks and possibly unravel terrorist networks. Specifically it meant that all communication using digital communication services should be stored for one year. The logging includes information about which devices that are talking to each other, where they are located, and when communication is taking place. The data retention directive took effect in 2007 and concerns mobile and landline telephones, SMS, EMS, MMS, emails, Internet telephony and other Internet communications.[89] Denmark was the first country to implement the surveillance on the basis of the EU directive data retention from March 2006.[90] More than 12.6 million Euro was given to The Danish Security and Intelligence Service (PET) for the strengthening of IT systems and interception of communications, in order to implement the directive.[91]

On the basis of the EU directive on data retention, the authorities can override respect for privacy, 'if it is in accordance with the law and is necessary in a democratic society in the interests of particular national security and public safety for the prevention of disorder or crime or for the protection of intellectual property rights or freedoms'.[92]

The act results in an enormous amount of registered information. It has been suggested that the telecommunications operators in 2010 made 550 billion registrations, corresponding to 100,000 per citizen pr. year.[93] The price for this huge registration is not clear, but it has been suggested that the price for only establishing the system was around 26 million euros, and that the annually operating cost is around 6.7 million euro.[94]

During the drafting period the proposal was heavily criticized by ISPs, cooperative housing associations, and non-governmental organizations for being disproportionate and inconsistent, *e.g.* letting private

[85] Teknologirådet, 2006.
[86] Ibid.
[87] Ibid.
[88] As of April 2014, the European Court of Justice abolished the data retention directive, as it was found to be inappropriately affecting fundamental human rights. The abolition was a fundamental development, but happened after the citizen summit and thus had no influence on the results from the summit.
[89] Justitsministeriet, 2006.
[90] Andersen, 2007.
[91] Ibid.
[92] Justitsministeriet, 2006.
[93] Willer, 2013.
[94] Pedersen, 2007.

entities store huge amounts of personal information while at the same time being easy to evade because of the many exemptions, such as libraries and universities not being included.[95]

There is now some recognition that the data retention contains restrictions and that it is very easy for clever terrorists to circumvent it. Some argue that the act should be completely abolished, while others have indicated that they prefer to try to close the gaps. It has for example been mentioned that librarians should check the identity of users of the library's computers, just as buyers of prepaid telephone cards should be registered.[96]

Data retention and scanning and combining of personal data from different databases can be used for both investigation and prevention of crime and terror. Retention, scanning and combining of data was considered to be acceptable to the majority of the participants at DBT's 2006 interview meeting as long as the purpose is *investigation* of specific terrorist attacks or crimes that have occurred. When considering *prevention* only a quarter of the participants were willing to accept the use of stored data.[97]

At the same time the majority of the participants found data retention to be potentially privacy infringing. For example they stated that traffic data from communication should not be stored for purposes beyond billing, which was the case. The opposition towards data retention could be rooted in the fear of data being used for something else than the original purpose, so-called function creep. Almost 80 per cent of the participants indicated that function creep is a serious privacy problem. In the group discussions the participants expressed anxiety towards the possibility that someone can create a profile of them based on personal data from different databases.[98]

Even though they were worried, about half of the participants considered scanning and combining of personal data a good tool that the police should use for the prevention of terror. Some of the sceptical participants emphasized that the amount of data can also get too enormous and therefore become useless. It is worth noticing that 4 out of the 27 participants stated that data retention and scanning of databases with personal information is never acceptable. At the same time the majority of the participants found it unacceptable for governmental institutions to store all data they find necessary for security reasons. This suggests that to the participants data retention involves some serious privacy problems. This was also the impression from the group discussions where many participants expressed their worries about the growth in data retention. Some participants pointed to the problem of who has access to this data. However, other participants found this worry exaggerated. Instead they questioned the idea that anyone should have a private interest in looking at the data of ordinary people.[99]

[95] Privacy International, 2011.
[96] Lauritsen, 2011b.
[97] Teknologirådet, 2006.
[98] Ibid.
[99] Ibid.

3 Process design – the citizen summit in Denmark

3.1 Organizational setting

Location

The Danish citizen summit took place in Aarhus, the second largest town in Denmark and the regional capital of Central Jutland. The demographics of this region reflects the diversity of Denmark as a whole when it comes to gender, age, profession and level of education, thus it provided a good basis for recruiting citizens for the summit with the required demographic diversity.

"Centralværkstedet" - the neighbour to the central train station in Aarhus – provided a perfect venue: easily accessible and able to provide screens and sound system, check-in area, food, service-minded staff and a good atmosphere.

The relatively high amount of missings per question in the survey results can be predominantly attributed to the poor WIFI-infrastructure of the venue.

Staff

Students, mainly from anthropology and political science at Aarhus University as well as DBT staff had the role as table facilitators. A training workshop was held before the summit, where methodology, voting system, content and programme of the summit was presented, and the table facilitators tried the discussion rounds themselves.

At three tables staffers from the DBT were taking extensive notes from the discussions and recommendation rounds.

Senior project manager at the DBT Jacob Skjødt Nielsen had the role of head facilitator. Project manager at the DBT Nanna Engberg was assisting this job, and project assistant at the DBT Emma Christiani Skov had the role as floor manager, assisting table facilitators and had the contact with the staff at the venue.

Citizen recruitment

Citizens were recruited by DBT via contact letters with an invitation to register for the event. The letters were sent 2 months before the summit to 6000 citizens, who were selected randomly from the national register (CPR). The selection was done, so that people under the age of 45 was overrepresented, as this group has been experienced to be harder to engage. Apart from the adjustment according to age based on previous experiences with recruitment for citizen summits, citizens were chosen so that it reflected the overall national demographics with regards to gender and degree of urbanization.

When the registration had been open for app. 3 weeks, it was obvious that the requirements would not be met, neither as to the number of participants, nor to the diversity among them regarding age. Therefore it was chosen to send additional 2500 letters to citizens under the age of 40 app. 1 month before the citizen summit. The Danish postal service provided the addresses for the second round of contact letters.

Based on previous experiences it was expected to get 400 sign-ups from the 6000 letters alone. Unfortunately we ended up having only 227 who registered for the event. From this group some had to withdraw their registration already before the summit due to illness, change of plans and other personal reasons. Thus we ended up having 169 participating citizens at the summit.

3.2 Structure of the citizen panel

Despite the extra efforts to reach the 200 citizens, and to have a group that reflected the overall national demographics with regards to age, there was an overweight of well-educated, elderly males.

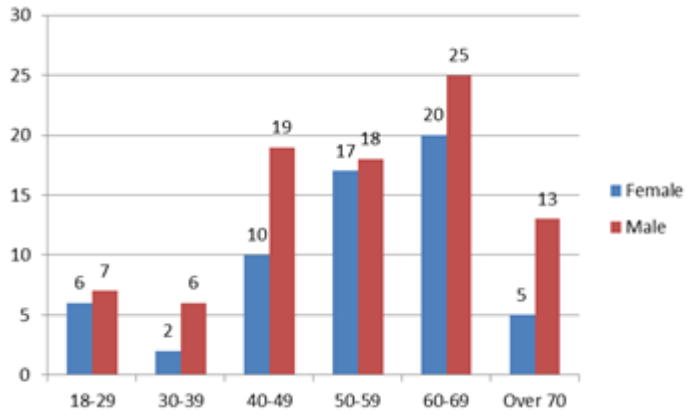


Figure 1: Age and gender composition, absolute numbers. Female total: 63; Male total: 94.

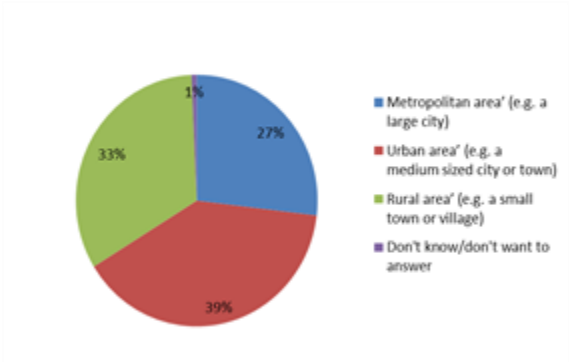


Figure 2: Area of residence

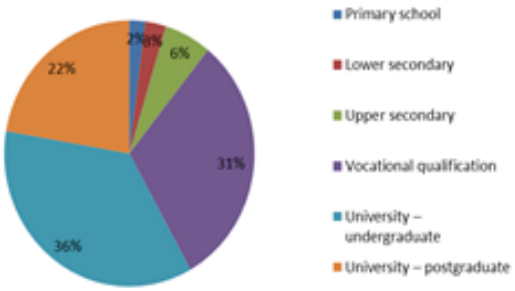


Figure 3: Educational level

3.3 How citizen assess the summit

The spirit at the citizen summit was good; most of the participants contributed eagerly in the discussions and formulation of the recommendation and expressed satisfaction with the structure and programme of the event.

The information material – both magazine and films – was well received. More than 60 percent of the participants stated that they didn't change their attitude towards SOSTs from participating, and approximately the same percentage stated that they were more positive than more critical towards SOSTs after participation (see figure 6 below).

Participants' assessment of the value of the event – both for themselves and for politicians – is crucial for the reputation of the methodology and thus the success of future citizen summits. Therefore it is positive to see the most citizens both felt that they gained new knowledge themselves, and that 73% considered the meeting to produce knowledge valuable to politicians.

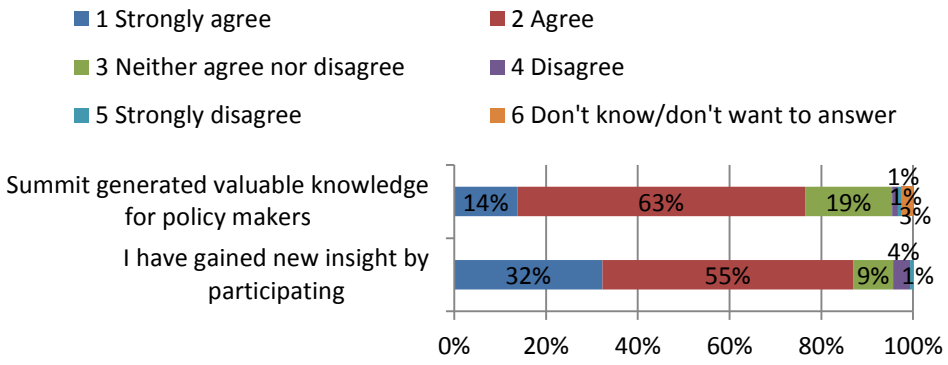


Figure 4: Attitudes on new perspectives and knowledge for policy makers

That the participants gained new insights is also reflected in the differences in the answers given to the question regarding their perceived knowledge ability about SOSTs, as seen below.

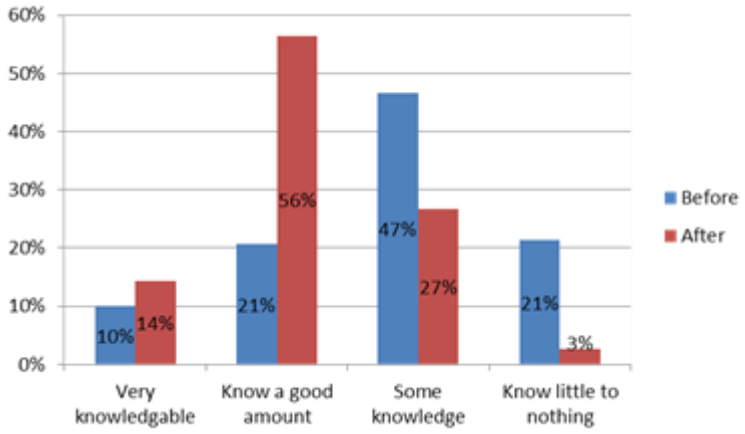


Figure 5: Perceived knowledge about SOSTs, before and after the summit

As can be seen in Figure 5, only 31% of the participants assessed that they were either 'very knowledgeable' or 'knew a good amount' prior to the summit. By the end of the summit 70% perceived themselves to be in this category. Maybe more importantly, only 3% perceived themselves to know little to nothing after the summit. Though the participants felt that they gained new insights and knowledge about SOSTs, 59% did not feel that it changed their attitude towards SOSTs, but we will get back to this later.

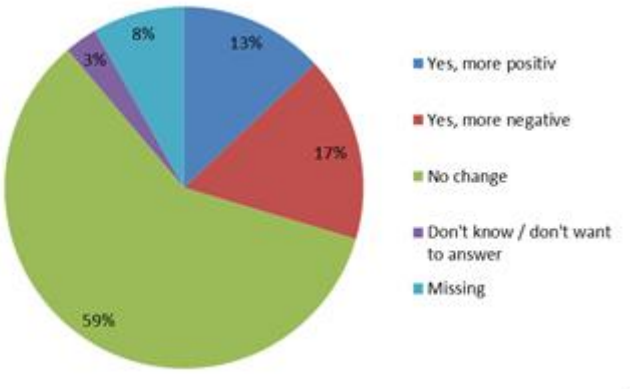


Figure 6: Changing attitudes towards SOSTs

10 postcards and an email with comments and evaluations of the event were received. Besides appreciating a well-conducted event, these suggested more time for debates, limitation to the number of questions (there were too many), and critique of some of the questions, that were considered vaguely formulated, easy to misunderstand or up for individual interpretation. Several objected to the questions "I am concerned…" because they did not know what to answer when they were not concerned.

4 Empirical results of the citizen summit

This section presents and analyzes the main quantitative and qualitative results of the Danish citizen summit. The analysis utilizes a combination of the qualitative and quantitative data gathered during the summit, in order to create a more holistic and in depth representation of the complex of attitudes towards security, privacy and surveillance. Included in the analysis are the votes given by the participants in the survey and input from the three rounds of discussion and the final recommendation round at the tables. The analysis includes both technology-specific and more general foci.

4.1 General attitudes on privacy and security

A large majority of the participants feel safe in their everyday life (90%) and feel that Denmark is a safe country in which to live (92%). As noted above, Danes have high degree of mutual trust and trust in the public system, something which is probably significant in explaining this response.

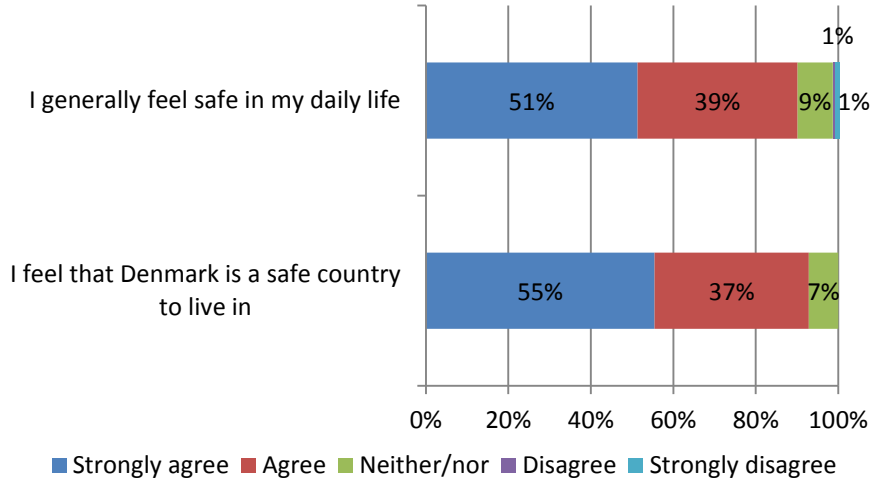


Figure 7: Perceived safety in daily life and of Denmark

Despite this perceived safety in everyday life and domestic considerations, two things are very interesting to note (see Figure 8). First, 92% of the participants responded that they worried when they were online on computers, smartphones or other devices. It, importantly, shows that surveillance might also have a counterproductive effect of making people more worried! Compared with above results, it indicates that people perceive of the internet as a specified sphere, separate from their daily life, which they feel unable to control and have less trust in. This, at least, was expressed by several of the participants in the discussion rounds, who felt that data privacy was a very opaque subject. They expressed a sentiment of being unable to control who collected data about them, when, how and for what purposes, and that all of this was generally characterized by being very opaque. In other words, people feel that they can't know exactly who is looking over their shoulder when they are using the internet. Even though they feel the internet interaction is something separated from the physical world, something still indicates that the factor of people often being solitary when surfing the internet or in an intimate sphere of perceived privacy, is heavily influencing the way they think of internet interaction.

Second, it is very interesting to note, that even though people feel, even to a high degree, safe in Denmark and in their everyday life, 63% ('strongly agree' or 'agree') still responded, that SOSTs should be routinely implemented to improve national security. This seems do derail the assumption, which expects that the more citizens are concerned about their security, the more they are likely to accept SOSTs. In this case, there does not seem to be a causal link between feeling safe and supporting implementation of SOSTs.

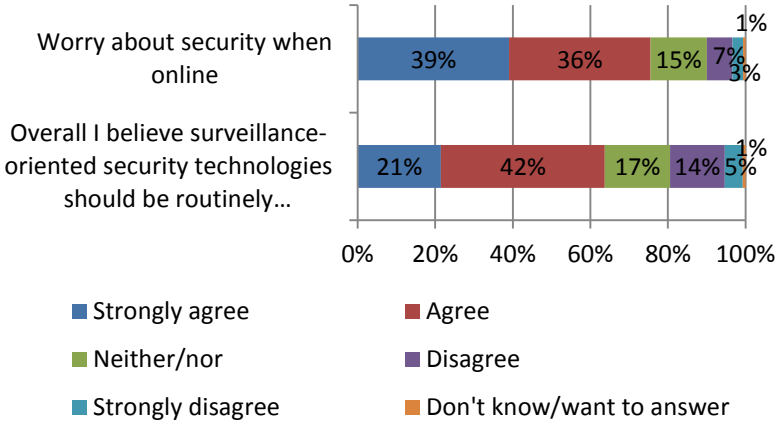


Figure 8: Perceived online security and support of implementing SOSTs routinely (prior to meeting)

Changes in the security attitudes

In order to uncover if, and how, attitudes had changed during the summit, as a result of the discussions, the videos and the further elaboration on the SOSTs, the participants were asked similar questions at the beginning and end of the summit.

The first question concerned whether they supported routinely implementing SOSTs in order to improve national security.

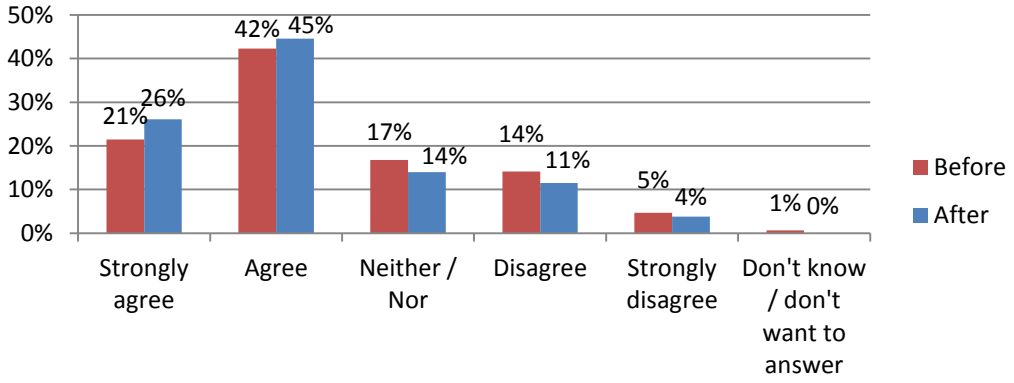


Figure 9: Change in attitude to whether SOSTs should be routinely implemented for national security purposes

The results (shown in Figure 9) indicate a tendency for the participants to have grown slightly fonder of SOSTs in the course of the summit. Though the support has not markedly increased, it has increased consistently across the board, with the support for SOSTs as national security tool, increased from an aggregate of 63% to 71% of the participants, and the amount of detractors decreasing from 19% to 15%.

The second set of questions concerned the degree to which the participants agreed that alternatives to surveillance based approaches should be given higher priority. Interestingly, the results of this poll did not change significantly in the course of the meeting. 63% agreed at the beginning at the meeting, while 62% agreed at the end of the meeting.

The third set of questions concerned whether participants considered that the routine application of SOSTs would erode their own and general privacy, respectively.

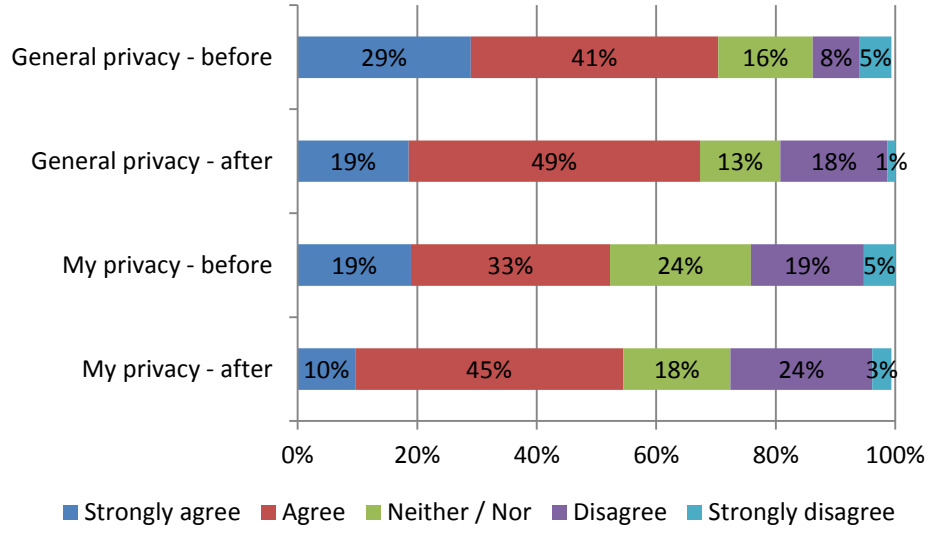


Figure 10: Differences in worrying about SOSTs eroding general and personal privacy, before and after the summit

The results from this poll suggest that, at the conclusion of the summit, compared to before the summit, more participants disagreed that they were concerned about the erosion of general and personal privacy on account of SOSTs being applied routinely. It also indicated that attitudes towards this question were less polarized after summit, with fewer in either of the 'strongly' categories. Despite the increase in unconcerned participants and the decrease in polarization, the vast majority were still concerned about the application of SOSTs when it comes to erosion of privacy, more so for the general privacy than for their own, but in both cases it is a significantly higher percentage worrying (general 68%; personal 55%) than those not worrying (general 19%; personal 27%). This difference between concerns for personal juxtaposed with general privacy will be dealt with in more detail below. Interestingly, the amount of people who worried about personal privacy increased slightly, unlike general privacy, possibly a result of them realising the extent to which SOSTs are being applied, but again, this change is marginal in the big picture.

Also interesting, is to see that the participants were more decided after the summit than they were before, with the neither agree nor disagree categories reduced by 3 and 6 percentage points, respectively for the general and personal privacy.

Perceptions of individual and collective aspects of privacy

There are many different interpretations of what constitutes privacy, and almost as many ideas of how important it is. To some it has physical or spatial character relating to intimacy, solitude, while others consider it to relate to anonymity of actions, proclamations or information about them.

The results from the survey conducted at the citizen summit shows that the Danish participants distinguish between their 'own' personal privacy and privacy in general, with the poll indicating that, weighing heavier on the minds of the Danish participants, is the concern for 'general' privacy. As shown above in Figure 10[100], 10% strongly agreed that they worried SOSTs were eroding their privacy, while 19% answered that they worried SOSTs were eroding privacy in general. The same picture goes for those responding 'agree', with 49% worrying about privacy in general and 45% for their own privacy. The same seems to count for those responding 'disagree' or 'strongly disagree', with those voting that they weren't worried about SOSTs eroding their privacy amounting to 27%, whereas the percentage not worried about general privacy totalled 19%.

[100] Here the results from the last poll will be used, as they correspond best with the participants' current views.

When turning to the two SOSTs dealt with in depth at the Danish summit, a fairly marked difference is discernible, both between how the SOSTs are perceived, but also how participants perceive the SOST in relation to themselves contra a common concern.

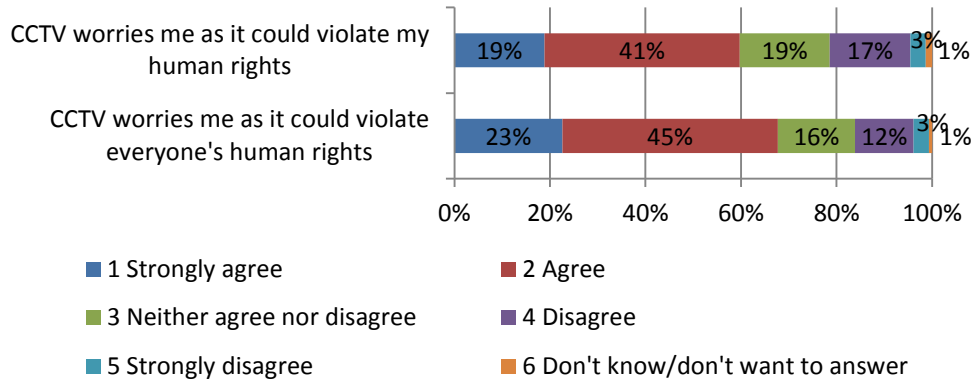


Figure 11: Worries whether smart CCTV violates human rights

The results of Figure 11 demonstrate a widespread concern, that smart CCTVs could be violating the human rights of participants, which also indicates that the participants feel somewhat uneasy with this technology. This will be dealt with in more detail later on. For the current analysis, what is noteworthy is that the concern regarding smart CCTVs violation of human rights, confirms the tendency seen in Figure 10. Both for 'strongly agree' and 'agree' it applies, that the proportions are larger for the concern relating to everyone, which is, not so much the participants themselves.

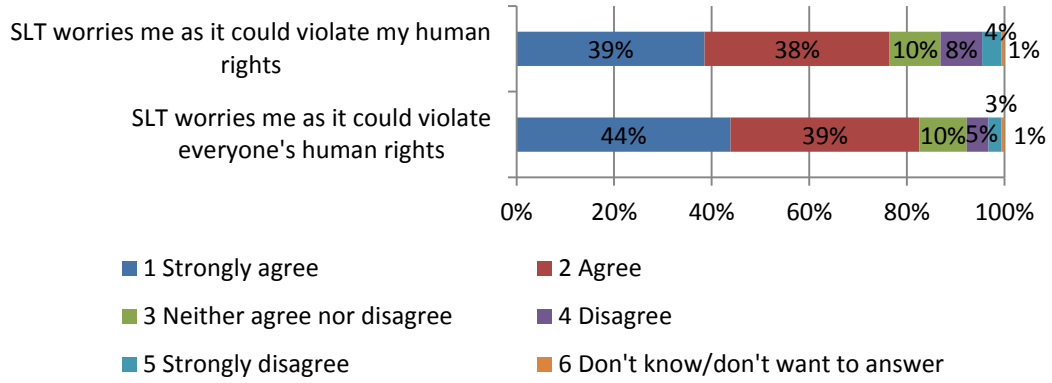


Figure 12: Worries whether smart SLT violates human rights

When we turn our attention to the results for the similar poll regarding SLT, we can see an analogous tendency to what has been seen in the previous two figures. In Figure 12 we can see that 77% agreed or strongly agreed, when asked about concerns that SLT could violate their own human rights, while the same numbers for concerns about everyone's' human rights are 6 percentage points higher.

So through three different poll results, a tendency is clear. While people generally are concerned that the implementation of these SOSTs might have a deteriorating effect their own privacy and violate their human rights, they are considerably more worried about how SOSTs could potentially violate the rights and privacy in general. When looking back at Figure 8, this seems contradictory; the participants worry that SOSTs might erode privacy and rights while, at the same time, they support its implementation. This

seeming contradiction will be illuminated below, through the further analysis of the results of the citizen summit.

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

In the previous section, a more general inquiry into the participants' attitudes towards security and privacy were made. The following section takes a more detailed look at how they perceived the application of SOSTs and their perception of and attitudes to the two specific SOSTs treated at the Danish summit – Smart CCTV and Smartphone location tracking (SLT). These can both be considered emerging surveillance technologies that will increasingly be utilized in the future, and thus the general public attitude towards them is important to uncover, in order for decision makers to make informed decisions that take the concerns and attitudes of those they are to represent into account.

As might be expected, given the longer track record of CCTVs in Denmark, more participants felt that they understood what smart CCTV is (89%) than what SLT is (79%), but this indicates that the participants were fairly confident that they understood the subject matter, which was also the impression given in figure 5, which showed that prior to the summit, 78% of the participants felt that they had at least some knowledge, and at the end only 3% felt that they had little to no knowledge about SOSTs.

As will be shown below, the Danish participant exhibited a curious combination of reservations towards SOSTs in terms of it being intrusive, violative and making them feel uncomfortable, but at the same time they were generally voting in favour of its implementation. Why this might be, is sought to be answered in section 4.3 on trust in security authorities.

The Danish citizen summit revealed that there is a general positive attitude towards SOSTs as a tool for increasing efficiency of infrastructure or as a tool for emergency services. Many participants for instance perceived CCTV as a positive instrument for monitoring traffic and thereby alerting authorities in case of traffic jams or emergency, and many recognized the positive benefits of SLT as tool to enable a flow at places with many people, e.g. an airport. The use of SLT to help find missing or hurt people was also perceived as positive.

As already shown above, the majority of the participants supported the routine implementation of SOSTs, even more so after the summit than before, and 45% of the participants agreed that national governments might as well make use of SOSTs if they are available, while almost a third disagreed with this. So while most agree on the implementation, there is a stronger tendency that the implementation of SOSTs is not a routine matter, and should not just be uncritically implemented. In line with this, is that 62% of the agreeing that alternative security approaches that do not entail surveillance should be given higher priority. In fact this was very uncontroversial, with only 12% disagreeing, but 25% being content with the current distribution of efforts between surveillance measures and the alternatives.

When considering SOSTs in general, the results from the survey showed that most participants had a number of concerns, in fact, very few of the participants were unconcerned about the information that is collected about them.

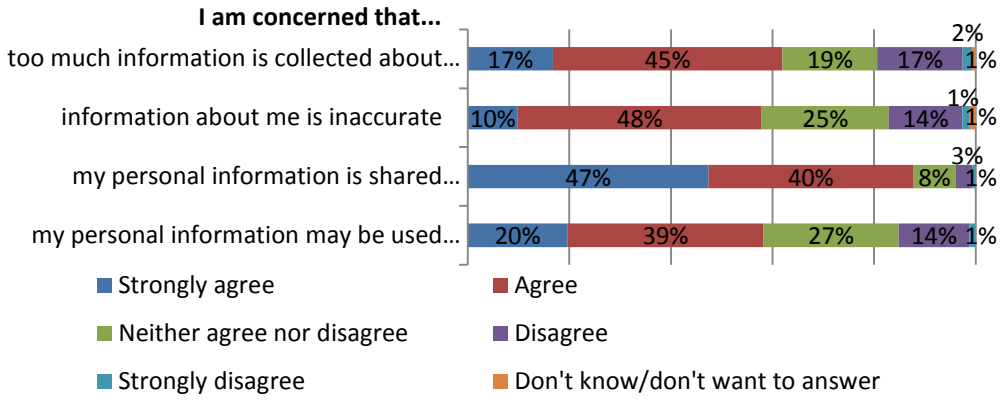


Figure 13: Concerns about different factors

What worried the participants the most, was that their personal information is shared without their consent, which mirrors a the feeling of powerlessness when it comes to controlling information that was also expressed by several participants at the summit, which in turn, is indicative of the feeling that many of the them also had, that it is very opaque exactly what data is collected about them, by whom and for what purposes. One middle-aged woman said "I think a lot of it [the collection of data] is something that is signed up for without realizing it, because most don't read the terms and conditions". When most participants at the same time worry that too much data is collected about them and that it could be used against them, a picture is emerging of people feeling kept in the dark and consequently powerless. This is further, confirmed by the results shown in figure 10 above. Here it was shown that more than 50% worried that SOSTs were eroding their privacy.

This seems to paint a picture of general distrust and detraction towards SOSTs, but as will be shown below, the picture is more nuanced than that.

4.2.1 Perceived effectiveness vs. intrusiveness of SOSTs

Having shown that the participants felt that they had substantial knowledge about SOSTs in general and the two SOSTs at hand, smart CCTV and SLT, we now turn to how the participants perceived the effectiveness of the SOSTs and how intrusive they considered them, and whether they would agree to accept the intrusiveness on account of the benefits that the SOSTs provide.

Effectiveness of SOSTs

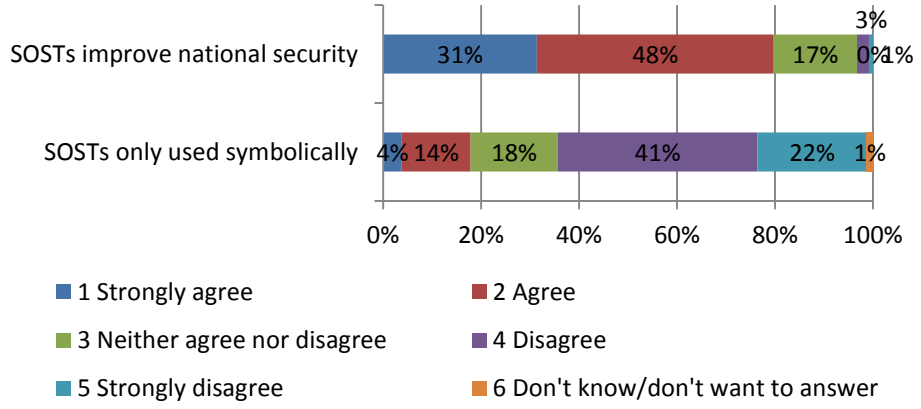


Figure 14: Perceived efficiency and purpose of SOSTs

The effectivity of SOSTs in general was largely undisputed by the participants in the Danish summit, and very few believed that SOSTs were only implemented in order to show that something is actually done to fight crime. As figure 14 shows, 31% strongly agreed that the use of SOSTs improve national security and 48% agree; a largely unequivocal result: the participants believed in the efficiency of SOSTs. This strengthens the results seen in figure 9, showing that the participants in general were in favor of implementing SOSTs.

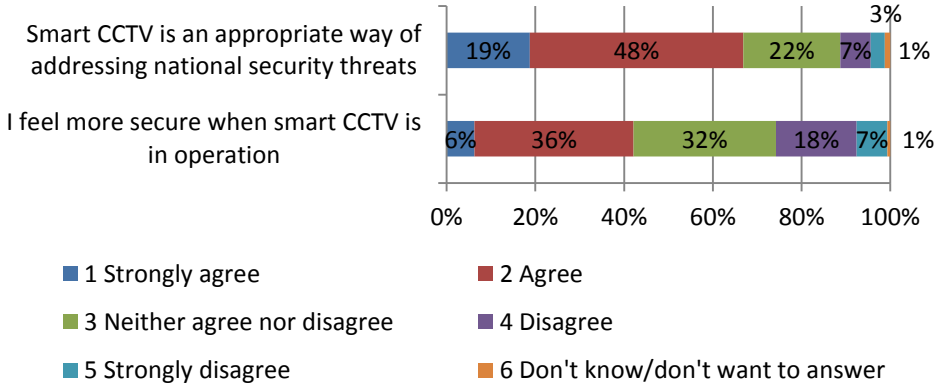


Figure 15: Smart CCTV enhancing security?

If we turn to the individual SOSTs, we can see that the participants were generally in accordance that smart CCTV is an appropriate way of improving national security. Very few outright disagreed with this. Further, the largest portion of them (42%) felt safer when smart CCTV is in operation. As will be shown below, when asked directly, 58% of the participants voted that they believed smart CCTV improves national security. So from this, it can generally be inferred that smart CCTV was perceived among the participants as being both appropriate and effective.

One reason why participants were more divided when it comes to whether they felt safer when smart CCTV is in operation could be that they hold the perception that smart CCTVs are not very preventive, but very effective after the fact, that is, in solving crimes once they have happened. This was also expressed by almost a third feeling neither more nor less safe when smart CCTV is in operation. This was also exhibited in the discussion around several tables, with the example of the Boston-bomber occurring several times. He was not exposed in time, but CCTV was used in solving who was the perpetrator. Another frequent example of accept was of the use in airports, traffic hubs, military buildings and government buildings.

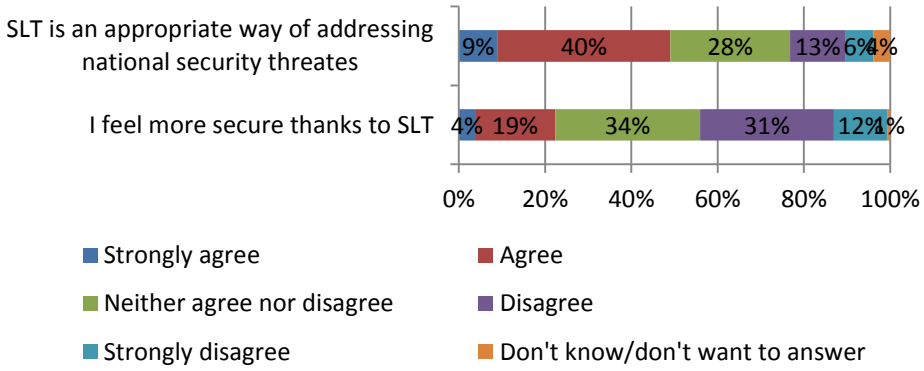


Figure 16: SLT enhancing security?

When it comes to SLT there was a little more discordance between the participants. While almost 50% still agreed that it was an appropriate means of addressing national security threats, there was significantly more disagreeing, than in the case of smart CCTV. It is very thought-provoking that, while 58% believed that SLT improves national security, only 23% felt more secure due to SLT, while 43% disagreed. This indicates that SLT may be perceived as more controversial in the eyes of the participants.

These results indicate that, while the participants generally believe in the efficiency of SOSTs, they are not entirely uncritical to which SOSTs are used and they do not unequivocally feel safer just because of its implementation. So far it seems that smart CCTV was considered both more appropriate and efficient as well as better at improving sense of security, than was SLT.

Intrusiveness of SOSTs

Having considered how efficient and effective the participants perceived SOSTs to be, next, the other side of that coin is analysed: the level of intrusiveness.

As was shown in figure 10, it is evident that a substantial amount of the participants were worried about how SOSTs influenced privacy. Both their own privacy and the privacy of others, with the latter being that which had most worried. This again substantiates that implementation of SOSTs is not an insignificant matter in the eyes of the participants. Only one in four did not worry about their own privacy, and less than one in five were unconcerned about privacy in general. All of which indicates that the participants perceived that SOSTs could potentially be intrusive in violating the privacy of themselves and others.

The results in figure 13 shines light on how different factors influence the participants' perception of SOSTs by showing what aspects of the use of SOSTs that they are concerned about. Here the common concern relates to being disempowered in controlling the data collection and subsequent use. What concerned the participants the most was that information about them was shared beyond their control. Painting a picture that is further enhanced by the discussions at the tables, were a very common message was the concern about who collects the data about them and what it is used for, as well as who gets access to it. In these discussions the participants voiced a concern, that to them all of this was opaque and that they felt substantially disenfranchised in terms of controlling their own data.

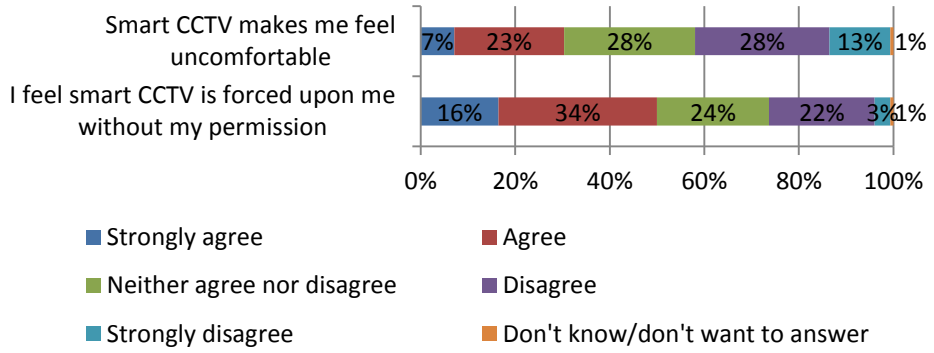


Figure 17: Sense of smart CCTV intrusiveness

Turning to the perception of the two specific SOSTs, the participants were split fairly evenly, when asked whether they considered smart CCTV to be intrusive (see figure 21 below), less than a third of the participants voted that smart CCTV made them uncomfortable, while 41% disagreed. While this shows a majority being comfortable with the implementation of smart CCTV, it also show that a not inconsiderable amount found that smart CCTV made them uncomfortable and that almost half the participants found it intrusive. Sense of disempowerment in terms of controlling data collection and usage indicated above, is to a degree confirmed in that 50% felt that smart CCTV was forced upon them without their permission, indicating that they felt disempowered. Considering the previously displayed results, what can be conferred from this, is that, while the participants were not necessarily against implementing smart CCTV, they would like to have more influence on where smart CCTVs are used as well as by whom. Which, to a

large extend, was confirmed in the discussion around the tables, where people were expressing a want for information and influence. This corresponds fine with the concerns raised in figure 11, which shows that a considerable majority of the participants worried that smart CCTV could both violate theirs and others' privacy, further indicating that this technology is not uncontroversial in the eyes of the participants.

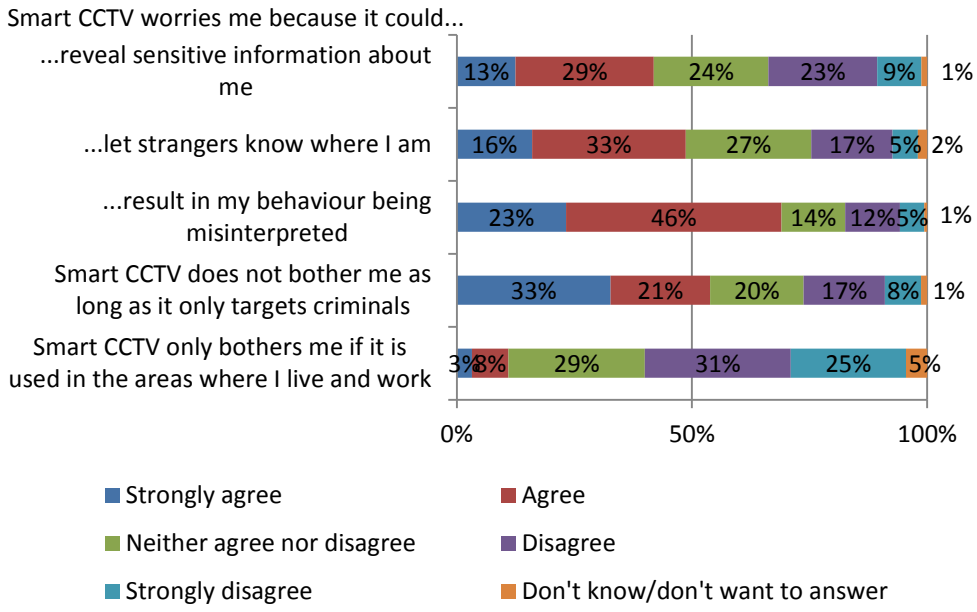


Figure 18: Factors of smart CCTV that worried participants

Figure 18 shows pretty clearly that what the participants worried the most about when it comes to smart CCTV was that their behaviour might be misinterpreted. This was also mirrored in the discussions where several persons noted how the video displayed at the summit showed how a smart CCTV system misinterpreted four people walking in a group as a car. This also displays that, the participants agreed that it might be an appropriate means for ensuring national security but the technology is not currently at a stage where they trust the conclusions made by it. The result in figure 18 very well supports what was discussed above, that the participants to some extent feel disempowered and unable to control who collects information about them and what it is used for. As we can see, considerable majorities worried about smart CCTV revealing sensitive information, revealed their whereabouts to strangers and that the information was misinterpreted. It is also evident here, that the spatial context of the application of smart CCTV matters less to the participants.

It is very interesting to note that, despite their exhibited concern for others' rights in figure 10 and 11, a majority voted that smart CCTV did not bother them as long as it was targeted at criminals, which in a sense is the same as saying, as long as it doesn't target me, but a not well defined group. One participant in his 50s, expressed concern about this poll result. To him, it was not clear where the line were drawn in what constitutes a criminal. This was resonated at other tables where a threshold for triviality in terms of what degree of severity of a crime would allow such SOST material to be used.

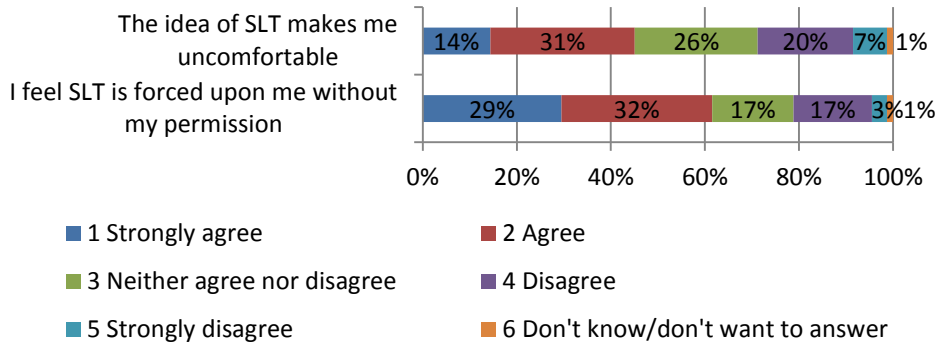


Figure 19: Sense of intrusiveness

Also when considering whether they perceived SLT to be intrusive, the participants were split pretty evenly, with 47% agreeing and 53% disagreeing (see figure 22 below), but unlike in the case of smart CCTV, the largest proportion of participants felt that the thought of SLT made them uncomfortable, though there was still a sizable amount of them disagreeing. And more than 60% felt that SLT is forced upon them without their permission, which is also considerably higher than was the case for smart CCTV, where the corresponding proportion was 50%. This suggests a trend, that SLT is more controversial than smart CCTV. This is also confirmed by fewer agreeing that SLT made them feel safer, than was the case for smart CCTV. As with smart CCTV, this indicates a perception of disempowerment and feeling of powerlessness, going hand in hand with the results from figure 10 and 12, that the vast majority of the participants worried that SOSTs and SLT could violate their rights and privacy.

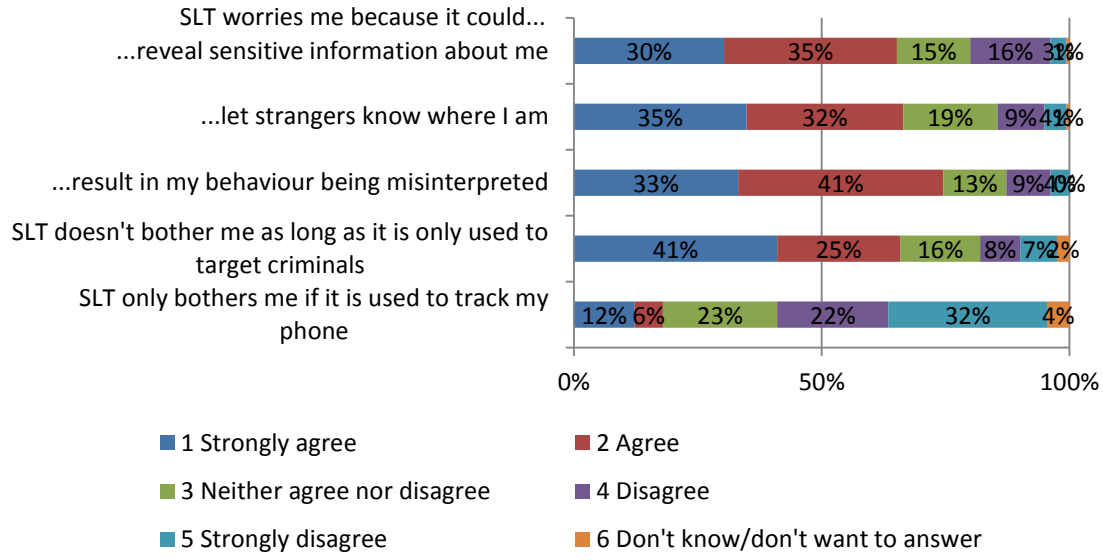


Figure 20: Factors relating to SLT that worried participants

In figure 20, it is evident that the vast majority of participants were concerned with the intrusiveness of SLT. As with smart CCTV, they were most worried that the data gathered about them could be misinterpreted, showing again a certain degree of mistrust in this technology. This held together with the participants generally being concerned that their personal data could be used against them, as well as them not feeling safer thanks to SLT indicates that it is considered, when analyzed all round, fairly intrusive, at least more intrusive than smart CCTV, and further less effective than smart CCTV. In terms of the factors in figure 18 and 20, the participants were also considerably more worried about SLT than smart CCTV. In

both cases the major concern seems to be misinterpretation and other system failures. Generally concerns about system failure were widespread among the participants, and another widespread concern was the perception of reverse production of evidence that many feared could develop out of indiscriminate mass surveillance, which made many participants emphasize that they were already actively aware that their smartphone activity could be monitored which lead many of them to exercise behavioral self-censorship.

It is very interesting, that the participants generally did not mind SLT as long as it was only targeted at criminals, even more so, than was the case for smart CCTV. This is very interesting, taking the comment above about what constitutes a criminal, in consideration and their general concern for others. This concern was repeated again in figure 20, with the vast majority of participants disagreeing that SLT only bothered them as long as it was tracking their own phone. It seems that the concern about others' privacy and rights, are only valid as long as they are not criminal.

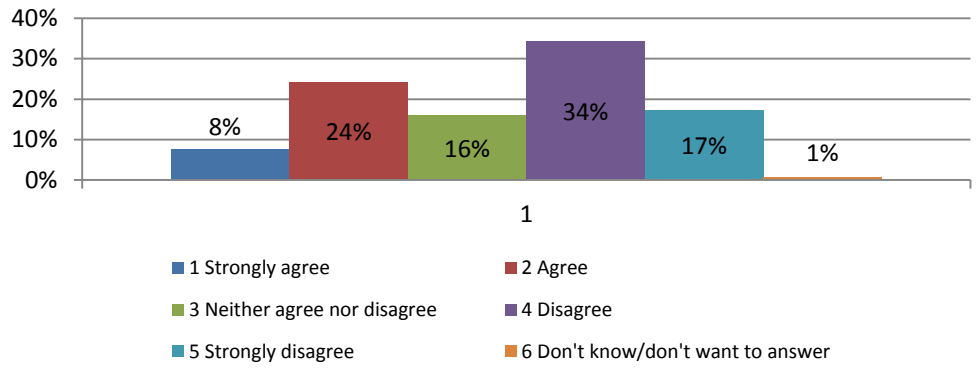


Figure 21: If you have nothing to hide, you do not have to worry about SOSTs

It becomes even more puzzling, when taking the results in figure 21 into consideration. Here the participants generally voted the exact opposite of the last poll in figure 20, but relating to SOSTs in general. Though they were split in fairly large groups, it paints a very different picture than the aforementioned poll, with over 51% disagreeing that if you have nothing to hide you do not need to worry, which does not correspond very well with the vote on SLT being just fine if only targeted at criminals.

Avoidance and resistance against surveillance

Before turning to whether the participants considered that the benefits outweigh the drawbacks, it will first be examined whether they would actively avoid or challenge the use of the two specific SOSTs.

An important aspect to understand the participants' willingness to challenge and avoid smart CCTV is the question of how often they notice them in the area around their homes.[101] The survey shows that most participants were generally not very aware of CCTVs in their daily lives. 14% noticed them often, whereas only 5% noticed them all of the time. 24% never saw them, 37% rarely and 20% sometimes saw them, which suggest that the participants have become fairly habituated to the presence of CCTV cameras, to a degree where they don't notice them anymore, or that they genuinely don't feel or notice their presence.

[101] Please note figure 2: area of residence, in which it can be noted that one third estimated that they lived in a rural area, whereas the rest either resided in urban or metropolitan surroundings.

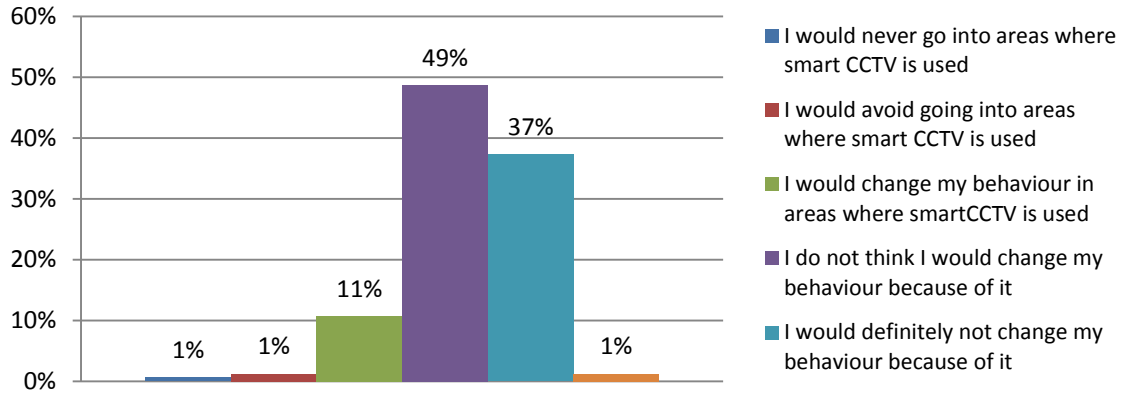


Figure 22: Active avoidance of CCTV

In figure 22 we can see the participants do not perceive smart CCTV as anything that would influence their behavior. Only 1% would never go into areas with smart CCTV, while another 1% would actively seek to avoid it. 11% would change their behavior in areas where smart CCTVs are in operation, but 86% would not let change behavior on account of smart CCTV, which indicates that despite worrying about different aspects, particular the sharing of data about them beyond their control and worrying about their own and others' human rights, they still would not let it influence their behavior.

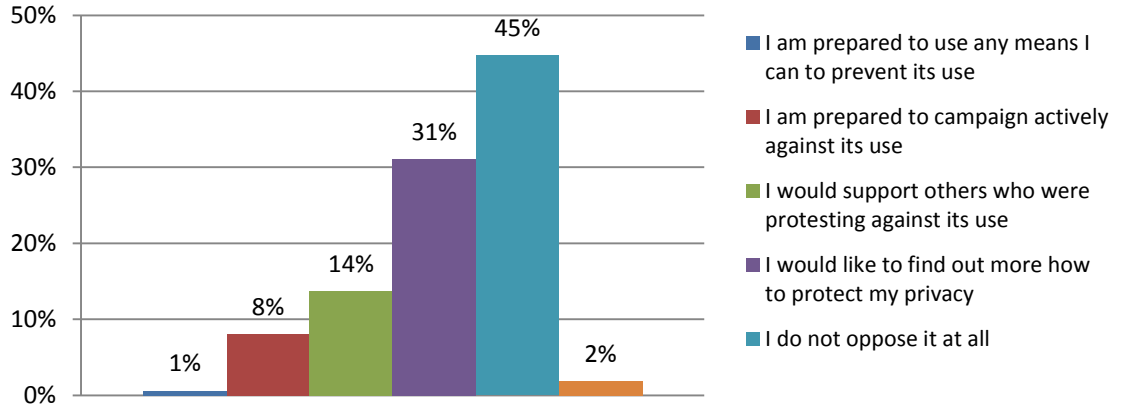


Figure 23: Willingness to challenge smart CCTV

In figure 23 we can further see that very few were actually willing to actively prevent its use or campaign against it. Even support for those campaigning against it was not very large. 45% did not oppose smart CCTV at all, and the second largest portion of 37%, would like more information about how to protect their privacy.

As shown earlier on, the participants were generally familiar with SLT, and when looking at the survey results, it is clear that most used their phones frequently, with 43% responding they used it often and another 43% responding 'all the time'. Only 3% used it rarely, and 11% sometimes.

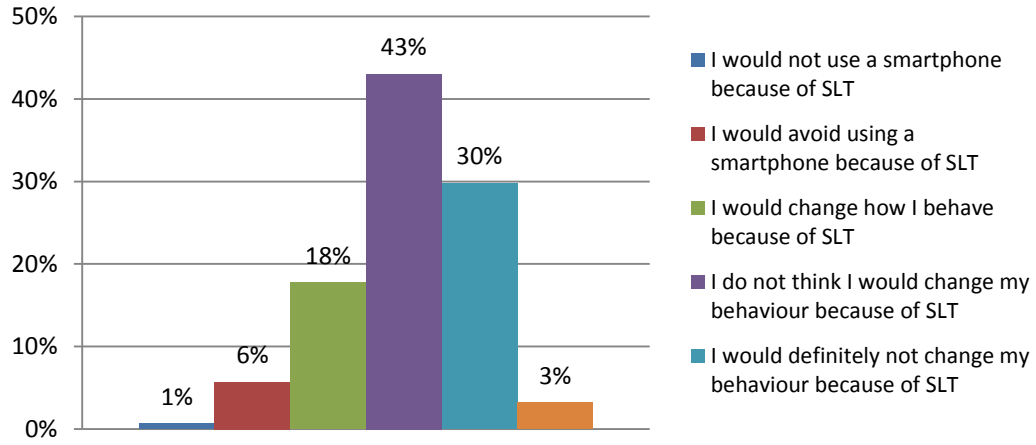


Figure 24: Active avoidance of SLT

The picture in figure 24 is fairly clear: while very few would either not used or avoid using a smartphone because of SLT, 18% would change their behavior. But as with smart CCTV, the vast majority either probably or definitely would not change their behavior because of SLT. As with smart CCTV, this indicates that they do worry about a number aspects concerning SLT, but it is not enough to make the majority change their behavior.

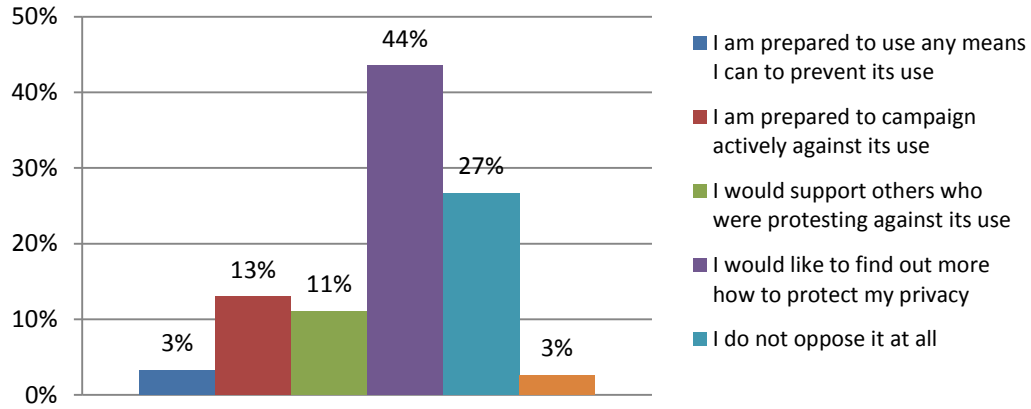


Figure 25: Willingness to challenge SLT

The picture in figure 25 is fairly similar to that in 23, but differs in one important aspect. As with smart CCTV, very few were willing to use any means to prevent the use of SLT, roughly on in eight were prepared to campaign actively against SLT, while 11% would support those who did. These numbers indicate that more participants were willing to actually do something to hinder the use of SLT than smart CCTV. But very interesting, almost half the participants would prefer to have more information about how they could protect their privacy. Compared to smart CCTV, the amount not opposing SLT at all is significantly smaller, though still substantial, which furthers the previous indications that SLT was considered to be substantially more controversial than smart CCTV.

Trade-off

Now that the participants' reflections and perceptions of the effectiveness and intrusiveness of SOSTs in general and smart CCTV and SLT in particular have been analyzed, the question remains, whether they would be willing to accept the SOSTs' level of intrusiveness given the benefits that they offer.

Usefulness	Intrusiveness: Low	Intrusiveness: High
Low	1%	6%
High	50%	41%

Usefulness	Intrusiveness: Low	Intrusiveness: High
Low	1%	8%
High	41%	47%

Figure 26: Intrusiveness vs. usefulness of smart CCTV and SLT, respectively

As evidenced in table 1 and 2, there is little discordance as to the usefulness of the two SOSTs in question. Only 7% question the usefulness of smart CCTV, whereas the same goes for 9% in the case of SLT. But in terms of intrusiveness the participants were divided in both cases. 51% did not consider smart CCTV to be intrusive, while 47% did. The reverse is true for SLT, where 42% did not find it intrusive and 55% found it to be intrusive. This makes the picture a bit clearer still.

While the participants may not change their behaviour on account of the SOSTs and they overall consider them to be useful, they are considerably more divided when considering the intrusiveness.

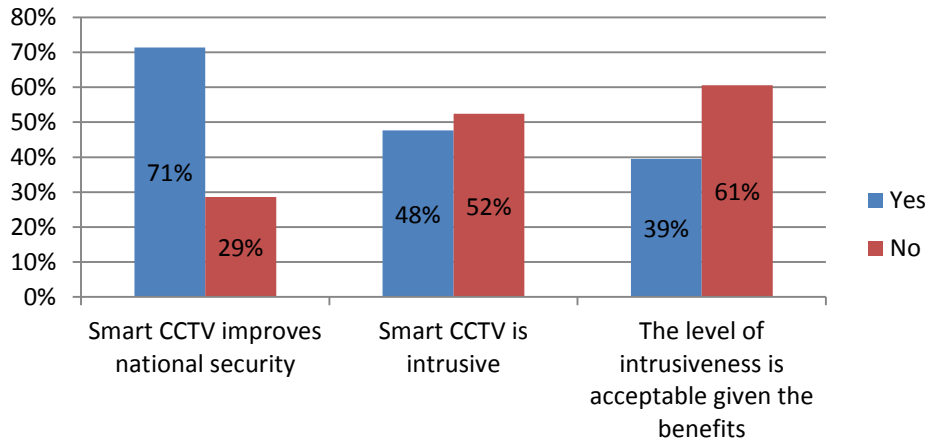


Figure 27: Effectiveness, intrusiveness and the trade-off of smart CCTV

This is clarified in figure 26 which consists of the results from three direct yes/no questions, where the participants were asked directly about usefulness, intrusiveness and whether they would accept the trade-off of privacy for security when it comes to the application of smart CCTV. Even though it is considered to improve national security by 71% of the participants, and 91% consider it useful in general, they are divided in terms of the intrusiveness. Despite its almost unequivocally perceived effectiveness and division to intrusiveness, a significant majority of the participants found that the intrusiveness of smart CCTVs does not make it a means justified by its ends.

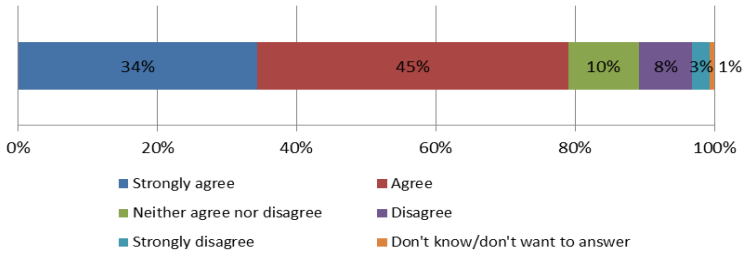


Figure 28: Support for using smart CCTV

As the last question specifically concerning smart CCTV, the participants were asked to consider whether they supported the adoption of smart CCTV as a national security measure. The result from that poll is fairly clear: the participants were generally in favour of smart CCTV used for national security purposes. This

indicates that they are willing to accept smart CCTV as a solution to ensure national security, provided that this is done with more openness than has been done so far. This will be further addressed in the recommendations given by the participants. In the discussions many were highlighting the positive aspects of CCTV cameras, e.g. in surveilling parking lots or other desolate areas in order to deter criminal behaviour, as well as its investigatory qualities in helping solving crimes. This result is still puzzling, though, considering the majority not agreeing that the intrusiveness is acceptable given the benefits of smart CCTV.

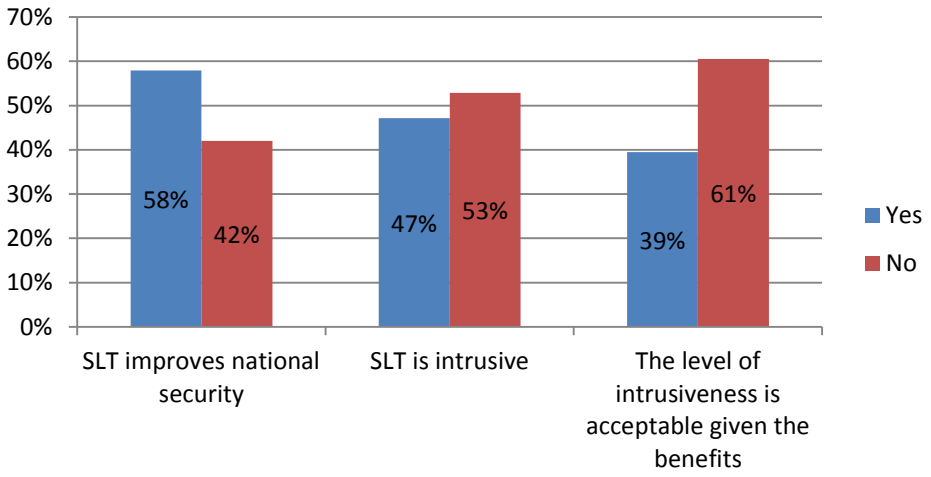
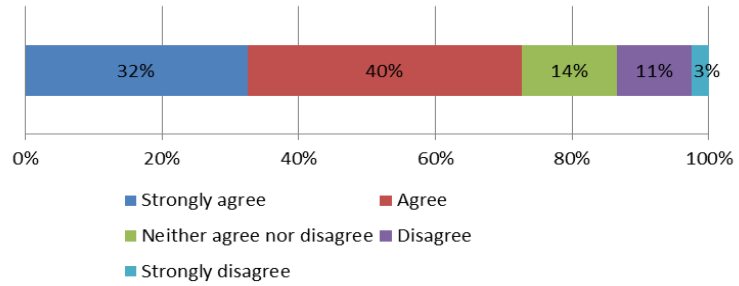


Figure 29: Effectiveness, intrusiveness and the trade-off of SLT

When considering SLT, more than half the participants believed that SLT could improve national security and 88% found it useful in general. This is less than for smart CCTV, but still a majority finding it useful. Again, the participants were split pretty evenly when asked directly if they found SLT to be intrusive, with a small majority not finding it intrusive. Despite this, a significant majority found that the level of intrusiveness was not justified by the benefits that SLT provides.



Just as with smart CCTV, the last question asked specifically about SLT, concerned whether the participants would support the adoption of SLT as a national security measure. Interestingly, a majority of 72% were in favour of this.

Figure 30: Support for using SLT

This indicates, like the case was for smart CCTV, that the participants as such, are not necessarily against the usage of the SOSTs in question, but they have reservations as to how this is done. This was particularly evident at several tables where people highlighted the benefits and conveniences provided by SLT, for instance the ability to locate elderly and demented people, people who get lost in the wilderness, down to everyday practicalities of locating your own phone if lost, but still less than 25% answered that they felt more secure thanks to SLT.

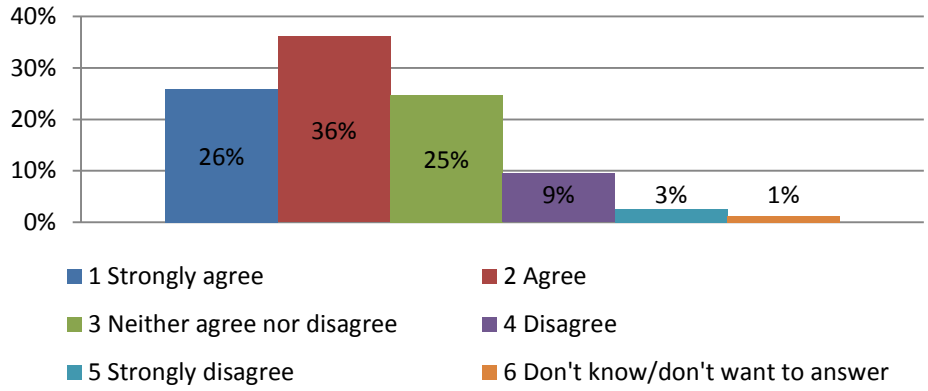


Figure 31: Alternative approaches to security, which do not involve SOSTs, should be given higher priority

But even though most supported the implementation of these SOSTs and considered them both appropriate and efficient, they also highlighted the need to focus on alternatives. When asked, 62% agreed that alternatives to SOSTs should be given higher priority. It was clear at the tables, that many considered that the SOSTs were indeed useful and appropriate means of ensuring national security, but that technological solutions could not stand alone. They need to be supplemented by measures that address social issues, education, segmentation etc. Very much in line with this, the vast majority was worried how both smart CCTV and SLT could develop in the future, which would underline the need to prioritize alternatives higher. Over half the participants strongly agreed that they worried how SLT could develop in the future and 28% agreed. The numbers were lower for smart CCTV, but showed the same trend. 72% either strongly agreed or agreed that they worried how it could develop in the future. This could be a sign of the participants fearing disenfranchisement and undisclosed implementation of these SOSTs. Many of the concerns regarding SOSTs, voiced in the discussions concerned the opaque nature of how SOSTs so far have been implemented. Many were ready to accept them provided that more information was disclosed concerning who was utilizing what SOSTs and why. Most did not need to have a case by case description of implementation, but just disclosure of what intelligence services it was available to and under what circumstances. In relation to this, one of the primary concerns voiced by the citizens, were that they felt unsure what exactly constituted suspicious behaviour. One participant gave the example of refraining from using an internet service while vacating in the U.S. because the password for her account was 'Kabul'. The participants were aware that the intelligence services would and/or could not disclose all information as to what would prompt them to initiate an investigation, but they would still like to have some guidelines under which they could feel relatively certain that they would not come under investigation.

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

As mentioned above, the Danish population generally have a high degree of trust in their public institutions and intelligence services. And as can be seen below, the participants generally had confidence in security agencies utilizing both smart CCTV and SLT.

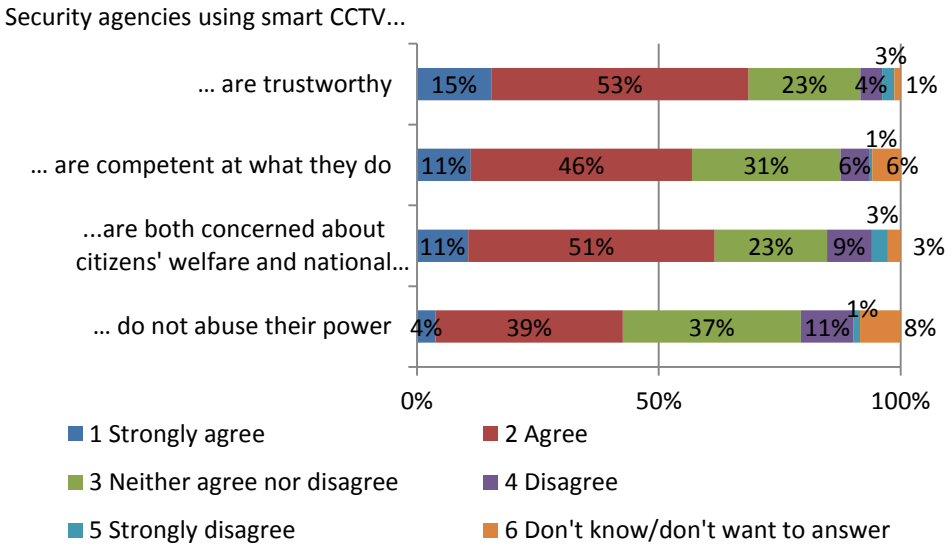


Figure 32: Trust in security agencies using smart CCTV

It is evident from figure 32, that the security agencies employing smart CCTV is considered uncontroversial by a majority of the participants. Most considered them to be both trustworthy and competent, concerned with both the welfare of citizens and national security. Though the largest proportion of the participants agreed that these security agencies do not abuse their power, a fairly large portion of 37% neither agreed nor disagreed. This could be because people are not familiar with the modus operandi of the security agencies, because people rarely consider this or because they are simply indifferent or unsure how to assess this. But generally it seemed that the security agencies were largely uncontroversial to most participants, only between 7-12% disagreed with any of the statements regarding smart CCTV.

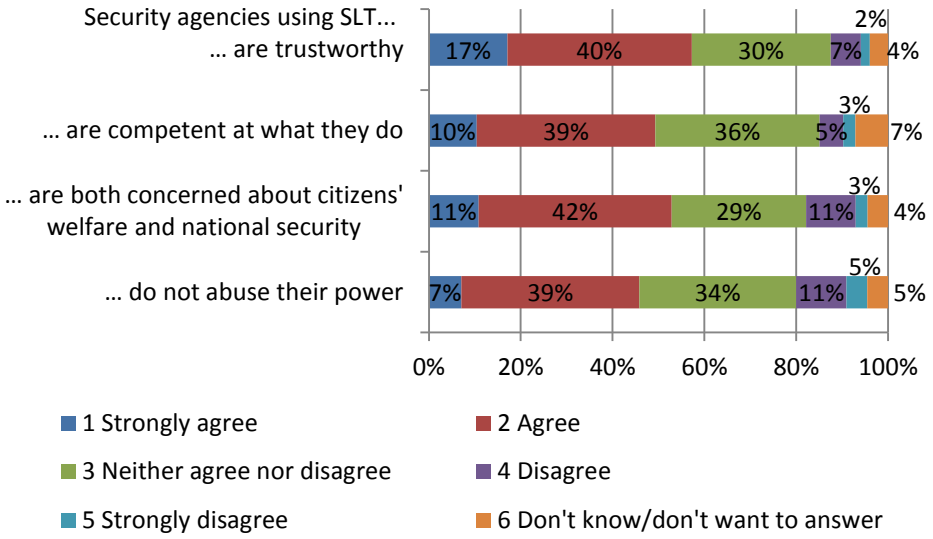


Figure 33: Trust in security agencies using SLT

The same goes for security agencies deploying SLT. While the largest proportions in each question agreed that the security services utilizing SLT were trustworthy, competent, not just concerned with national security but also citizens' welfare and not abusing their power. Surprisingly large proportions, though, neither agreed nor disagreed, but still only few disagreed with these statements. This indicates, as would by and large be expected, that most participants found the working of the Danish security services employing these SOSTs to be fairly uncontroversial, even though they still perceived the SOSTs themselves to be a bit more controversial. These results, to some extent, explain why the citizens are so accepting of SOSTs. Had the trust in the security agencies been significantly lower, it is very probable that the acceptance levels for both SOSTs would also have been significantly lower.

The trust in the security agencies must be expected to be predicated on the participants having faith in the laws and security mechanisms insuring against abuse. But the survey showed that the participants, when asked whether they considered that the laws and regulations in place ensured against misuse, only 35% answered 'yes' for smart CCTV and 31% for SLT. So while the participants generally trusted the security services deploying these SOSTs, they also did not have much faith in the legal framework put in place to protect them. This is likely due to the disclosures over the past years, from Edward Snowden on an international level, and in relation to the NETS-scandal[102] and the hacking of the Danish company, CSC, a described above. The survey further showed that 48% either strongly agreed or agreed that once in place, SOSTs are likely to be abused. While one in four disagreed and 26% did neither agree nor disagree, this shows that some of the trust in the legal framework and security mechanisms is lacking. It is arguably, problematic that the majority of the participants found that regulations and legislation is insufficient to protect against the misuse of SOSTs, and that almost half find it likely that SOSTs will be abused. As one woman in her 50s expressed during the summit: "We have trust for now, but they [the security agencies, ed.] must also make themselves deserving of our trust."

4.4 We trust you, but…

From the above analysis, it is clear that the implementation of SOSTs was generally not a trivial matter to the participants in the Danish citizen summit.

While a majority generally felt safe, in Denmark and in their daily life, a considerable majority supported the routine implementation of SOSTs, and smart CCTV cameras and SLT in particular. Both of the latter were considered to be useful and efficient in ensuring national security, though also intrusive to many. The

[102] NETS is a major Nordic provider of payments, credit card and financial infrastructures. A computer consultant sold information to tabloid newspapers about financial transactions done by celebrities.

participants were found to worry more about violation of others' rights, than their own. This might be because of the frequently stated "I'm too insignificant for anyone to pay attention to"-perception, which could indicate that they did not consider themselves to be subject to these sorts of surveillance, and thus did not need to worry. This could be further supported by the majority not agreeing with the 'nothing to hide, nothing to fear'-statement which is often heard when legitimizing indiscriminate surveillance. Overall this could indicate that the participants did consider surveillance more a society-wide problem than a personal one, which would explain why they are more concerned with the rights violations of others. Though the participants generally supported the implementation of these SOSTs, they also had a range of reservations towards them. They would generally like more information about what is used by whom and why, as well as under what conditions this utilization is allowed. Many also found the indiscriminate nature and intrusiveness of the SOSTs problematic. They were concerned that the burden of evidence would be reversed, because everyone is subject to surveillance and thus indirectly under suspicion. One man pushed the situation to its extreme by rhetorically asking: "Should we shoot ten people because we know one of them is the killer?" Others worried about function creep, e.g. that social services started getting access to this information and started using SOSTs based data against citizens in cases of suspected fraud. They wanted guidelines for a triviality limit for what the data could be used for. In short, they wanted more information about who collected information, why and for what ends. At one table, for instance, it was pointed out that they knew that something is being done, not exactly what. It was emphasized that this sort of secrecy risks breeding both myths and insecurity, and that "peace of mind is caused by knowledge about the process and the technology." When not being informed, the participants felt that they were being disempowered which led to frustration among some. Some felt powerless because of this, "if you would want to stop this sort of surveillance, what could you even do?"

Many of the participants were well aware of the curiosity of almost everyone being deeply concerned about the SOSTs but still they almost all endorsed its usage. One very important point, related to this, is that while most were worried about SOSTs, the discussions at the tables showed that the surveillance techniques used by private corporations generally were much higher cause for worry, than those used by security agencies and public institutions.

When comparing the results of smart CCTV and SLT, it is particularly interesting that the participants found SLT to be far more controversial than smart CCTV in most aspects, but when it came to their implementation, they were almost equally accepted. This may be caused by three factors. For one the participants have been habituated to CCTV for many years and have gotten so used to them that they don't notice or see them in their daily lives. SLT on the other hand, is a never concept which means that the newness factor might play a role. Many would prior to the meeting probably have been fairly unacquainted with SLT. This is somewhat substantiated with more people agreeing or strongly agreeing that they understand what smart CCTV is than what SLT is. Secondly, and probably equally important, there is a question of spatial proximity. Whereas CCTVs are spatially delimited in that they are perched on walls and in this sense immovable, smartphones necessarily follow the individual because he or she would necessarily be carrying it. This creates a sense of being followed and monitored much more closely, than with mounted CCTVs, even though succession of them might monitor you. Finally, it was evident in the discussion, that when discussing smart CCTV, many confused this with regular CCTV, which they would be far more willing to accept, given that CCTV only records but does not analyse, register or prompt security personnel. Thus, for smart CCTV and SLT it applies that they are equally accepted, but neither are uncontroversial.

4.5 Citizens' recommendations to policy makers

The recommendations from the participants at the tables can be divided into three categories, which are to some extent interrelated: empowerment through education and information, 'Surveillance ombudsman', and transparent legislation.

Many participants agreed that government and public use of SOSTs could be justified. Though many worried about government surveillance, what seemed to be much more concerning to most, was the surveillance techniques used by private corporations. It was emphasized, that surveillance must not be implemented as a trade-off with privacy; the participants generally wanted it both ways, and did not consider increases in one to necessarily be on account of the other. In line with this, they generally argued that alternative solutions should be fostered and prioritized. One frequent example was the use of

Natteravnene, an organization of volunteer adults present in areas with nightlife, in order to help young people and prevent conflicts, crime and vandalism. Many felt that this approach, based on social work and dialogue, which has been proven preventive, is a good way of addressing issues in the nightlife. Many of the written recommendations suggested non-technological solutions and emphasized focus on social action instead.

Empowerment through education and information about how intelligence services and law enforcement agencies use SOSTs is key in fostering the trust in them. This was a resounding point made by all the tables. For one thing the participants wanted to have greater insight into which SOSTs are being used by public institutions and security agencies. Further they want to know for what purpose and under what circumstances their use is allowed. Particularly the last point was emphasized heavily. But most importantly they wanted to know who collects their data and who is given access to it. In essence, transparency of the application of SOSTs was essential. One of the things that made the participants feel the most disenfranchised and disempowered were the inability to find out who is collecting data about them, what data is being collected, how it is collected, and what this is being used for. They wanted to be given a right to view the data that is stored about them, and if the data is misleading, they want the ability to apply for having it corrected. Further they want to know how long the data is stored for, and possibly have an obsolescence time, by which the data is destroyed. So this generally concerns information availability; but the participants did not just want information to be made available, they would also like for it to be actively disseminated. This should be done through primary school education from when kids are old enough to have smartphones, so they from the beginning are made aware of the consequences that their actions have, and that the internet is not a separate sphere, in which their actions have no bearing in 'reality'. Many emphasized that kids were not aware that what they put on the internet is never going to disappear and could potentially come back to haunt them in their later life, and that the information they give away for free, is being used to make money off. Supporting these primary school efforts should be informational campaigns targeted at the wider public in general, so that information is disseminated as widely as possible. In essence, for the participants it was important to empower the citizens through information dissemination so people could make informed decisions about their internet and phone activity as well as being informed about when and why they are being monitored.

Another recurring theme between the tables was the demand for a legitimate body monitoring and handling complaints about the use of SOSTs, what was repeatedly called a 'surveillance ombudsman'. This sort of body was variously conceived of as being domestic in scope, founded at the EU level or as an organ within the UN. One aspect that was important to many, though, was that it was accountable to the public it sought to serve, for this reason one participant suggested that this entity should be comprised of politicians from the entire political spectre of the parliament so there would be both parliamentary control and political representation of the public. While some emphasized the necessity of immediate input legitimacy, that is electoral legitimacy, others pointed to the fact that data is inherently international, and for that reason a Danish entity without any transnational cooperation or anchoring would essentially be powerless in anything but controlling the Danish intelligence services and security agencies. This was their reason for emphasizing the need for international organs. They were also adamant that it should not become stuck in international diplomatic deadlock. As to what should be considered by this ombudsman, there was also some discrepancy. Some argued that it should look into individual apps for smartphones, computer programs etc., others that it should be concerned with citizen complaints, others again that it should concern itself with fundamentally important cases of principle. This recommendation is also founded in the participants wanting to empower the citizens through the option of complaining about abuse and unwarranted data collection as well as an option of correcting misrepresenting data.

Connected with the first category, is the need to have transparent legislation that is, in the words of one group, "that is transparent to the citizens". One concern regarding the existing legal framework addressing privacy and use of SOSTs is that it is widely incomprehensible to most ordinary citizens, very well exemplified by the concept of agreeing to 'terms & conditions'. While most modern citizens agree to these several times a month, almost none actually have any idea what exactly is being agreed to, which was also highlighted by one participant, who pointed out that most of the collection of data and registration conducted by private actors, is in reality something that people have unwittingly agreed to by agreeing to incomprehensible and purposefully extensive terms and conditions. Generally, the laws determining what is allowed for both public security agencies and private corporations collecting data are simply too difficult

for most people to read and understand, and they are consequently disempowered by not knowing their rights and the rights of others. So several tables called for clearer legislations, setting forth exactly what is allowed for both public bodies and security agencies as well as for private corporations. Further, the participants wanted the applicable laws and regulations to keep better up with the reality of technological development, than is currently the case. Whether this regulation should be international or domestic in scope was subject to some discordance. Again, some pointed to the inherent international nature of data necessitating international governing bodies, while others highlighted the inertia of international law making and the risk of such legislation being watered down. But enforcement was highlighted as very important. The legislation should be anchored in sanctions for violation and they should further serve as guarantees for non-violation of their citizen's rights. Another aspect that the participants were very insistent on, was disallowing by law, functionally irrelevant tracking, registration and data collection in smartphone apps, so the apps that are installed do not collect and sell data that is not necessary for its functioning. In general the selling of data collected to third parties was, as could be seen in the survey, one of the things that worried the participants the most, and thus also one of the recommendations that they were most adamant about. In all the discussions, there was wide agreement that selling data to third parties was, if not morally questionable, then at least controversial, and most people wanted legislation against this. The participants also, as a minimum, wanted an opt-out option so they could chose not to be registered, and many highlighted the benefits of letting this sort of registration be conducted on an opt-in basis, rather than opt-out, so it would always be a matter of a conscious choice. This was mostly directed at the private companies' gathering data about them, rather than the security agencies' data collection. As a final point in this regard, the participants would like to implement a right for the individual to know what is registered about him or her. Both by public security agencies and by private corporations; so that the individual can become aware of what is collected by whom and if they are willing to accept the collection conducted by the private actors and whether the information gathered by public bodies and security agencies is correct and not misrepresentative.

In conclusion, the recommendations from the participants can be summed up in a sentence: they want empowerment of the citizens through transparent legislation, an accountable, legitimate controlling body and education and information dissemination.

5 Summary and Conclusions

Denmark is a country with extensive surveillance, and the surveillance is broadly accepted in the public debate. Among other things, the surveillance in Denmark consist of CCTV surveillance, a comprehensive civil registration system, a pervasive registration of data and telephone communication and increasingly use of biometrically technologies. These are the most debated technologies in the media and the public debate. But, roughly speaking, discussions about surveillance and threats of infringements of privacy are not something which occupies the Danes in their daily lives. The "Big brother" society is not as big a fear as it was earlier, because they have, to some degree, become habituated to these new SOSTs. Further reasons can be found in the country's historical background. Danes have a high degree of social trust and a long history of registration of citizens. The registration system is perceived as a crucial part of the Danes everyday life and is an essential part of the efficient welfare state. In 2010 the civil registration system correlated with NemID, and more services was integrated into one system. The design of the system is sometimes being criticised, but the criticism is rarely about its raison d'etre. In the course of the past decade, domestic and global developments of terror and diplomatic crises, has seen Denmark's situation change with and within a new world order of new types of threat. Faced with changes in type and level of threat, the level of surveillance and registration of citizens has been increased, through the implementation of a number of anti-terror legislations enhancing the authority of the Danish intelligence services, without these developments inciting extensive public debate.

The preceding pages paint a fairly consistent picture of the participants at the Danish SurPRISE citizen summit's attitudes towards security and SOSTs. The vast majority of the participants were willing to accept the routine implementation of SOSTs; even more so after than before the meeting, this, despite them almost uniformly felt both safe in their everyday life and in Denmark as a country. Further, the two SOSTs being scrutinized in depth at the summit, smart CCTV and smartphone location tracking (SLT) were found to be both appropriate and effective means of ensuring national security. Even though both were perceived to be intrusive, and that the majority of participants were not willing to accept the intrusiveness on account of the benefits that the SOSTs provided, a majority were still willing to accept the implementation of both by security agencies in order to ensure national security. Further, very few were willing to actively challenge or avoid using a smartphone because of SLT or going into areas with smart CCTV in operation, but many would like to have more information pertaining to how they could protect their privacy.

This is not to say that the implementation of SOSTs was considered a trivial matter to the participants. Quite on the contrary, the participants did voice a fair few concerns in the course of the summit and the results from the survey also show that many, if not most, had considerable concerns. Overall, the majority were concerned about the influence of SOSTs on theirs and others' privacy and human rights. Of major concern, was the, for the participants, unanswered question of who was collecting personal information about them. Many expressed uneasiness with not knowing who collected the information, what sort of information was being collected, as well as what it was for and who it would be made available to. In connection to this, they were worried that the indiscriminate nature of SOSTs meant that too much information was being gathered about them and that they were unable to control what was being collected and who received it. Generally speaking, the majority did not oppose the application of SOSTs by national security agencies. The security services employing both SOSTs were considered both trustworthy, competent, considered with citizens' welfare and not abusing their power. From the notes of the table discussion, it is evident that what worried them more was the massive registration and collection of data, undertaken by private actors. They felt that the legislations on the subject is opaque to the regular citizen, who is in this sense disempowered from making informed decisions, because they are highly unlikely to read, and even less, to understand the 'Terms and conditions' that they agree to. In the table discussions, the participants also expressed worries about function creep, that is, information and information collecting initially gathered for one purpose being used for another. In general, they felt that the secrecy with which SOSTs are currently being employed breeds unnecessary fear and helps create myths, and consequently disempowerment of the citizens. The participants were also very aware of the seeming incongruence between being fundamentally very worried about the usage of SOSTs but at the same time generally supporting the implementation of SOSTs by security agencies for national security purposes. The results from the survey also showed that a considerable majority wanted alternative approaches to

security, not involving SOSTs, to receive higher priority, and, in line with this, that they feared how both SLT and smart CCTV could develop in the future.

When comparing the survey results concerning the two SOSTs being treated in depth at the summit, it is interesting to note, that while they are both considered comparatively efficient and capable of ensuring national security, SLT was generally perceived as far more controversial by the participants. On almost all factors, SLT had more people 'agree' or 'strongly agree' that they worried than was the case for smart CCTV. Keeping this in mind, it is very interesting that the support from the participants for the implementation of these two SOSTs by security agencies, was very similar.

The recommendations to policy makers, given by the participants at the summit, were characterized by the participants generally not minding that national security agencies employed SOSTs, as long as this did not result in trade-off between security and privacy. In line with that, non-technological alternatives to security should be emphasized and prioritized higher, with social efforts being mentioned frequently. The recommendations can generally be put in the three categories: empowerment through information and education, surveillance ombudsman, and transparent legislation. The participants wanted information about who is using what sort of SOST to monitor and register the citizens, why and who is given access to this data, and under what circumstances it is allowed to employ what, and how long the data is stored. This should be disseminated in an efficient manner through primary school education and public information campaigns across multiple media. In this way, they wanted to empower the citizen to make informed decisions regarding their general actions. Another step in empowering the citizens that the participants sought was the establishment of a 'surveillance ombudsman', that could represent the citizens' interests and to which it should be possible to file complaints about violation of rights and abusive surveillance. The scope of the ombudsman varied between tables, with some wanting one domestic in character, while others suggested EU-level and others again a UN organ. Lastly the participants were demanding transparent legislation that keeps up with the technological development, and which is to make plain and obvious to citizens what the security services and what private companies are allowed to do, what technologies they can use, under what circumstances, for what and who would be targeted. Further the legislation should make clear what the data could be used for and who would be allowed to access it as well as information about storage time, preferably with an obsolescence clause prompting data to be destroyed after a certain time period. They further wanted clear information about what private corporations vis a vis governmental security services were allowed to, and what these corporations were doing. This also relates to the opaque nature of the terms and agreements that most will sign without reading or understanding. The legislation also is to disallow function creep, or at least make it more evident when an app or similar is function creeping. The legislation is to be anchored in enforceable sanctions and exist in mutuality with the surveillance ombudsman. Whether this should be on a national, pan-European or international level was not uniformly agreed upon.

Summing up, the participants were calling for empowerment of Danish citizens through information dissemination and education, a 'surveillance ombudsman' and an improved transparent legislation.

6 Bibliography

Andersen, N. T (2007): *Hej, husk fra i dag bliver alle dine sms'er registreret og lagret i et år*, in Information.dk - Politik & international, viewed the 4th of august 2012, <http://www.information.dk/146473>

Berlingske mener (2013): *Mit hjem er min borg*. In Berlingske Tidende. Viewed the 1st of October 2014. <http://www.b.dk/berlingske-mener/mit-hjem-er-min-borg#!>

Bjerregaard, Anne (2009): *Danskerne vil have tryghed gennem overvågning.* Viewed 20th October, 2014. <http://www.altinget.dk/transport/artikel/2009-3-3-danskerne-vil-have-tryghed-gennem-overvaagning>

Campell, J. and Hall, J (2006): *Introduction: The state of Denmark*, in Campel, Hall and Pedersen (eds.): *National Identity and Varieties of Capitalism*. Montreal: McGill University Press.

Danske Medier (2012): Danskernes brug af internettet. Danske Medier, København. Viewed 22nd October 2014. <fdim.dk/sites/default/mediearkiv/rapporter/danskernes_brug_af_internettet_2012_rapport.pdf>

Davidsen-Nielsen, H (2011): *Sikkerhedsfolk: Overvågning er for udbredt*, in Politiken.dk – Danmark, viewed the 5th of August 2012, <http://politiken.dk/indland/article1362271.ece>

Den Store Danske (2011): *IT- og Telestyrelsen*, viewed the 20th of September 2012, <http://www.denstoredanske.dk/Samfund,_jura_og_politik/Samfund/Ministerier,_styrelser,_udvalg_og_r%C3%A5d/IT-_og_Telestyrelsen>

Den tværministerielle arbejdsgruppe om terrorbekæmpelse (2005): *Det danske samfunds indsats og beredskab mod terror.* Statsministeriet.

Det Kriminalpræventive Råd (2005): *TV-overvågning – Fakta om TV-overvågning i Danmark*, viewed the 9th of August 2012, <http://www.dkr.dk/sites/default/files/dkr_mat_083.pdf>

Dinesen, Peter Thisted and Sønderskov, Kim Mannemar (2012): *Hvorfor stiger tilliden?*, *politica,* 44. årg. nr. 1 2012, 87-110. viewed the 16th of September, <http://pure.au.dk/portal/files/42042899/hvorfor_stiger_tilliden.pdf>

DR.dk (2011): *Is Big Brother watching you?*, Detektor, Danmarks Radio, viewed 24th of September, <http://www.dr.dk/P1/Detektor/Udsendelser/2011/09/28132144.htm>

Elkær, M. (2011): *IT- og Telestyrelsen trækker stikket ud og lukker*, Computerworld, viewed the 20th of September 2012, <http://www.computerworld.dk/art/198378/it-og-telestyrelsen-traekker-stikket-ud-og-lukker>

Fenger-Grøndahl, Malene (2008): Paragraf 114's usynlige konsekvenser. Information.dk, viewed 12th October 2014. <information.dk/176531>

Fenger-Grøndahl, Malene (2013): Den danske antiterrorlov. Faktalink.dk, marts 2013. Viewed on 10th October 2014. <http://www.faktalink.dk/titelliste/den-danske-antiterrorlov/hele-faktalinket-om-den-danske-antiterrorlov>

Forskningspolitikk (2012): Interview med direktør Lars Klüver: Teknologirådet nedlagt og genrejst som Fonden Teknologirådet, in Forskningspolitikk 3 – 2012, viewed on 15th October 2012, <http://www.fpol.no/Forskningspolitikk/Sider/default.aspx>

Friis, K. (2012): *Over 3 mio danskere nu på Facebook*, in b.dk, viewed the 24th of September, <http://www.b.dk/tech/over-3-mio-danskere-nu-paa-facebook#>

Fukuyama, Francis (2004): *State-Building – Governance and World Order In the Twenty-first Century.* London, Profile Books.

Iversen, Jes & Andersen, Steen (2008): *Co-operative liberalism: Denmark from 1857 to 2007.* In Fellman, Susanna et. Al: Creating Nordic Capitalism, the business history of a competitive periphery, Palgrave Macmillan, 2008.

Justitsministeriet (2003): *Endelig besvarelse af spørgsmål nr. 98 og 99 af 18. december 2003 fra Folketingets retsudvalg (Alm del. - bilag 300)*, viewed 21th of September, <http://webarkiv.ft.dk/img20031/udvbilag/lib3/20031_10383/20031_10383.pd>

Justitsministeriet (2006): *BEK nr 988 af 28/09/2006 (logningsbekendtgørelsen)*, in Retsinformation.dk, viewed on the 17th of august 2012, <https://www.retsinformation.dk/forms/R0710.aspx?id=2445>

Justitsministeriet (2011): *LOV nr 422 af 10/05/2011*, in Retsinformation.dk, viewed 24th of September 2012, <https://www.retsinformation.dk/forms/r0710.aspx?id=137097>

Justitsministeriets Forskningsenhed (2006): *Litteratur om effekten af tv-overvågning m.v.*, Justitsministeriet, viewed the 15th of August, <http://www.justitsministeriet.dk/fileadmin/downloads/Forskning_og_dokumentation/litteratur.pdf>

Justistitsministeriet and Datatilsynes (2008): *TV-overvågning*, viewed the 26th of September 2012, http://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Publikationer/Pjece_om_tv-overvaagning.pdf

Kamil, Carolina (2012): *Frihedsparagraf er hullet som en si.* In Berlingske tidende. viewed the 1st of October 2014. <http://www.b.dk/nationalt/frihedsparagraf-er-hullet-som-en-si#!>

Kildebogaard, J. (2012): *Hver fjerde voksne dansker har en iPhone*, in version2.dk, viewed the 24th of September, <http://www.version2.dk/artikel/hver-fjerde-voksne-dansker-har-en-iphone-45032>

Lauritsen, Peter (2011a): *Efter 9/11: Overvågning blev hverdag*. Radio program "Harddisken", Danmarks Radio, Viewed the 1th of August 2012, <http://www.dr.dk/harddisken/blog/2011/09/07/efter-911-overvagning-blev-hverdag/>

Lauritsen, Peter (2011b): *Big Brother 2.0*, Informations Forlag

Madsen, K (2013): *Danskerne er verdensmestre i tillids.* Viewed on 22nd August 2014. <politiken.dk/debat/debatindlaeg/ECE1893230/danskerne-er-verdensmestre-i-tillid/>

Mchangama, Jacob (2009): *Hvornår er prisen for terrorbekæmpelse for høj?* B.dk. viewed the 15 October, 2014. <www.b.dk/kommentarer/hvornaar-er-prisen-terrorbekaempelse-hoej#!>

Mortensen, H. and Valeur, E. (editors) (2009): *De overvågede*, Forbrugerrådet & DI Redaktion

Nemid.dk (2012): *Hvad er NemID?*, Viewed the 1th of september 2012, <https://www.nemid.nu/om_nemid/hvad_er_nemid/>

Norton-Taylor, Richard (2014): *UK military operations since cold war have cost £34bn, says study.* In theGuardian.com, viewed 21st October, 2014. <www.theguardian.com/world/2014/april/23/uk-military-operations-costs>

Pedersen, R. (2007): *Pris for nye logningsregler: 200 millioner kroner*, in Computorworld.dk, viewed the 26th of September 2012, <http://www.computerworld.dk/art/41594/pris-for-nye-logningsregler-200-millioner-kroner

Personregistrering.dk (2012): *Om personregistrering*, viewed the 8th of September 2012, <https://www.personregistrering.dk/index.php?id=80>

Price Persson, C. (2012): *Derfor er danskerne verdens mest tillidsfulde.* Viewed 22nd of august 2014. <videnskab.dk/kultur-samfund/derfor-er-danskerne-verdens-mest-tillidsfulde>

Ritzau (2014): *Fakta: Danske sager om terror.* Jyllands-posten.dk. viewed on 20th October 2014. <jyllands-posten.dk/indland/politiretsvaesen/ECE6802301/fakta-danske-sager-om-terror/>

Rådet For Større IT-Sikkerhed (2012): *Digisikker 2012*, Rådet For Større IT-Sikkerhed

SikkerhedsBranchen (2009): *ITV-Statistik 2009*, in sikkerhedsbranchen.dk, viewed 24th of September, <http://www.sikkerhedsbranchen.dk/index.asp?http://www.sikkerhedsbranchen.dk/artikler.asp?mode=vis_subpage&kategoriid=3&subpageid=287>

Stampe, C. (2010): *Politisk flertal for ændring af terrorlov,* in Information.dk – Politik & International, viewed the 26th of September, <http://www.information.dk/239804>

Privacy International (2011): *REPORT: Denmark*, viewed the 18th of September 2012, <https://www.privacyinternational.org/reports/denmark/ii-surveillance-policies>

Teknologirådet (2006): *D 5.3 Danish Report - Interview Meeting About Security Technologies and Privacy*, PRISE Security Resarch, viewed the 25th of September 2012, <http://www.prise.oeaw.ac.at/docs/PRISE_D5.3_Danish_Interview_meeting_report.pdf>

Teknologirådet (2010): *Biometri – brug af biometriske teknologier i det danske samfund*, viewed the 4th of September, <http://www.tekno.dk/pdf/projekter/p10_biometri/p10_Biometri_brug_af_biometriske_teknologier_i_det_danske_samfund.pdf>

The Danish government, Danish Regions, Local government (2011): *The Digital Path to Future Welfare – egovernment strategy 2011-2015*, viewed the 8th of September, <http://www.digst.dk/Home/Digitaliseringsstrategi/~/media/Digitaliseringsstrategi/Tilgaengelig_engelsk_strategi.ashx>

TNS Opinion & Social (2012): *Special Eurobarometer 390*

Cyber security, European Commission, viewed the 19th of September 2012, <http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf>

Togsverd, T. (2007): *Privacy og digital forvaltning*, ITEK, viewed the 21th of September 2012,

<http://di.dk/SiteCollectionDocuments/Downloadboks%20-%20lokale%20filer/Downlads%20lokale%20filer%2005-08/Privacyogdigitalforvaltning.pdf>

Version 2 (2014): *Tidslinje over CSC-hackersagen som set hos Version2*. viewd the 20th October 2014. <version2.dk/interaktiv/csctidslinje>

Wendel-Hansen, Jens (2013): *"Boligen er ukrænkelig"*. On Videnskab.dk. Viewed the 1st of October, 2014.

<http://videnskab.dk/blog/boligen-er-ukraenkelig>

Wikipedia (2012): *Islands historie*, viewed the 26th of September, 2012,

<http://da.wikipedia.org/wiki/Islands_historie#Island_under_Danmark_.281380-1918.29>

Willer, Jakob et. al (2013): *Høring over udkast til forslag til lov om ændring af straffeloven, retsplejeloven, lov om konkurrence- og forbrugerforhold på telemarkedet, våbenloven, udleveringsloven samt lov om udlevering af lovovertrædere til Finland, Island, Norge og Sverige (ændring af revisionsbestemmelse*). Viewed 1st October, 2014.

<http://www.teleindu.dk/wp-content/uploads/2012/08/JM-h%C3%B8ring-revisionsbestemmelsen-24.01.2013.pdf>

7 List of Figures

8 List of Abbreviations

Abbreviation	Definition
CCTV	Closed circuit television
CPR	Civil Registration System (Det Centrale Personregister)
DPI	Deep Package Inspection
EEC	European Economic Community
EU	European Union
FE	Danish Defence Intelligence Service (Forsvarets Efterretningstjeneste)
GDP	Gross domestic product
NATO	North Atlantic Treaty Organization
NemID	unique ID number in Denmark
NGO	Non Governmental Organisation
PET	Danish Security and Intelligence Service (Politiets Efterretningstjeneste)
PKK	The Kurdistan Worker's Party (Partiya Karkerên Kurdistan)
SLT	Smartphone Location Tracking
SOST	Surveillance-oriented security technology

9 Annex

9.1 Table recommendations

Template[103]

Hvad er hovedbudskabet i jeres anbefaling?

_____

_____

_

Hvad er baggrunden for anbefalingen? Hvad er udfordringen?

_____

_____

_

Jeres anbefaling // hvad bør gøres? Hvordan kan udfordringen løses?

_____

Recommendations – content[104]

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?
It must not be a choice between surveillance and privacy. We need both. Therefore, the technology should be designed and legislated so both are possible.	The criteria for selection and analysis of data is to be drawn up by humans, and it requires taking an ethical stance. *Evidence* is needed before initiating surveillance. Greater transparency from companies and authorities about what the surveillance is used for.	An ethical council (commission / fora) that should take a stand on current and coming technological surveillance. Participation across political, religious and ethical and other interests.

[103] 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.

[104] Translated from Danish

Surveillance should be opted in rather than opted out on peoples phone / internet. Greater transparency in "trade conditions" for ordinary people. Differentiation between public and private data collecting. Clearer / more distinct information to the people.	Increased use of surveillance - the public is insecure. Ensure balance between peace of mind and privacy. Fear and insecurity must not control our lives – private as well as public. Surveillance is fine, but it increasingly throws suspicion on people.	education in primary school regarding the surveillance society. Pitfalls of internet trade/apps. Signposts that we are under surveillance and by who. These companies should need authorisation and their data treatment and ethics should be subject to control. The control is to be carried out by a Danish agency (our a common European institution developing rules and regulations).
More and clearer information and transparency about the use of personal information.	Lack of knowledge about use (in general) and abuse (NSA, Google (sale of and trade with information) etc.)	Information must be made available to the citizens (both nationally and from the EU) - About purpose of use, who is conducting the surveillance, what technologies are utilized, is information stored and for how long? What are the procedures and the legislation in force? The rules for private and public entities, respectively, must be made clear. Appointment of an ombudsman like institution, monitoring and securing EU's IT infrastructure. Information / education could be via documentaries, OBS (information to the public about society), pamphlets etc.
Clearer legislation and clear information for the citizens.	The citizens lack knowledge and information about the existing legislation on the subject. The citizens don't have knowledge about security technologies in general. There is insecurity about what influence the security technologies will have in the future.	Quick legislation should keep up with the technological development. Registration of who is allowed to use surveillance and what the surveillance may be used for. An active informational effort is necessary, educating the citizens – it must be easily understandable information that is easily available.

The central message is that there should be a balance between the use of security technologies and the violation of privacy that they entail. By this is meant: If a private company gathers data, an impartial public authority must monitor and control the gathering, use, storage and passing on, including sale, of information. Public authorities should be subject to control from independent supervision. Private individuals subject to violation in connection with the surrendering of information, should have appointed a counsel for defence and be secured presentation to a judge, cf. rules regarding wire tapping.	The background is that surveillance provides security for the public, while violating the public. The challenge is, therefore, to create a foundation for security while ensuring that private persons or groups are not violated unnecessarily. Another challenge is that the technology develops faster that the legislation.	as citizen it should be completely transparent what you are agreeing to, if you, for instance, download an app. E.g. concrete geographical location. Unnecessary information must not be demanded. If countries outside the EU wants to sell / promote software [and] technology inside the EU, these countries and their companies must accept and adhere to the legislation in the EU. In addition, refer to ad 1, 2, and 3 under the first question.
The legislation must be construed internationally. Control should be spread to more agencies to protect against abuse. Regarding control, there should be made technological, legal and ethical considerations. These considerations must also be made in the development of the systems.	The information is potentially no sufficiently secure. Continuous evaluation whether the gain/utility value is equal to the encroachment /possible harm – how much personal freedom should we give up? It is physically impossible to control how the information is circulating.	The task must be lifted to EU level, which means common European legislation. Data must be protected, so citizens can opt out of sharing with e.g. countries outside the EU. Greater transparency. Service shouldn't be conditioned on giving away information about oneself, that is fundamentally unnecessary to the companies.

The overarching recommendation: the legislation must keep up with the technological development to prevent abuse.	Insecurity regarding private actors. Violation of constitutional rights.	Regarding apps: no general accept, the buyer must give permission to track (as an example). Advanced surveillance: information disclosing that an area is under surveillance and who is behind the surveillance. The passing on of information (data gathered through smart phone tracking and anpr) should be announced to the users.
Information about use and abuse of the various surveillance technologies with special concern regarding the terms and agreements we make (with e.g. Facebook, …) Right of access to documents regarding what is registered about ones person.	We want to increase our knowledge, so we can make conscious/informed decisions. Preventive effect	Information via newspapers – social media – consumer councils – OBS (information to the public about society) A data consumer council on EU level / ombudsman
Independent entity – a la 4th state power monitoring the collected data.	Common legislation on the subject of data security. Implementing it. Attaining a common stance and legislation in the EU.	A common "data ombudsman", that is independent and impartial regarding the collected data.
Surveillance is OK! But there needs to be legislation on the subject ensuring that surveillance adheres to the general human rights.	Peace of mind (Security) is created through surveillance and the surveillance technology provides convenience (e.g. BroBizz (Automatic access/registration buzzers)). Legislation is ensuring that the surveillance technologies are not being abused.	Legislation should ensure the informational level, following new technology, allows common people the possibility of take a stand on / opt out of surveillance. There should be cross control between the different authorities, in order to prevent abuse of collected data.

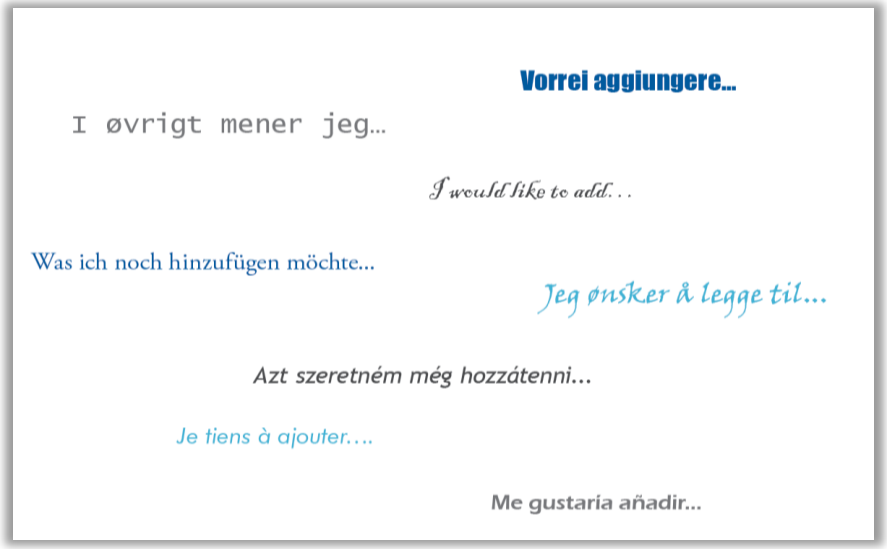
To prevent abuse of the surveillance, using uniform legislation.	To prevent abuse (also includes unwarranted sharing/spread across borders) of - Surveillance - Collected data	Surveillance in the public space must be relevant, justified, and understandable. This must particularly count when surveillance takes place within the home, violating peoples private sphere. Control and surveillance of those using surveillance.
It is ok to utilize technologies, but it is very important that the agencies using the information, are subject to independent and impartial supervision. Trusting them is essential.	Concern regarding abuse of data. We want to utilize the technology, but with peace of mind. To keep legislation up to data relative to the development. The challenge is global, not just a Danish one.	If the EU could find common legislation to counter abuse as well as for development of the technology and the use of it, trust could potentially be build. Try to develop an attitude of respect for the individual. Start in Denmark, spread to the EU, spread as far as possible. Create public understanding and support for the technological development, it should not be curbed.
Information about surveillance must be available to the citizens. Public debate about tracking.	Protecting the citizens. Make citizens aware about in what regards they are not covered.	Ensure transparency, knowledge of legislation. Division of legislation on commercial private and State surveillance. Independent source to supervise legislation from an ethical standpoint. Clarification about storage, by whom, how and duration. The legislation must keep up with technology, and preferably be ahead of it.
Streamlining of legislation at the highest international level is necessary. Legislation in force throughout the world, so large multinationals like Google cannot evade it. We must start by setting an example in the EU.	Data is flying around between servers throughout the world, therefore EU legislation alone will not prevent American surveillance users such as NSA from reading our G-mails. But we can at least set an example to follow – hopefully.	First of all: more education and dialog between politicians and citizens, and from the politicians to the citizens. Who is monitoring me and why= What can you do with a smart phone? What does it take before an authority or others are allowed to collect data about me? Education should start already in primary school

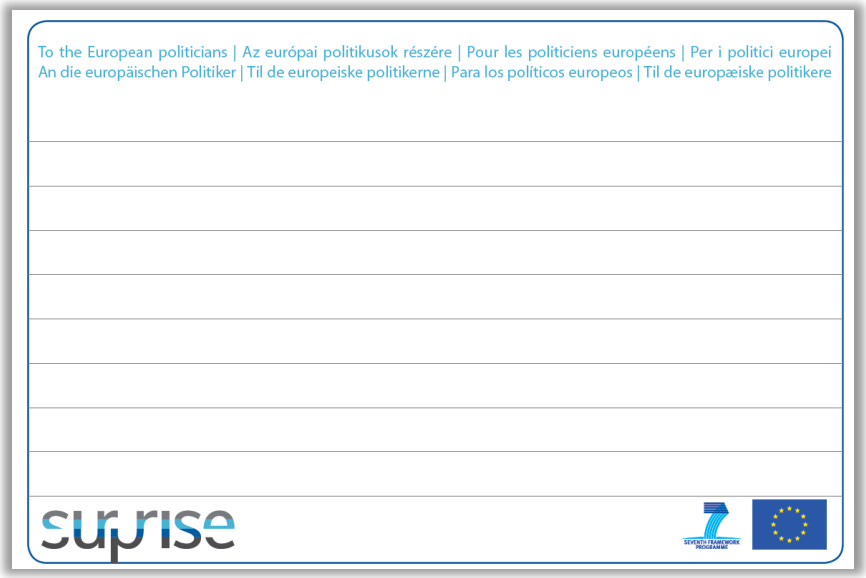
		– children have smart phones, too. Thereupon, concrete, specific legislation across the EU: Who can collect data, what are the demands for storage, how is it ensured that data is not stolen or abused? How far can the data travel to third and fourth parties? Who has the legal responsibility, if data is abused, e.g. to break in while people are not home, because the smart phone says that you're in Spain?
We are proponents of using modern technology for surveillance but it must be ensured that the individual is protected – and violated as little as possible.	Background: we want to apply the technological possibilities. Challenge: to carry out surveillance without violating the individual.	Politicians on international level (not just EU level), must develop clear guidelines for utilizing the aforementioned technologies. We should challenge consumers to demands suppliers to develop apps against commercial surveillance.
Legislation of commercial exploitation of advanced technological surveillance Public debate regarding the "concept of freedom", how does surveillance affect personal freedom, what are we moving towards (development)?	More transparency, violation of privacy, and commercial exploitation. Utilization of "highest common denominator" in the EU, so that national legislation isn't neglected.	For instance public debates in the Ethical Council, and other relevant councils, agencies, NGOs etc (for instance the Danish Data Protection Agency, Datatilsynet). - more transparency / clarity when approving purchases of apps. - Possibility to see what country an app is from → more visibility in other legislation.

Data collection cannot be stopped, but education and information about it can be changed. IT is important that our new generations are educated through the school system. It must be something you can act according to.	Everyone around the table is old enough to have known an age before Facebook and smartphones. Everything you do is something you cannot evade again. Our generation has opted for this, the young generation must opt out.	It must be a subject, just like sex education (from the year you start school). Abuse of data must be treated – stronger legislation. It is important to ensure destruction of data. The young must be told what happens with what they use. Education to change of attitude. What does the signs look like? Information that recording is taking place must be provided every time, both in public and private. Make an obsolescence paragraph – maybe 5 years, when everything is deleted.

9.2 Postcards

Template





Postcards - content[105]

Feedback	Recommendations to European Policy makers	Other
	We need to continually be able to live as free humans without worrying that data about us is sold and connected. We need to not be controlled with the consequence of being manipulated and guided by multinational corporations, e.g. in relation to our consumption and information.	
		The issue concerning EU Bruxells-Strasbourg travelling must be solved now. It is amateurish that a decision has not been reached.
	Surveillance data (of any kind, e.g. COOP's consumption data, the libraries' check-out data, the banks' street cameras, BroBizz, Telmore's cellphone data etc.) should be considered as related to individuals/sensitive data, and thus rules should govern the combination of surveillance data and insight into registered surveillance data.	
	Any company should, at the request of any citizen, hand over all data that the company may have concerning the citizen.	

[105] Translated from Danish

	Democratic, parliamentary control must be ensured, in both individual countries and in the EU parliament before permission is granted for smartphone tracking, smart CCTVs etc. This permission should be given on base of all political groups in parliament, under the slogan 'everyone keeps an eye on everyone'. No private corporations should be given permission.	
	Education in use of online services/media/apps/GPS for everyone, but especially for young people. Should be e.g. 2-4 lessons a year in social sciences – this would likely be enough to create awareness Tools to monitor yourself (what is tracked about me?) Better tools/information about how to disable tracking (many do not know how)	
	Suggestion 1: chip for senile and demented ought to be obligatory with consideration to the security of the demented. Suggestion 2: IT should be put on the primary school schedule, so students learn what it is about and when to watch out. Suggestion 3: prepaid telecommunication solutions should be abolished, because they enable criminals to hide.	
		I find it worrying that new technology for security surveillance is implemented before legislation concerning this is ready.
	The EU ought to develop a common security industry that can match the American, and a European security industry that secures the rights and privacy of citizens.	
	Legislation ought to have focus on ensuring 'privacy, as defined on p. 17 in the information material, supplemented with institutions that can ensure democratic control on the subject and ongoing debate about the development.	
	When a country surrenders sovereignty it is a very substantial and violating process, that may include a public referendum. When we surrender personal sovereignty, e.g. by accepting an app or the conditions on Facebook, it happens with a single click and we usually don't see what we accept – that must be changed, so what we agree to is far clearer.	

	My philosophy is to avoid mishaps, esp. 1a and 1b. 1 alternative solutions should receive much higher priority in solving issues when possible. 1a poka-yoke Slower traffic (roundabouts, etc) in these places replace cameras. Dogs to sniff for narcotics. 1b behavioural adjustment of young people (preventive solutions) 2 CCTV cameras (are needed)	
	We need a nationwide discussion regarding ethics – morals – attitudes to surveillance and what we as humans are willing to accept, and how we treat each other, both internally in the country and between countries – nationalities.	The politicians also have great need to participate in these discussions and regain grounding in reality.
	A precautionary principle that requires sufficiently substantial suspicion. An independent control organ 'watching the watchmen' should be implemented A need for labelling and declarations on goods that simplifies, e.g. EULAs Communication online ought, by default, to be private, that is, without risk of surveillance, as e.g. DPI.	
		Do not forget, in all the enthusiasm for intelligent surveillance, that a society at ease requires a citizen at ease - with share in a reasonable (re)distribution – and an eye to others and thereby basic human rights.
	Give the police increased authority to control surveillance (-companies), that is, more control of surveillance companies and authorization of surveillance companies.	
	Less surveillance (e.g. work mail) at the work place. E.g. do we need a work email? Can we not chose ourselves?	
	More resources ought to be directed at finding alternative – ethical – unique solutions.	

	Storage of surveillance data ought to be time limited, maybe to 48-72 hours. The same ought to apply for electronic footprints, where the storage should maybe even be limited to 24-48 hours.	
	Increase surveillance at the borders, then we can reduce private surveillance.	
Excellent summit!!! Ps. In regards to the consent form, it ought to be you signing to taking great care of my data/information.		
To DBT: I was not impressed by the quality (precision and uniqueness) of many questions.		
Excellent event in every aspect ☺		
I think it is important that the age distribution of the summit is representative. i.e. more young people are needed. They have an entirely different view on the subject, I think.		
I think that there was a lack of participants with different ethnic background than Danish. It must, among others, be those whom the 'terror' surveillance is about.		
Use Danish consultants so the questions are more clearly formulated and not hypothetic. Ensuring clear formulation without reverse questions.		

Very good and well run event, with the one minus that several questions ought to have been clearer or explained (especially all the 'are you worried'-questions appeared to me as if they more emphasized the last part of the statements than whether people are actually generally concerned).		
Excellent event in Aarhus on 18/1-14, with two content issues: a lot of 'on the board education'/screen fixation → too little time at the tables. Normally, precondition differences are enriching, but in this case it entailed a very slow discussion, as there was great disparities in knowledge of what e.g. constitutes "security services".		
Feedback on the summit and form: during the day I have to a large extend, felt a lack of information regarding the current legislation – it is difficult to take a stance on what is secured by legislation (q 75) if you are not presented with it (which the debates were also coloured by). Moreover, I think the debates had too little focus – could have been guided more, so talks only focused on the technologies in question and not drones, corporate surveillance of shopping habits etc. some survey questions precondition certain attitudes, e.g. q. 44 "worries me because…" – what should I answer if it does not worry me? In several of		

the questions the answer categories were open to interpretation. I think it would have been more correct/true and fair responses, if there had been explanatory background information for each question – put in different contexts. Think that the votes have been to superficial and therefore don't think the results will be true and fair, because we probably have different understandings of the questions.		

The following was received on email:

Feedback	Recommendations to European Policy makers	Other
In my group, 7, we formulated this central message, that I would like to follow up on with some additions, that were not included in the groups hand-in. "it must not be a choice between surveillance and privacy. We need both. Therefore technology should be designed and legislation written, so both are possible." I would like to sharpen or concretize to individuals should have right and ownership of their own information and movements. Ownership means that I have the right and opportunity to decide whether the information is used and for what. Information and movement should also be available to laypeople in an understandable way. Technologies today are neither designed nor controlled in a way that enables this. It should apply to people with clean criminal records. If someone does not have a such, the right of ownership should be graduated to the character of the crime they are convicted of. If this can be provided, then surveillance technologies can be widely deployed by both public and private corporations. I can then allow for the information about me to be used for a, for me, comprehensible purpose, and nothing else. A limited consent, so that you in e.g. Nem e-post (or what the public eBooks is called) can chose in detail how you want to receive mail. Ownership also means that I can sell my attention and information to companies, if I want to, and that private companies do not exploit my attention and consent without my knowing and active consent. By, in this way empowering both individuals and companies in one strike, a frugal cooperation can take place.		
Thank you for the opportunity to contribute. I would say, though, that there were too many click-questions and too little debate options; rotating between the tables would have been good.		