"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 6.6 - Citizen Summits on Privacy, Security and Surveillance: Country report Norway

Lead Beneficiary: NBT

Author(s): Marianne Barland (NBT)

Due Date: June 2014

Submission Date: September 2014

Dissemination Level: Public

Version: 1

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

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

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

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

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

Table of Contents

Executive Summary

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

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

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

In this report the results from Norway are presented.

Norway is a country characterized by a strong belief in democracy, individual autonomy and the rights to privacy. The Norwegian term for privacy, “personvern”, has been debated and defined in many ways over the years. “Personvern” is a distinctly Norwegian notion, that captures the right to private life and integrity, but also the right to control one owns personal data. This wide definition of and view on privacy has developed over time, and combines the “old” view on privacy, something related to integrity and the right to private life, and the new challenges related to gathering and processing of personal information brought on by digitalization.

National security and safety has been an important issue for Norwegian governments since the cold war. But fragmented coordination and few incremental changes has caused many debates. Until the 22nd of July 2011, Norway has had very few incidents that have made a crisis-driven change in policies. After the terror attack in Oslo and Utøya in July 2011, national security and preparedness has been on top of the political agenda. This has also spurred public debate about democratic values like privacy, openness and transparency. The debate has re-emerged and intensified after the revelations about the NSA and the PRISM program.

February 1st 2014, 130 Norwegian citizens were attending the SurPRISE citizen summit in Oslo, Norway. Organized in small groups, the participants discussed and voted on questions related to the topic of surveillance, privacy and security throughout the day. At the end of the summit, they wrote their own recommendations to policy-makers. The participants were aged between 18 and 77 and with various backgrounds. Inhabitants of all Norwegian counties were represented.

The Norwegian participants have an inherent feeling of safety in their everyday life, and they consider Norway a safe country to live in. But at the same time, our increasing digital society creates new challenges and threats that need to be considered. The discussions at the citizen summit gave a general support for the use of surveillance-oriented security technologies to increase national security. The participants showed support for implementation of such technology, but were at the same time very concerned about infringement of their privacy. Untargeted mass-surveillance of citizens was considered highly intrusive, and the citizens demanded laws and regulations to control this. They considered privacy a fundamental right, and wanted this right to be protected, both on a collective and individual level. While they were supportive of security measures implemented by security agencies, they were

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

more skeptical towards private companies using the same technology for marketing or other commercial use.

Two technologies were discussed more in detail at the Norwegian summit: internet surveillance by deep packet inspection and smartphone location tracking. While seen as an effective measure for national security, deep packet inspection was not considered very effective for the participants' individual security. The technology was considered highly intrusive, and the participants were worried about how the use of deep packet inspection could develop in the future.

Smartphone location tracking was considered somewhat less intrusive than deep packet inspection, but as location was considered sensitive information for many participants, they had privacy concerns also for this technology. The technology used in location tracking was more familiar to the participants than deep packet inspection, as it is something they use themselves, for example in maps or other apps on their smartphones. Some participants explained that the tracking feature of smartphones was something that created a feeling of safety – knowing that they could be located if something happened. At the same time they were worried about untargeted surveillance, and wanted to control how location tracking was used.

When writing their own recommendations to policy-makers, there were few participants who recommended putting an end to surveillance completely. Instead they wanted policy-makers to work together and create international regulations and control bodies, and to limit surveillance to cases where there are proven suspicion of criminal activities. The participants' recommendations also focused on transparency and information to citizens – that we should know what kind of information is collected about us and our activities, and how this information is used. To make children able to take informed choices in the future, the participants also recommended stronger focus on technology and privacy in education.

This report starts off with an introduction in chapter one. In chapter two, we give a short introduction to privacy, surveillance and security in Norway. Chapter three introduces the process design of the Norwegian citizen summit, while chapter four presents the empirical results from the voting, discussions and recommendations from the summit. Chapter five presents a summary and conclusions.

1 Introduction

Privacy and security are two important elements in society today. How national security agencies approach their goal of keeping citizen secure has developed over the years. Technology has become an important element in measures taken, and more often than not, these measures include surveillance of citizens.

In Norway, privacy is considered a fundamental right and an important element of democracy. During the recent decades and especially after the terror attacks in Oslo and Utøya in 2011, there has been debates on how we can have a secure and safe society, and at the same time uphold democratic values like privacy, openness and transparency.

In these discussions it is rare to ask citizens about their opinion. Even though it is policy-makers who in the end make the decisions, it is the citizens who have to live with the consequences. A citizen summit is a good method for collecting signals and opinions in the populations on the benefits and challenges related to important topics. The participants at a citizen summit are not representative for the population, but are a broad group of citizens from different backgrounds.

February 1st 2014, 130 Norwegian citizens attended a citizen summit to discuss and vote on topics related to surveillance, privacy and security. The participants were between ages 18-77, came from all over the country and from various backgrounds. They spent the day discussing, voting and formulating their own recommendations to Norwegian and European policy-makers. The citizen summit was part of the EU-funded SurPRISE-project, and twelve European citizen summits were organized during the spring of 2014[2]. At the Norwegian summit, two specific technologies were discussed: online surveillance by deep packet inspection and smartphone location tracking.

This report presents the result from the Norwegian summit. The results are based on the discussions around the tables and the results from the voting during the event. The content from the discussions was recorded by four dedicated note takers, and notes from the table moderators. The participants were also encouraged to write postcards to the policy-makers if they wanted to communicate an individual message.

[2] See http://surprise-project.eu for more information

2 Privacy, security and surveillance in the national context

2.1 Country profile of Norway

Norway is a country covering the western stretch of the Scandinavian Peninsula, from north to south along the Atlantic coastline. There are approximately 5.1 million inhabitants in Norway, of which 624,000 reside in Oslo, the capital. The wider Oslo region comprises almost 25 percent of the total population. The other major population centers are located along the western and northern coasts facing the North Sea and the northern Atlantic. The BNP per capita is 65,000 USD PPP, among the world's highest. The state intervenes in the economy mostly by redistributive means and as a neutral majority shareholder in publicly owned companies. The Gini coefficient is low, between 0.24 and 0.27, Norway thereby being one of the most egalitarian countries of Europe together with Slovenia and Denmark. Furthermore, the society is characterized by high levels of interpersonal and institutional trust, significantly above the European and OECD average.

Norway is a constitutional monarchy with the royal head of state having formal powers only. The government is led by a prime minister, currently Erna Solberg from the Conservative party, and the parliament is unicameral. The form of government is parliamentarian, with minority coalition governments being the norm and majority coalitions exceptional since the 1980s. Seven parties regularly gain seats in the parliamentary elections, of which the Labor party and the Conservatives regularly obtaining the largest shares, in that order. At the time of writing, the government is led by a recently formed two-party minority coalition comprising the Conservatives and the right-wing populist Progress Party. The Norwegian welfare state, established mainly during the post-war era, remains politically unchallenged. The political center is somewhat to the left of that of most other European countries.

The country's EU-relations are complex. Norway is not a member of the Union, but it is a member of the single market through the European Economic Area. As such, it is subject to most EU laws and directives. There have been two referenda over the country's full accession to the EU, one in 1972 and one in 1994, both resulting in a slight negative majority. The voting patterns followed geographical and demographic patterns, with the largest urban areas and the south and south-west of Norway voting in favor of admission, and the northern parts and more rural areas voting against. These patterns are still recognizable today, although the Eurozone debt- and financial crisis has significantly reduced the support for Norwegian EU-membership. The traditional political fault lines on which the current party system is based do not correspond to those guiding attitudes towards the EU, thus making the established parties reluctant to engage in EU-related debates, let alone reviving the prospect of a Norwegian membership.

2.2 Security issues, policy and strategies

2.2.1 Three main principles

The Norwegian government's approach to security and safety has since the 1990's been guided by three core principles: liability, decentralization and conformity[3].

The liability principle implies that every ministry and authority has responsibility for internal security and safety within its own sector. It is closely related to the doctrine of individual ministerial responsibility, emphasizing strong sector ministries. The decentralization principle emphasizes that a crisis should be managed at the lowest operational level possible. This corresponds with the principle of local self-government, and makes geography a central additional organizing concept. The ministers bear the

[3] Christensen, Lægreid og Rykkja (2012): How to cope with a terrorist attack? – A challenge for the political and administrative leadership. COCOPS Working Paper No. 6 (http://www.cocops.eu/wp-content/uploads/2012/08/COCOPS_workingpaper_No6.pdf)

ultimate responsibility for actions within their ministry, including those of subordinate agencies. The third principle, conformity, emphasizes that the organizational forms in a crisis should be as similar to "normal organization" as possible. In a working paper from the EU-project COCOPS (Coordinating for Cohesion in the Public Sector of the Future)[4], an interesting paradox is described. The principle of liability implies strong vertical coordination within specific sectors, but weak coordination between them. Decentralization implies strong horizontal coordination across sectors at a low lever, and hence less coordination between vertical levels of governments.

National security and safety has been an important issue for the governments since the cold war. But fragmented coordination and few incremental changes has caused many debates.

In 2000, the Green paper "A vulnerable society"[5] described measures that could strengthen Norwegian security and preparedness, and formulated the base for Norwegian security and safety strategies. The recommendations included a strengthening of the relationship between the police and the ministry of defense, establishment of requirements for the operation of critical IT systems, inclusion of attacks with chemical and biological weapons in hospital emergency plans and a strengthening of emergency information before and during a crisis.

The Green paper from 2000 was followed by a White paper in 2002[6]. The white paper highlighted terrorism as one of the most important challenges ahead, to a much larger degree than the Green paper.

The Green paper, "Protection of critical infrastructures and critical societal functions in Norway"[7] was published in 2006. It highlights the same challenges as the Green paper from 2000, and states that the preparedness to handle most adverse situations is established, and that society's ability to deal with everyday accidents is good.

Just a couple of months before the devastating attacks in 2011, the Ministry of Justice published the action plan: "Collective security – a shared responsibility"[8]. This was Norway's first action plan for the prevention of radicalization and violent extremism. It presented four priority areas: knowledge and information, cooperation between authorities, dialogue and involvement and support to vulnerable and at-risk persons. The report stated "Norway is one of the safest countries in the world and creating a safe and secure society is a fundamental aim of every government. […] We have no guarantee that no serious situations will arise and the terror threat can change rapidly". Two months later, Norway experienced a terror attack which killed 77 people and injured almost 300.

2.2.2 After the terror

On July 22nd 2014, Norway experiences its deadliest attack since World War 2. A terrorist executed two sequential attacks claiming a total of 77 lives. A car bomb placed in the center of Oslo – in front of the governmental building housing the office of the Prime minister, killed eight people. Less than two hours later, the terrorist arrived at Utøya, an island hosting the annual summer camp for the Labor party's youth division. Dressed as a police officer, he killed 69 people at the island. The terrorist was an ethnic Norwegian man, aged 33. The evidence indicates that he was a "lone wolf", operation on his own.

These incidents made it clear that the country was not prepared for such an attack, and in the aftermath there have been many debates about how one can improve national safety and security. An important element in this debate has been the trade-off between security and societal values like openness, privacy, democracy and freedom of speech. Surveillance-oriented technologies have been part of this debate. As security is becoming more and more connected to technology – politicians' tasks are more challenging. Good intentions are not enough; the rush for new technological solutions has sometimes undermined the values they are there to protect.

In 2012, a governmental appointed commission published its report[9] – a green paper analyzing Norwegian preparedness and security policies in the aftermath of the terror attacks. The commission

4 Ibid.
5 http://www.regjeringen.no/nb/dep/jd/dok/nouer/2000/nou-2000-24.html?id=143248
6 http://www.regjeringen.no/nb/dep/jd/dok/regpubl/stmeld/20012002/stmeld-nr-17-2001-2002-.html?id=402587
7 http://www.regjeringen.no/nb/dep/jd/dok/nouer/2006/nou-2006-6.html?id=157408
8 http://www.regjeringen.no/upload/JD/Vedlegg/Handlingsplaner/Radikalisering_engelsk.pdf
9 http://www.regjeringen.no/nb/dep/smk/dok/nou-er/2012/nou-2012-14.html?id=697260

concluded that the attacks could have been prevented if one had used already existing measures. The main conclusions from the commission were:

- The ability to recognize risk and learn from exercises has been to weak
- The ability to implement action plans has been to weak
- Ability to coordinate and interact has been lacking
- The potential of ICT have not been used effectively
- Management's ability and willingness to clarify responsibilities, establish goals and take action to achieve results has been inadequate

Following this green paper, two white papers have been produced; on terrorist preparedness (2013) and national security (2012).

The White paper on national security[10] presents measures for increasing national security and preparedness. The paper introduces a new principle for Norwegian security policy: the principle of cooperation ("samvirkeprinsippet"). This principle tries to solve the challenges of cooperation and coordination between different sectors and sector-levels. In the White paper, Internet is presented as a strategic security challenge. Related to this (but not the exclusive reason), the Police Security Services (PST) got a 21 million NOK increase in their budget. This was aimed at investments and development within the field of cyber security, communication control, reconnaissance and VIS (the Schengen Visa Information System).

In 2013, the White paper on terrorist preparedness was published[11]. This report presents further measures for preparedness and introduces a national strategy for combating terrorism. The strategy has five goals which include prevention of radicalization processes and extremism, international cooperation and managing if an attack does happen.

This report does to a larger degree than earlier policy documents, emphasizes Internet and ICT as important elements, both as a challenge and a solution. The report acknowledges that Internet is an important arena for communication and sharing between individuals and groups. The Internet is also an arena for planning and executing criminal actions. The Police Security Service needs more robust and accessible ICT solutions to be able to handle these challenges.

Both criminals and law enforcement have become more active online. This activity relates both to planning criminal activity and cooperation online, and cybercrime. After the terror attacks in 2011, the police, the Police Security Services and the Intelligence Services are planning new investments and strategies for use of ICT and Internet. What these developments include and what the results will be is still uncertain.

2.3 Privacy issues

2.3.1 Defining privacy

The Norwegian term for privacy, "personvern", has been debated and defined in many ways over the years. "Personvern" is a distinctly Norwegian notion, that captures the right to private life and integrity, but also the right to control one owns personal data[12]. This wide definition of and view on privacy has developed over time, and combines the "old" view on privacy, something related to integrity and the right to private life, and the new challenges related to gathering and processing of personal information brought on by digitalization.

Norway is a country characterized by a strong belief in democracy, individual autonomy and the rights to privacy. The Norwegian constitution of 1814 does not have a specific provision for the protection of privacy, but in a more general term it states that authorities have a duty to "respect and secure human

[10] http://www.regjeringen.no/nb/dep/jd/dok/regpubl/stmeld/2011-2012/meld-st-29-20112012.html?id=685578
[11] White paper 21 (2012-2013): Terrorberedskap. Oppfølging av NOU 2012:14 Rapport fra 22. juli-kommisjonen. http://www.regjeringen.no/nb/dep/jd/dok/regpubl/stmeld/2012-2013/meld-st-21-20122013.html?id=718216
[12] Green paper 2009: 1 "Individ og integritet. Personvern i det digitale samfunnet» http://www.regjeringen.no/nb/dep/kmd/dok/nouer/2009/nou-2009-1.html?id=542049

rights" (section 110c)[13]. Although human rights are not specifically defined, the incorporation into Norwegian law of the European Convention on Human Rights and Fundamental Freedoms of 1950, and the International Covenant on Civil and Political Rights of 1966, diminishes this shortcoming. The Criminal Code of 1902 includes a section that punishes the violation of privacy ("privatlivets fred") caused by "public disclosure of information relating to personal or domestic affairs"[14].

Processing of personal data is regulated through the Personal Data Act from 2000[15] (PDA). The purpose of the act is "to protect natural persons from violation of their right to privacy through the processing of personal data". The Act does this by ensuring that all data are processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and private life and ensure that personal data are of adequate quality"[16]. Norway is not a member of the EU, but the PDA is designed so that Norwegian law is brought into compliance with the EU Data Protection Directive 95/46/EC.

The PDA provides strong protection of someone whose data have been collected. It states that everyone has a right to access the data collected about them, that all incorrect data must be corrected and that you have the right to block your name from use in direct marketing.

When it comes to the notion of personal data, a distinction is made between *personal data* and *sensitive personal data*. Personal data is seen as a piece of information or an assessment that can be linked to you as a person. Sensitive personal data is information on race or ethnicity, political or religious affiliation or information on criminal history, medical history, sexual relations or membership of worker unions[17].

The Norwegian Data Protection Authority ("Datatilsynet") is responsible for monitoring and enforcing the PDA. Their main task is to "facilitate protection of individuals from violation of their right to privacy through processing of their personal data"[18] .

The Data Protection Authority is organized under the Ministry of Local Government and Modernization, but executes its tasks independent from the Government and private interests. The DPA has existed since 1980, and is well known and respected among Norwegian citizens[19]. The DPA is funded under the National Budget, and has in 2014 a budget of 38,624 mill NOK (approximately Euro 4,783,000). The budget has increased somewhat the last five years, from Euro 3,627,500 in 2009. The DPA has 40 employees.

Decisions made by the Data Protection Authority may be appealed to the Privacy Appeals Board (Personvernnemnda).

2.3.2 Global surveillance monitor

In Privacy Internationals Global surveillance monitor from 2007, Norway is classified with "systemic failure to uphold safeguards". The report states that there are few safeguards, and widespread practice of surveillance[20]. In PIs monitor from 2011, Norway gets positive remarks in some areas[21]. Proposals for introducing new, privacy intruding technology, e.g. body scanners has been turned down, and specific laws regarding workplace surveillance are in place. Despite these positive efforts, there is still room for improvements. Medical privacy is challenged by the fact that one use centralized registries for medical databases. Financial privacy has also been degraded, by granting more actors access to records of financial transfers in and out of Norway.

---

13 Bygrave and Aaø (2001): Privacy, Personality and publicity – An overview of Norwegian Law, in M. Herny (ed), international Privacy, Publicity and personality Laws. London: Butterworths) http://folk.uio.no/lee/publications/Overview_Butterworths.pdf

14 Ibid.

15 The Personal Data Act of 14 April 2000 No. 31 in English (http://www.ub.uio.no/ujur/ulovdata/lov-20000414-031-eng.pdf)

16 The Personal Data Act, Section 1

17 www.datatilsynet.no

18 http://datatilsynet.no/English/

19 Inger-Anne Ravlum (2005): Pinning our faith on Big Brother … together with all the little brothers? Oslo: Transportøkonomisk institutt

20 Privacy International (2007): Global surveillance monitor 2007

21 Privacy International (2011): Global surveillance monitor 2011

2.3.3 Data retention directive

EUs Data Retention Directive (2006/24/EF) was adopted by the Norwegian Parliament April 2011. It was planned to be effective from April 1st 2012, but was postponed several times. In early 2014 it was still not effective. The delay was partly caused by disagreements on distribution of costs, and adaption of the telecommunication industries' IT systems. The Ministry of Transport and Communication planned to set it into force by January 2015[22].

Before and during the debate of the directive in the Norwegian Parliament, there was a lot of political and public debate on the topic. The bipartisan organization "Stop the data retention directive" (Stopp Datalagringsdirektivet") was set up in 2009. They collected approximately 13,000 signatures against the adoption of the directive. The group "Digital Privacy" (Digitalt personvern) was created in 2011 with some of the same organizers as "Stopp Datalagringsdirektivet". This group has set an aim to fundraise enough money to try the Data Retention Directive at Norwegian Court[23].

In 2014, the Data Retention Directive was declared invalid by the EUs Court of Justice, due to its interference with privacy and private life. The Norwegian Government's response is to look into how the collection of data from telecommunication can be done, so that privacy is being protected.

2.3.4 Reactions to NSA and the PRISM program

The information revealed by Edward Snowden on the NSA's mass surveillance programs have been met with dismay, surprise and disappointment in Norway. The revelations have sparked a renewed and recurring debate on privacy and surveillance, related to the changing nature of privacy, big data, and social media. Also, the revelations have highlighted the need for more transparency both in order to promote greater understanding for the work of intelligence agencies and most importantly to secure stronger oversight mechanisms of such agencies. This last point has been particularly important as doubts have been cast on the extent to which elected officials are able to exert their authority over the Norwegian intelligence community.

The political parties to the left of the then governing Labor party have generally expressed support to Snowden, while the opposite is true for the parties to the right, with the exception of the center-right Liberal party which campaigns regularly on themes such as freedom of information and personal privacy rights. The center-left Labor-party has been less than outspoken on the matter, following a traditional Atlanticist line in all matters foreign- and defense-policy related. The Conservatives, in power since September 2013, have also refrained from stating an official position on either the revelations or Snowden himself. Additionally, in January of 2014, prominent figures from the Socialist Left Party nominated Snowden for the Nobel Peace Prize, but this effort has not garnered any considerable support from major news outlets or politicians.

All of the major national newspapers, regardless of political affiliation, declared their support to Snowden's actions and condemned the bulk gathering of information by the NSA and consistently refer to him as a "whistle blower". Several outlets have repeatedly called for a re-evaluation of the relation between elected officials and intelligence agencies, specifically regarding the need for an increase in the powers of the parliamentary intelligence oversight committee, and stricter rules on the collection and treatment of metadata.

Following the media attention of December 2013 on the collaboration between the Norwegian Intelligence services (NIS) and US intelligence agencies, the director of NIS announced in March 2014 that, breaking with a decades-old policy of secrecy, NIS would from now on be more transparent in order to avoid misinformed accusations similar to those that followed the mentioned leak.

[22] http://www.regjeringen.no/nb/dep/sd/dok/hoeringer/hoeringsdok/2013/horing-om-datalagring---forslag-til-regl.html?id=725244

[23] http://www.digitaltpersonvern.no/

2.3.5 Surveillance-oriented security technology – implementation in Norway

Police and intelligence

The Norwegian police forces are free to set up CCTV cameras without applying to the Data Protection Agency. There are a limited number of cameras put up by the police, approximately twelve nationwide[24]. During major events, like the World Ski Championship in Oslo in 2011, there were put up additional cameras, but these were taken down after the event.

Private companies have to apply to the Data Protection Agency before installing CCTV cameras, and numbers from the DPA suggests that there are approximately 21,300 cameras owned by private companies in Norway.

In April 2012 changes were made in the law regulating CCTV. The definition of "camera" was broadened so that "look alike" or dummy cameras are regulated under the same law. On the other hand, the new text emphasizes that it only includes fixed cameras, excluding for example hand held or mobile cameras.

The police have expressed their interest in using drones for surveillance. This is still not implemented, but there is a growing interest for this technology in several sectors in Norway. Seeing an increasing non-military use of drones, for example by the police or media, the new regulation of cameras might be challenged in the future.

Transportation

eCall is the European system for emergency service. The system is implemented in cars, and in the case of a crash, automatically calls the nearest emergency center. Even if the passengers are not able to speak, the system transmits data, including the exact location of the car. The positive effect of eCall is clear; it cuts emergency services response time. But even though the system is in a default "sleep" modus, it has a surveillance aspect that many people find intrusive. The European Commission adopted the introduction of eCall in 2011, and the system is to be implemented by the end of 2014.

Even though Norway is not a part of the European Union, many regulations are implemented without much adaption. One example of this is the EU regulation on safety in airports after the attacks in the US 9/11. This was implemented in Norway in April 2003.

In 2007 the Norwegian Aviation Authority, Avinor, proposed to try out body scanners in the security checkpoints at Stavanger Airport. The scanners were to be tested on the airport personnel, but strong reactions from the public, Labor unions and the workers themselves, led to cancellation of the implementation. There have not been any proposals of implementing body scanners after this.

Since April 2010, all new Norwegian passports contain an electronic chip that contains biometric information. The biometric data are included to give a more precise identification. The process of implementing the biometric passports was executed fast, and the Data Protection Agency was skeptical of the way the biometric passports were introduced. They would have wanted a more thorough process and assessment of the new passports and how the biometric information could challenge privacy.

Databases

The EURODAC system is an information database containing data on immigrants and asylum seekers in Europe. By registering fingerprints, governments can determine whether an asylum applicant or illegal immigrant has previously claimed asylum in other countries, and whether an asylum applicant entered the European Union unlawfully. Knowing that governments use fingerprints for identification in the EURODAC system, several immigrants have tried removing their fingerprints before arriving in Norway, by burning or sanding their fingertips.

After the 22nd of July, there was a debate in Norway on whether or not the terrorist could have been detected before he acted. One of the things that were picked up on was the international network called Global Shield. This is a program that aims at detecting smuggling or trade with chemicals that could be used to build explosive devices. This database uses toll data and registers anyone who buys listed chemicals. The Norwegian police security services got an alert from toll officials giving them, among others, the name of the terrorist in Norway after he bought ingredients for his bombs.

[24] Number based on inquiries to the police departments in the country

A dilemma when using data from Global Shield is determining when to actually investigate further. Someone might buy a very small amount of legal chemicals and still be registered on the list, because these chemicals could be used as part of a bomb. One example is farmers buying manure online. Since manure could be used in bombs (like it was in Norway) their information would be stored by Global Shield.

Another important form of data registration and sharing is the one the citizens do themselves. Even though this isn't a surveillance practice being implemented by "someone" or the government, it is important to consider how much data we actually put online for example when using social media. Almost everyone in Norway now owns a smartphone, and with this mobile sensor in our pockets, enormous amounts of data are registered every day. Does this affect our view on privacy? And do we actually consider the traces we leave when sharing a picture, "checking in" to a new place or liking a webpage?

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

2.4.1 The Lund commission

The Lund commission was appointed to investigate allegations of illegal surveillance of Norwegian citizens by the intelligence services. Their report[25] was presented to the Parliament in March 1996 and concluded that there had been extensive surveillance of individuals belonging to the political left and communist groups. After this practice was exposed, the Parliament passed a law, so that anyone who suspected that they had been monitored had the right to see the content of their files.

The report caused a lot of public and political debate on surveillance practices by the intelligence services. The courts were criticized for not having oversight of the process, especially when it was revealed that kids as young as 11 years old had been monitored.

After these revelations, the Parliament established the Norwegian Parliamentary Intelligence Oversight Committee ("EOS-utvalget"), an oversight body to oversee intelligence, surveillance and security services carried out to safeguard national security interests.

2.4.2 National privacy survey

As previously stated, Norway has a high level of trust between the citizens and the governments. This is shown in several surveys on a wide range of topics over the years.

In 2005, the Data Protection Authority made a population wide survey on citizen's knowledge about and attitudes towards privacy[26]. Both private and governmental institutions are considered trustworthy when it comes to processing of personal information. The police get the highest rating, and 91 percent have great trust in how they handle personal information. The survey also examined in what situations the citizens worried about misuse of their personal information. Use of Internet, was the one situation where over fifty percent were worried that their information might be misused. Also, younger and better educated citizens were less worried than others. When it comes to the use of mobile phones, forty percent were worried about misuse. Contrary to the use of Internet, higher educated citizens were less worried than the rest, when it came to location tracking of mobile phones.

In 2013, the Data Protection Authority did a new survey, where they asked if people have become more concerned with privacy in the last couple of years. 46 percent of the population says they are more concerned now than before and only two percent say they are less concerned now than two years ago. The respondents were also asked who they thought had most responsibility to protect their privacy. 53 percent answered that it was themselves, through their own choices. 33 percent meant the government was responsible by making regulations, and only 14 percent placed the responsibility at the institutions

[25] Rapport til Stortinget fra kommisjonen som ble oppnevnt av Stortinget for å granske påstander om ulovlig overvåking av norske borgere («Lund-rapporten»)
https://www.stortinget.no/Saker-og-publikasjoner/Publikasjoner/Dokumentserien/1995-1996/Dok15-199596/

[26] Inger-Anne Ravlum (2005): Pinning our faith on Big Brother … together with all the little brothers? Oslo: Transportøkonomisk institutt

that hold the information. The survey also shows that 69 percent of the population thinks it is important that the regulation protects information revealing your movement and places you have been. This kind of data has become more sensitive the latest years. In the privacy survey from 2005, 48 percent answered the same way.

The survey from 2013 also asked the respondents what kind of personal data they thought was most important to protect. Interestingly enough, their answers differed a lot from the definitions of "sensitive personal data" in the PDA. The respondents rated information about politics, religion and union affiliation as least important. Content in emails and phone conversations, information about your health and social security number was rated as most important to protect.

A large part of the Norwegian population owns a smartphone. There have been concerns about the large amount of digital traces that are left behind every day, many of them relating to a person's location. In 2010, a service called "Bipper" put location tracking on the agenda. Bipper is a service that once installed on a child's smartphone, lets the parent control what numbers the child can and cannot call, and allows the parent to track their children's location. The service spurred a debate on the relationship between a child's privacy and parental control, where the Data Protection Authority was critical of this kind of service[27]. A survey from the Data Protection Authority from December 2013 showed that eight out of ten thinks that privacy is important for a free and democratic society.

After the NSA scandal broke in 2013, government's surveillance of citizens has gotten a lot more attention than earlier. The NSA story also showed a lack of knowledge in the population and the media about what kind of intelligence exists and whom the intelligence services monitor[28].

2.4.3 Participatory activities – the PRISE project

In 2007, the PRISE project[29] conducted interview meetings in several European countries. 26 Norwegians participated in a meeting, discussing their views on security technology and privacy.

The participants expressed little fear of terrorist attacks, and discussed security technologies in relation to other forms of crime. Data retention and social media was something the participants were very interested in, mainly caused by the introduction of Facebook that same year. The limited number of CCTV cameras (at least compared to other European countries), makes this a little debated topic in Norway. On the other hand, location tracking was something the participants were eager to discuss, and they were more critical towards this than the other European participants[30].

Another interesting result from the PRISE interview meeting was that what people define as threats and what they see as infringement of privacy, differ widely. The participants also said that their views change, depending on their own and others' experiences.

[27] Ole Petter Baugerød Stokke (2010): Mobiltjenesten Bipper overvåker barn ("Bipper monitors children") http://www.vg.no/teknologi/artikkel.php?artid=10017672

[28] Teknologirådet og Datatilsynet (2014): Personvern – Tilstand og trender (The Norwegian Board of Technology and the Data Protection Authority : «Privacy – status and trends»)

[29] http://www.prise.oeaw.ac.at/

[30] PRISE (2008): D 5.8 Synthesis Report –Interview meetings on Security Technology and Privacy

3 Process design – the citizen summit in Norway

The Norwegian citizen summit was held on February 1st 2014. The venue was a conference center in the center of Oslo, called "Folkets Hus" ("The House of the People"). The preparations and organization of the event was done by the Norwegian Board of Technology (NBT).

The recruitment process started in December 2013. 10,000 contact letters were sent to randomly drawn addresses in Norway. The addresses were accessed from the National Population Registry, and the sample included addresses from all counties, gender and ages. Information on educational background is not included in the National Population Registry; therefore this was not a criterion when sending out the contact letter.

The contact letter included a short introduction to the project and the Norwegian citizen summit, together with an info sheet with more information on the SurPRISE project. The recipients were asked to register their application at a website, or get in contact with the NBT for a registration form sent by mail.

Approximately one week after the letters were sent out, the NBT also started recruiting through other channels. A short introduction article was posted at www.teknologiradet.no, with a link to the online registration form. This article featured twice at the NBTs newsletter (1,750 recipients). It was also shared on Facebook (506 followers) and Twitter (2,180 followers).

In total, 186 people registered at the web side. In addition, two people registered by mail, after receiving the form from the NBT. All who registered received confirmation letters. Confirmation letters were first sent out in the end of December, and then continuously whenever someone new registered.

About ten people withdrew their registration after receiving the confirmation letter. This was mainly due to other obligations the same date as the citizen summit. The weeks before the event, there was also some cancellations due to illness or other urgent matter. At the event, 154 participants were expected, and 126 people attended.

The NBT had recruited 33 people for various roles at the event. The head facilitator was the project manager at the NBT responsible for the SurPRISE project. She was assisted by one project manager. The Director and the Communication officer of the NBT were present all day and handled various tasks. 24 table facilitators guided the participants through the day. About half of these were master students from the University of Oslo. The rest were employees and former employees at the NBT and other governmental institutions that work close with the NBT. Four staff members filled the roles as note takers.

3.1 Structure of the citizen panel

A total of 126 people participated at the event. 44 percent of the participants declared to be women, 53 percent men. The distribution of age was good, and quite close to the country distribution of Norway[31]. The largest age group was between 40 and 59 years old (44 percent). This group was slightly overrepresented, as this age group constitutes 31 percent of the Norwegian population. 29 percent were between 18 and 39 years old (29 percent of country total), and 24 percent were over 60 years old (21 percent of country total).

[31] All country statistics from Statistisk Sentralbyrå - «Statistics Norway» 2013 (www.ssb.no).

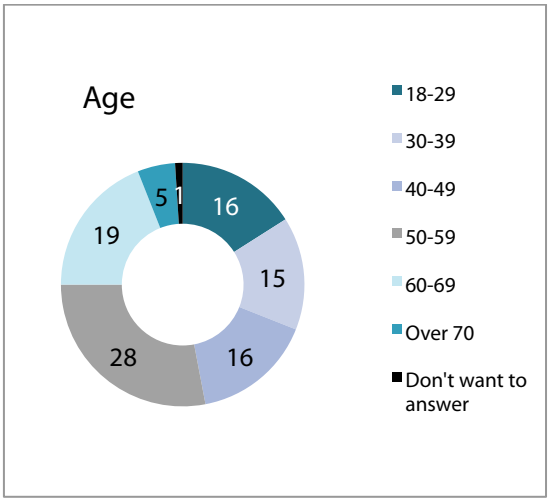


Figure 1: Age (Percentage)

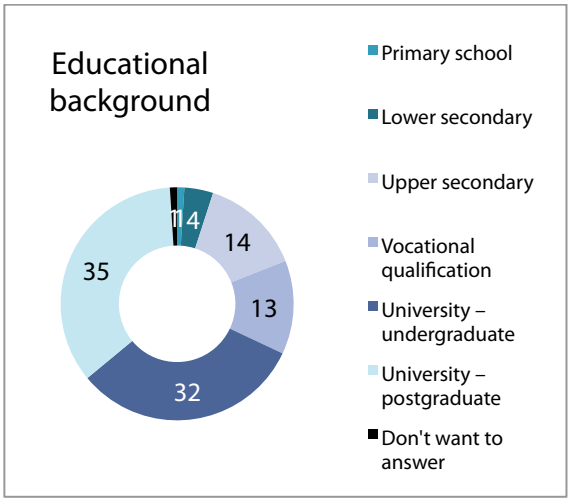


Figure 2: Educational background (Percentage)

Norway has a high-educated population. 27 percent of males and 33 percent of the female population has undergraduate or postgraduate level. This is reflected in the participant group, where 67 percent reported education on undergraduate or postgraduate level.

The average annual income in Norway is 470,900 NOK (approximately Euro 57,625). 38 percent of the participants reported that they earned more or a lot more than this. 46 percent earned less or a lot less than the national average.

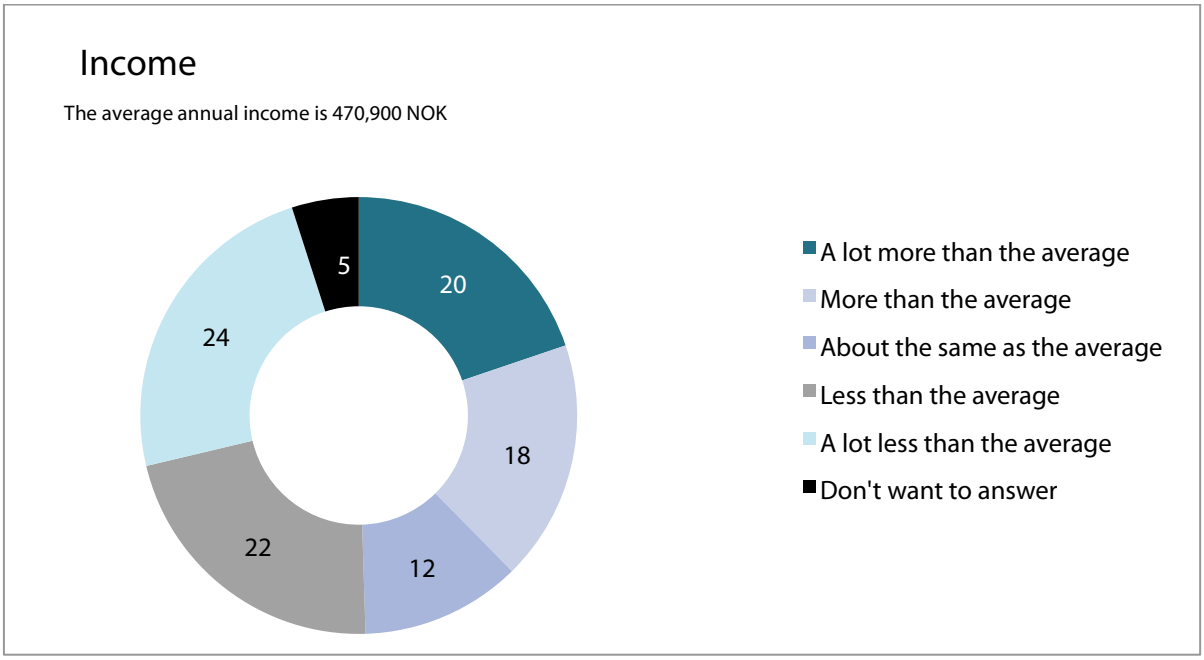


Figure 3: Income (Percentage)

The NBT decided to recruit participants from the whole country. This gave the summit an inclusive quality, and the participants appreciated meeting people from all over the country. Several participants from the north of Norway wrote in their registration that they were very glad to be included, as they sometimes felt that the Oslo-region was the only one heard in projects like this. The summit had

participants from all 19 counties represented. 21 percent answered that they lived in a large city[32]. 34 percent lived in an urban area, whereas 32 percent lived in a rural area.

Almost all participants at the summit were Norwegian citizens. One person was citizen of another European country, while two people had a dual citizenship from two European countries. 11 percent of the participants answered that they belonged to a minority group.

3.2 How citizens assess the summit

The participants gave a positive evaluation of the citizen summit. 66 percent answered that they gained new knowledge by participating. This is also reflected in the questions related to how much knowledge they had of the topic before and after reading the information magazine, seeing the films etc. 50 percent said they knew little or nothing about surveillance-oriented security technologies. Towards the end of the summit, only 1 percent answered the same.

Although many participants said that they gained new knowledge, over half of them (55 percent) left the meeting with the same attitudes as they arrived with. For the rest of them, 11 percent left the meeting more positive towards surveillance-oriented security technologies, and 33 percent were more negative.

After spending a whole day debating and voting, 84 percent of the participants agreed or strongly agreed that the summit had produced valuable input for policy makers. This high number clearly shows that participation in an event like this feels valuable for the citizens.

During the event, the participants were encouraged to use postcards if they wanted to give feedback on the organization of the summit. Through these postcards the NBT received very positive feedback on the organization of the event and the citizen summit as a method. The messages on the postcards highlighted the positive experience of meeting and discussing with others, and the diversity, in age, background and experience, around the tables.

[32] Oslo (the largest city in Norway) is home to approximately 624,000 people (Source: SSB)

4 Empirical results of the citizen summit

4.1 General attitudes on privacy and security

The citizen summit started with questions mapping the participants' general attitudes on privacy and security. Norway is a country characterized by high level of trust, and this might explain the high feeling of safety reported at the event, where the majority of the participants stated that they generally feel safe in their everyday life (82 percent). An even higher number, 90 percent, felt that Norway is a safe country to live in. Only 3 percent disagreed with this statement.

As stated in previous chapters, there have been several public debates about security, technology and privacy in the last years, especially after the terrorist attacks in 2011. There have been many different views in these debates, and it seems that Norwegians are concerned about privacy, but at the same time supportive of surveillance-oriented technologies when they are used to improve national security. 80 percent of the participants agreed to the statement "use of surveillance-oriented security-technology improves national security.

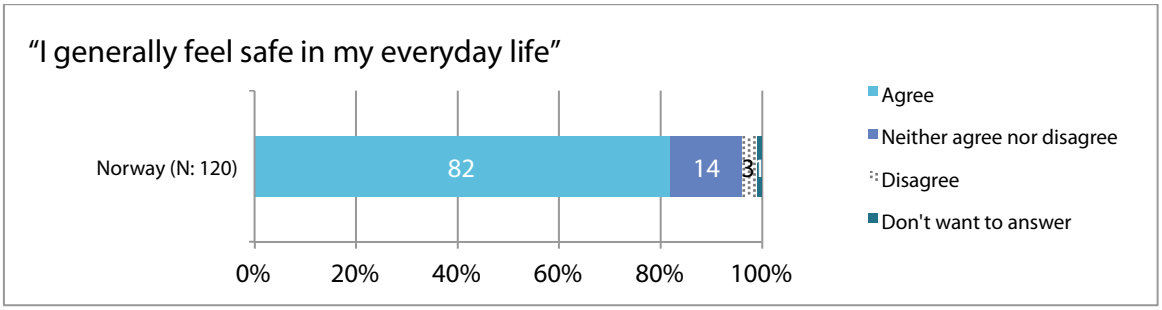


Figure 4: "I generally feel safe in my everyday life" (Q3)

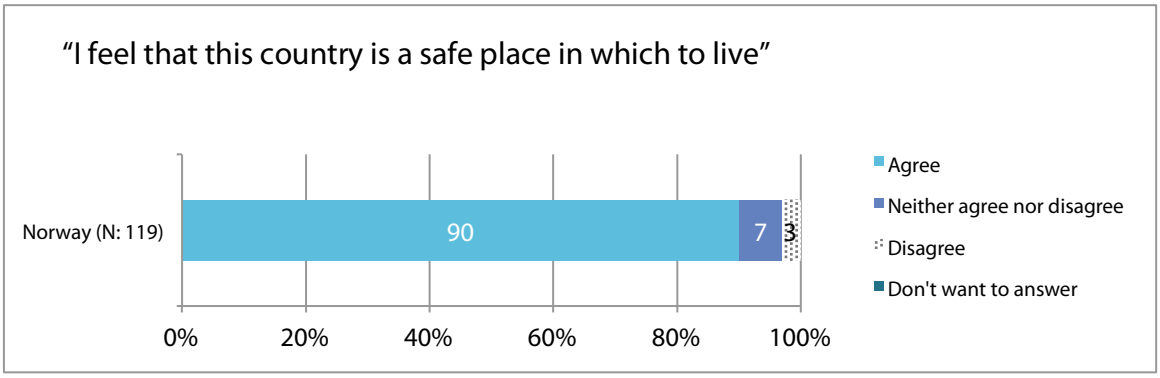


Figure 5: "I feel that this country is a safe place in which to live" (Q5)

In the discussions around the tables, and in the recommendations to policy-makers, many participants were concerned with the need to keep our society safe - both from more "traditional" threats like terrorism, but also from cybercrime and illegal surveillance. They had become more aware of possible threats, but public debates had also made them more aware of the importance of privacy.

Take care of every citizen's safety without infringing privacy Postcard from participant[33]

[33] All postcard from participants to policy-makers are listed in Annex

4.2 Use of surveillance-oriented security technologies

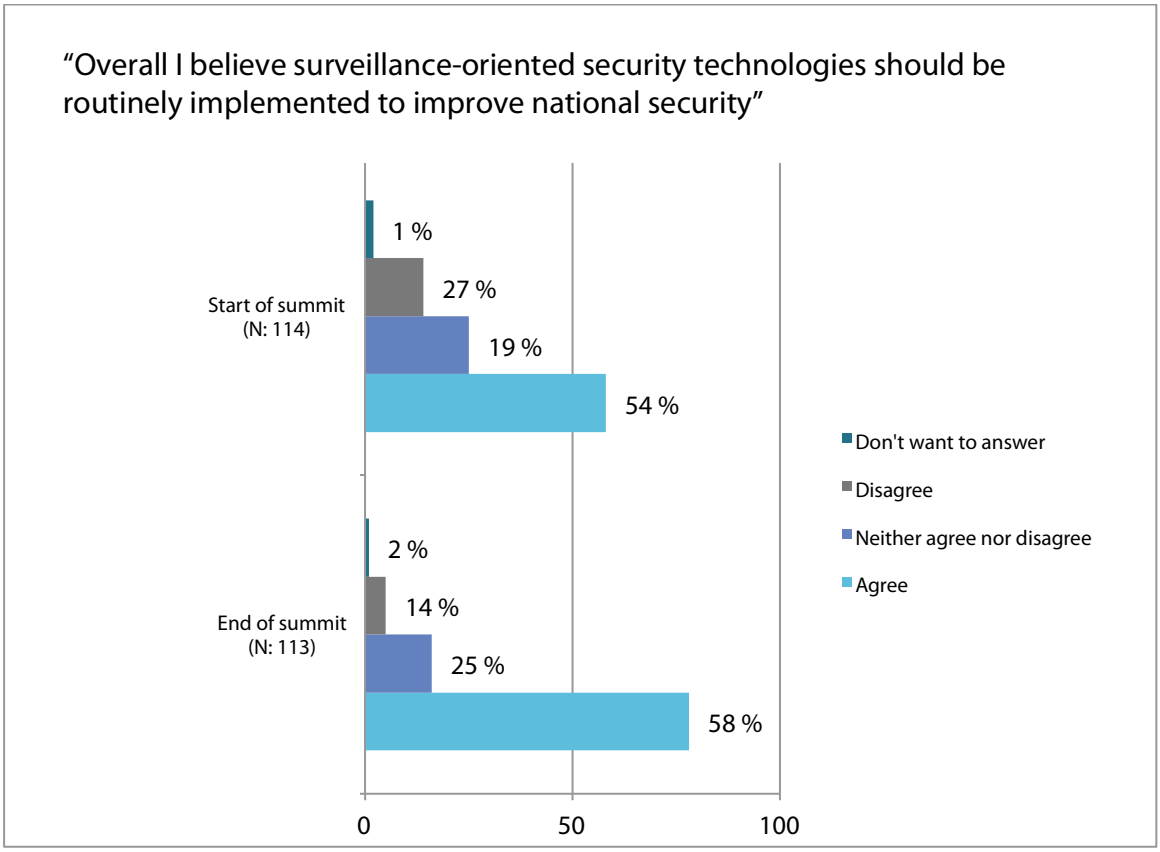


Figure 6: "Overall I believe surveillance-oriented security technologies should be routinely implemented to improve national security" (Q7 and Q94)

Overall, the Norwegian participants were positive towards the use of surveillance-oriented security technologies to improve national security. They were asked twice about this, at the start and the end of the summit, and as shown by Figure 6 their attitudes became somewhat more positive at the end of the summit.

4.2.1 Perceived effectiveness vs. intrusiveness of surveillance-oriented security technologies

After a general discussion of surveillance-oriented security technologies, the Norwegian participants discussed two technologies in detail: internet surveillance by deep packet inspection and smartphone location tracking. The participants were somewhat familiar with these technologies, and respectively 74 and 90 percent said that they understand what deep packet inspection and smart phone location tracking is. At the tables, some participants referred to the media attention about NSA and the PRISM program as one of the reasons they knew about these surveillance technologies. Participants also mentioned the SurPRISE information booklet as a source of information.

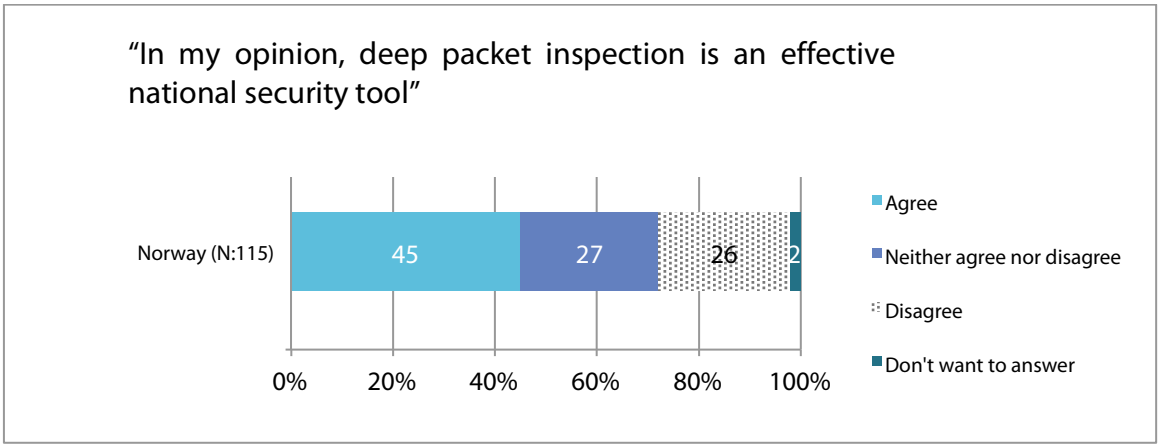


Figure 7: "In my opinion, deep packet inspection is an effective national security tool" (Q22)

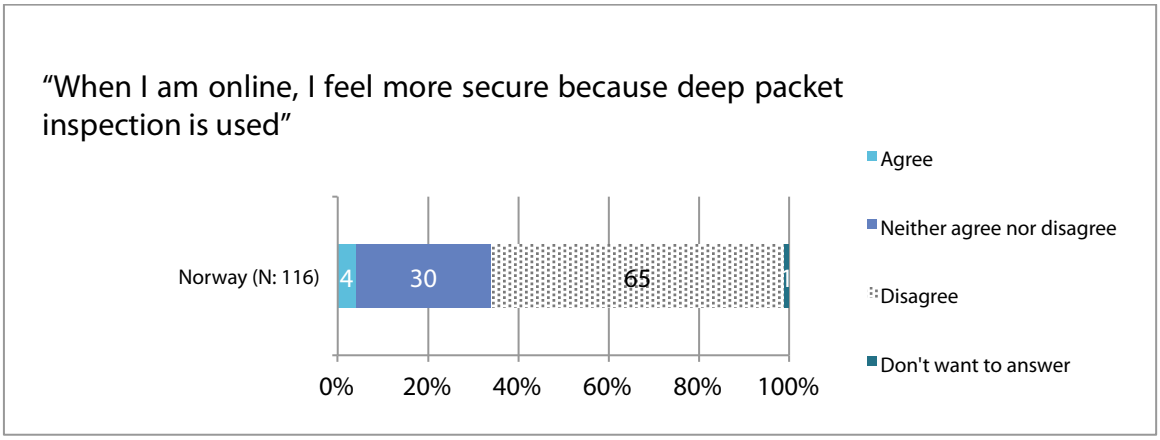


Figure 8: "When I am online, I feel more secure because deep packet inspection is used" (Q24)

Figure 7 shows that almost half of the participants perceived deep packet inspection as an effective national security tool. 26 percent did not agree with this statement, while almost the same percent (27) neither agreed nor disagreed.

As stated earlier, Norwegians generally feel safe in their everyday life. But when questioned about Internet and safety, 57 percent said that they worried about safety when they were online. Although 45 percent thought deep packet inspection was effective when it comes to national security, it was only 4 percent who felt safer online because of deep packet inspection. These differences show that the technology was perceived more effective at a national level, than for the participants' individual feeling of security.

During the table discussions, some participants expressed concerns about online threats. They were unsure of what the increased use of Internet and smartphones meant to their safety, and wanted to know more about online surveillance and the data that are collected about them. But because they had little knowledge about the actors that used deep packet inspection and how and when it was used for security reasons, the technology was not considered relevant for their personal security. It was rather looked at as something used by intelligence services and police when it came to national security.

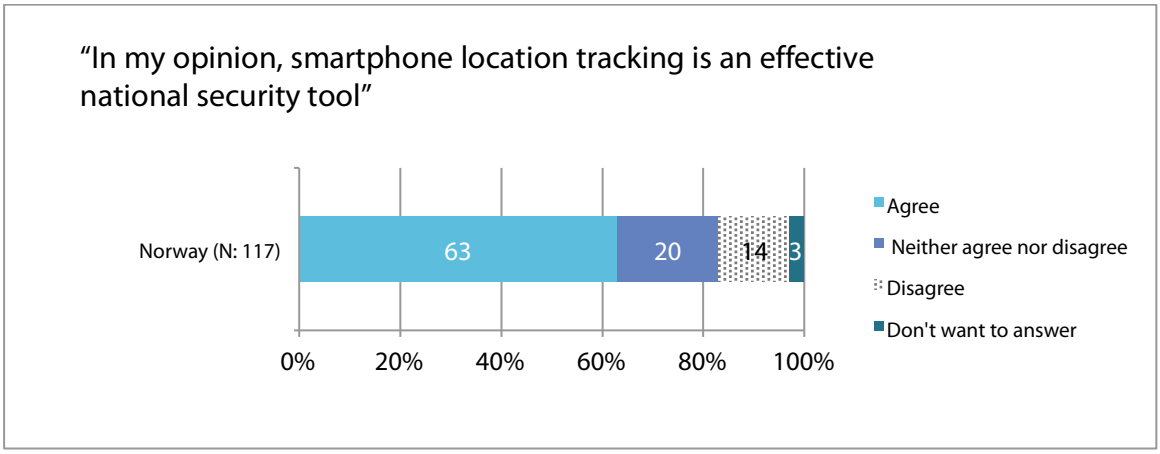


Figure 9: "In my opinion, smartphone location tracking is an effective national security tool" (Q 27)

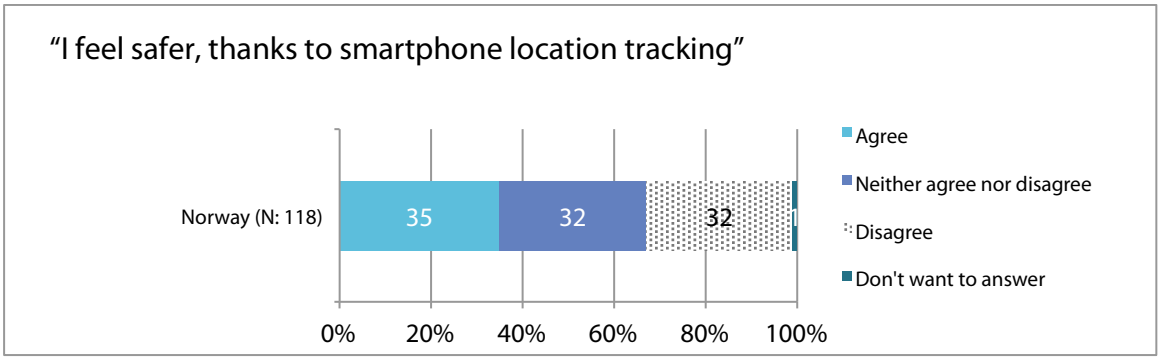


Figure 10: "I feel safer, thanks to smartphone location tracking" (Q29)

Smartphone location tracking was in general seen as a more effective technology for increased security than deep packet inspection, and 35 percent of the participants felt more secure because of location tracking. One of the reasons for this could be that it is more familiar to the citizens. It is a technology they carry with them and use themselves, for example when using online maps or apps localizing possibilities for public transportation. Even though smartphone location tracking is seen as more effective than deep packet inspection, the percentage that see it as effective it is not very high. This might reflect the fact that for many people, this technology is not first and foremost seen as a security technology. The commercial use is more familiar for them, as it relates more to their daily use of their smartphones. These commercial uses include personalized marketing and offers based on your location. It also includes a range of services and application related to travelling, transport, weather services etc. Participants also mentioned that they were positive to functionality that could track their phone for example if it was stolen.

Over the years, there have been several stories in Norwegian media of how the police use location tracking of mobile phones in their investigations. The most common use has been to confirm the presence of a person at a certain time and place, or to exclude a person's presence from a specific time and place. The last years, it has also been paid more attention to the use of location tracking when trying to find people who are lost, for example seniors with dementia or hikers getting lost in the mountains. Several participants mentioned that carrying their smartphones gave them a feeling of safety. It enabled them to contact help if needed, and they also felt safe knowing that they could be located if they were unable to call for help themselves.

4.2.2 Major concerns about surveillance-oriented security technologies

Many of the participants expressed skepticisms towards the use of deep packet inspection, and found it highly intrusive to their privacy. The fact that it can access very personal information like the content of communication, location and browser history was something the participants felt as uncomfortable. 78 percent of the participants said they worried that deep packet inspection could reveal sensitive information about them.

84 percent of the participants worried about how deep packet inspection could develop in the future. The NSA revelations had been an eye-opener for many, and knowing the amount of information that can be accessed from our online activity made some participants worry that online anonymity would be impossible in the future. The need for new and international legal frameworks was seen as important, and even more – an oversight body that could intervene if someone broke the law when using deep packet inspection in an illegal way. Although many worried about the future, some participants had hopes that one would be able to develop technology that would be more difficult to abuse. The concept of "privacy by design" was mentioned by one participant, and she hoped that future technology developers would use their knowledge to increase privacy, instead of increasing surveillance.

Almost 80 percent of the participants worried that deep packet inspection could violate their human rights. An even higher number, 89 percent, worried that deep packet inspection could violate everyone's fundamental rights.

Even though the possibility of locating smartphones improved perceived security for some, it felt intrusive for others. For them, the feeling of freedom was lost when they knew they could be located almost anywhere. Almost 90 percent of the participants felt that smartphone location tracking was something that was forced upon them without permission. The fact that they are not able to choose for themselves whether to activate or deactivate all tracking features, felt intrusive to several participants. The only option was to not use a smart- or mobile phone at all, and in today's society that was considered impossible by many of the participants.

62 percent of the participants worried that smart phone location tracking could reveal sensitive information about them. When asked specifically about location, 74 percent were worried because the tracking technology could let strangers know where they were.

More than two thirds of the participants were worried about how the use of smartphone location tracking could develop in the future. From the discussions, some participants described their fear as a scenario where the police or other security agencies know where everyone is all the time, picturing a "Big Brother" watching everyone. Several participants described their location as sensitive personal data, and wanted to have the possibility to stay "hidden" from tracking technology, also in the future.

The number of participants that worried about smart phone location tracking violating their fundamental human rights was somewhat lower than for deep packet inspection. But the same tendency was present: that the participants were more concerned about everyone's human rights, than their own.

The participants were in general somewhat more concerned about deep packet inspection than smart phone location tracking.

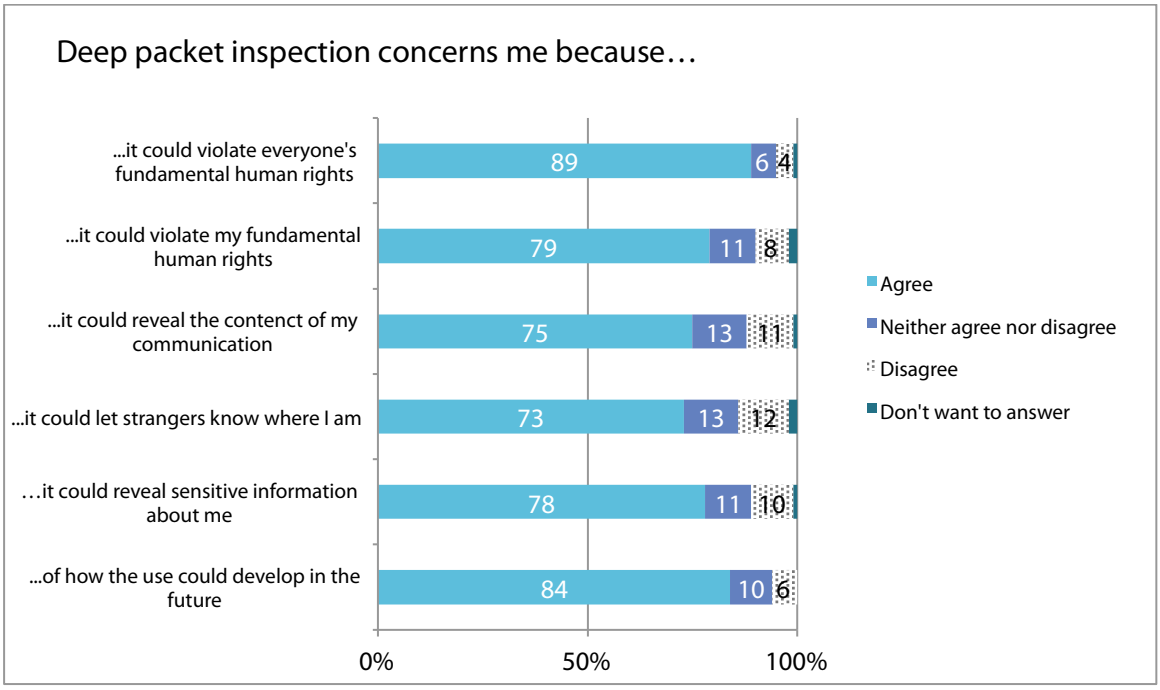


Figure 11: "Deep packet inspection concerns me because…" (Q36, 46, 47, 49, 50, 51)

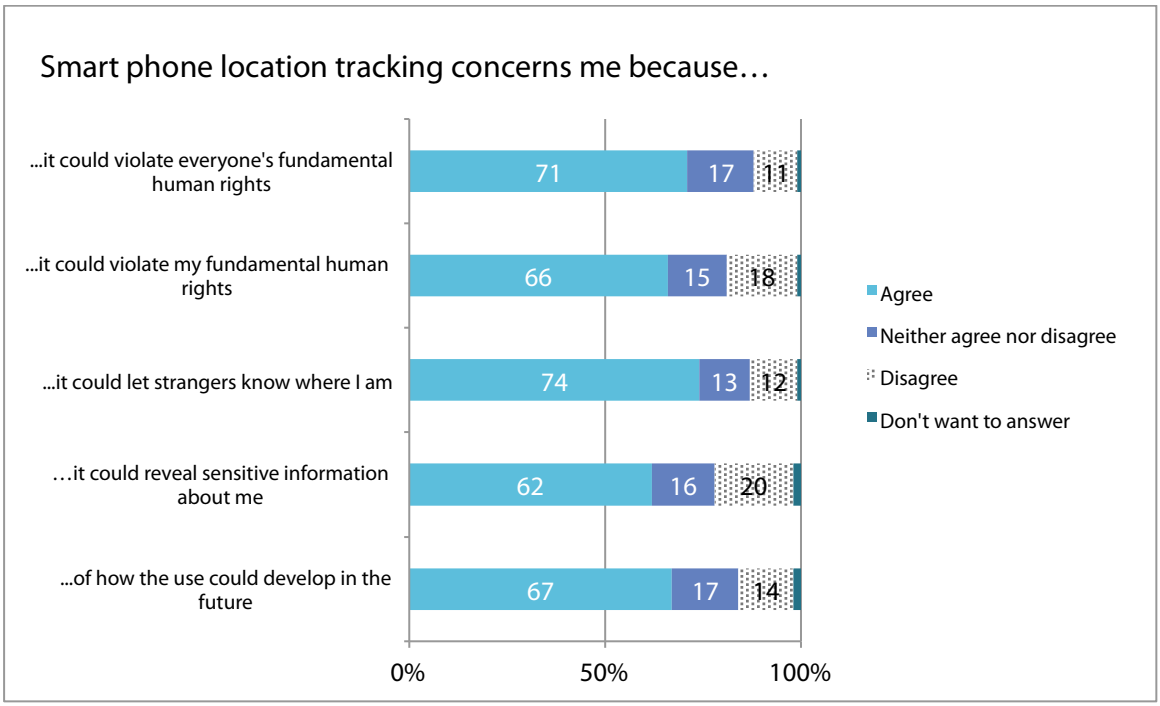


Figure 12: "Smart phone location tracking concerns me because…" (Q39, 52, 53, 55, 56)

4.3 Avoidance and resistance against surveillance

The Norwegian participants were frequent users of both Internet and smart- and mobile phones. They are familiar with solving tasks online, and as the Government and municipalities have a strategy of "digital first"[34], this digitalization of online services will probably increase in the future.

The increasing use of online services and digital tools means that we leave behind more digital traces than before, and the number of actors that collects data about you is also growing. Although many participants were not bothered by this, some feared that this might lead to a chilling effect. Knowing that information about your online activity is collected can make you hold back and don't do the things you would normally do, in fear that the information might come up later or in another context that you expected. Companies almost always make users accept specific terms and conditions before they can start using an application or service. Several participants said that even though they wanted to read all these terms, they were too many and too complicated. This lead to indifference, and they accepted everything, even though they in some cases might reject or avoid the service because of the terms and conditions.

At the citizen summit, we asked the participants if they would change their behavior because of surveillance-oriented security technologies like deep packet inspection or location tracking of their phones.

Few of the participants said that they would stop using their smartphones or definitely change their behavior because of location tracking. Almost half (48 percent) of the participants didn't think they would change their behavior at all.

For deep packet inspection, 28 percent said they would change their behavior to avoid deep packet inspection. In the group discussions several people mentioned that they thought Internet surveillance could have a negative effect on the way we work and internal communication at the work place. They feared that employees would hold back and be more careful about what they communicate by email.

Some participants mentioned stories of people being denied entry permits, for example to the US, because of things they had written on social media like Facebook and Twitter. Although they were aware of examples like this, the majority of the participants did not think they would change their behavior because of deep packet inspection.

The participants were also asked whether they would actively challenge the use of location tracking and deep packet inspection for security reasons. Very few participants wanted to take actions to prevent the use or campaign actively against location tracking, and 17 percent did not oppose the use at all. The majority of the participants, almost 70 percent, wanted to learn more about how they could protect their privacy.

[34] The principle of «digital first» entails that when citizens interact with governmental or municipal institutions, their preferred means should be digital, not the more "traditional" use of telephone or letters.

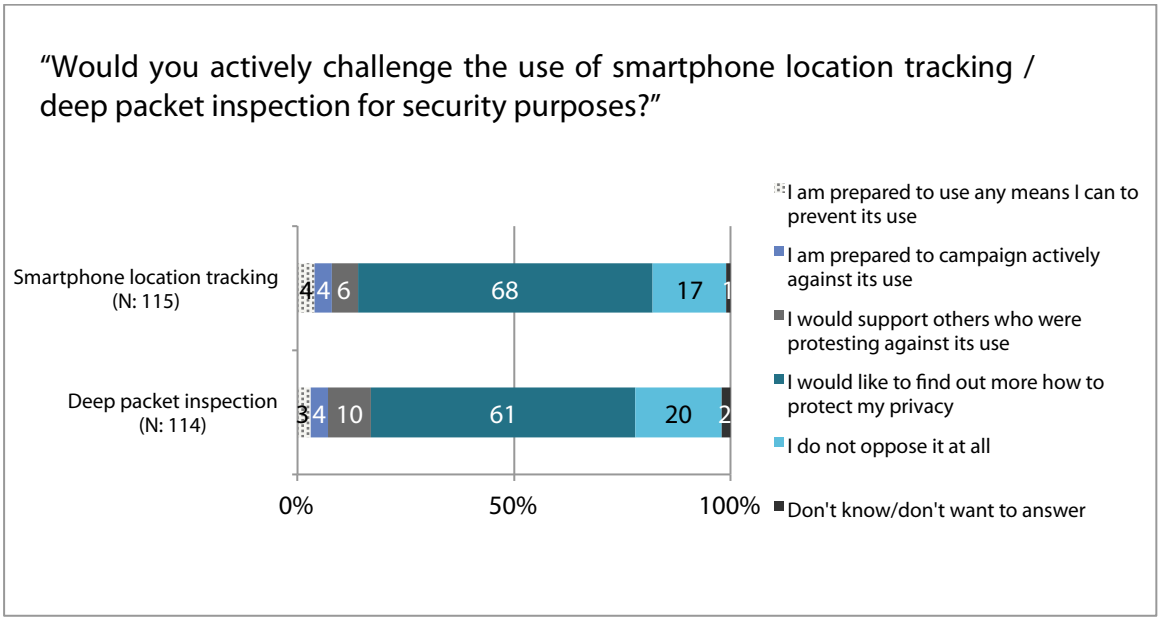


Figure 13: "Would you actively challenge the use of smartphone location tracking / deep packet inspection for security purposes? (Q58 and Q59).

From the discussions and previous questions we know that the participants were generally positive towards surveillance-oriented security technologies being used to improve national security. This could explain why there are few who say they would change their behavior or actively challenge use of these technologies. Their answers might be different if the technologies are used for commercial purposes.

In the table discussions, the participants expressed a more skeptical attitude towards private companies using deep packet inspection or location tracking. The chilling effect was mentioned by several people and some argued that especially deep packet inspection could be a barrier for democracy.

A general attitude amongst the participants was that the uncertainty of who collects information and how it is used for commercial uses creates a negative attitude towards deep packet inspection. At the same time, this negativity is not enough for them to actually change their behavior.

4.4 Individual and collective aspects of security and privacy

4.4.1 Opinions on security

Almost all the participants thought that surveillance-oriented security technologies improve national security. Only 5 percent disagreed with this.

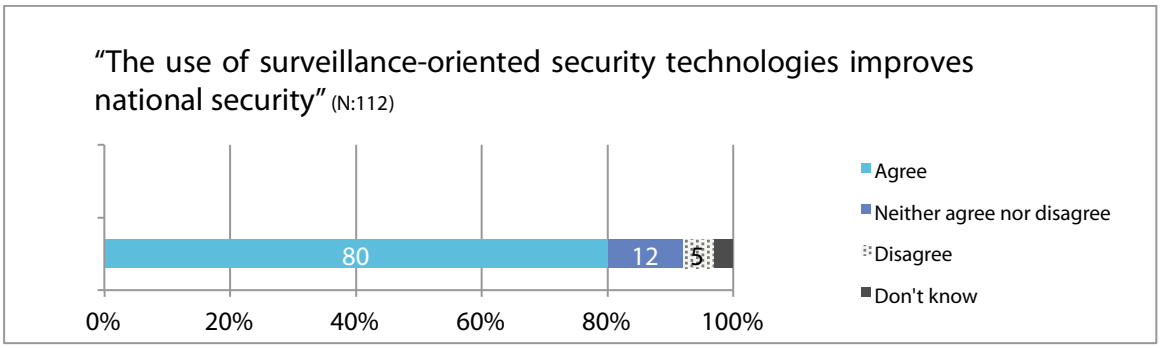


Figure 14: "The use of surveillance-oriented security technologies improves national security" (Q84)

It also seemed that the participants assess the technologies and their implementation as somewhat effective, as only 16 percent agreed to a statement saying that the technologies "are only used to show that something is being done to fight crime". The Norwegians' high trust in the state and governmental bodies might explain this tendency. When a technology is implemented for security reasons, the citizens assume that the state and security agencies have a good reason to do so.

Even though the participants were quite positive towards the technologies presented at the citizen summit, it was clear that they also found them intrusive, and were worried about their privacy being invaded. When asked to relate to the statement "If you have done nothing wrong you don't have to worry about surveillance-oriented security technologies", only 23 percent agreed to this. 57 percent disagreed or strongly disagreed.

Somewhat contradicting, almost two thirds of the participants said that deep packet inspection and smartphone location tracking did not bother them as long as it only targeted criminals.

During the discussions, many of the participants were unsure of when and how surveillance-oriented security technologies are used for security reasons (especially in the case of deep packet inspection). This uncertainty could explain their sometimes contradicting answers. One the one hand, the citizens trust that the surveillance is used to target criminals and prevent criminal activity. On the other hand, knowing that you are being monitored even though you have done nothing wrong creates a negative attitude towards the implementation of such technology.

When discussing these topics, several participants expressed concerns about the balance between a safe society where security agencies are able to stop criminals by surveillance, and an open and democratic society where everyone's privacy is protected. As most of the participants had a strong feeling of safety in their everyday life, the discussions mostly focused on collective and national security.

4.4.2 Opinions on privacy

In the recommendations to policy-makers, many of the tables define privacy as a fundamental right, and a right that is very important to protect. However there were few tables which tried to define what privacy is. More interestingly, it seemed that privacy is something that is perceived quite differently from person to person. Some participants looked at privacy as parts of laws and regulations (something "judicial"), while others described it more in the sense of a personal feeling of safety and integrity (something "subjective").

Privacy was considered important to most participants, but as previously stated, there were different opinions on what privacy implies. Many tables discussed if the traditional notion of privacy was adequate to handle the digital reality of today. Some participants went as far as saying that privacy was an illusion in the digital world we live in today, and that it was more important to create a framework to handle and manage all the data that is collected, than trying to stop the surveillance of citizens.

The participants were asked at the start and the end of the summit, if they were concerned that the use of surveillance-oriented security technologies eroded privacy (on individual and collective level). One can see that the participants became somewhat more concerned throughout the summit. Their concern grew more at the collective level than the individual.

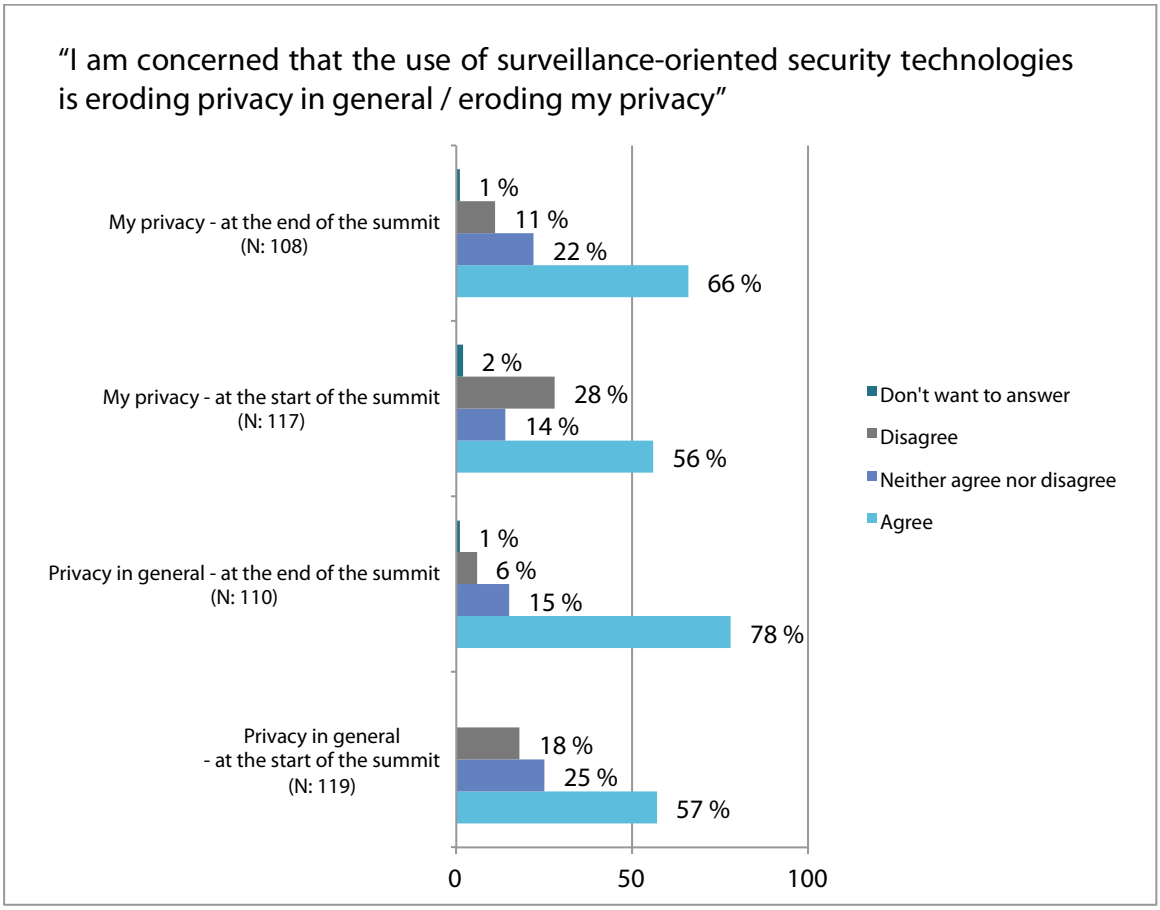


Figure 15: "I am concerned that the use of surveillance-oriented security technologies is eroding privacy in general / eroding my privacy" (Q8, Q9, Q95 and Q96)

To further investigate the relationship between the collective and individual level of privacy, the participants were also asked whether surveillance-oriented technologies only bothered them if it was used to track their own smartphone and online activities. For smartphone location tracking, only 12 percent agreed with this, while 73 percent disagreed. For deep packet inspection, 22 percent agreed and 65 percent disagreed. These questions clearly show that privacy is valued as a fundamental right for everyone, not just for oneself.

4.4.3 Individual privacy and personal data

"A simple wish, don`t store data you don`t absolutely need. Don`t use surveillance without serious suspicion of crime." Postcard from participant

The increasing amount of personal data that is collected was a recurring topic in the group discussions. More than two thirds of the participants were concerned that too much information is collected about them and that the collected information might be used against them at a later time.

The participants wanted actors that do collect data, to inform them that this is being done. Their concern about this related to the unease they felt about secret mass surveillance, especially from the use of deep packet inspection. One participant with minority background argued that deep packet inspection made him more conscious of how and what he communicated with others. He feared that social services like Facebook and Skype would become subject to surveillance, and the people no longer

dared to use these services to private communications. This would particularly be the case in countries with oppressive governments.

Many services inform their users through an agreement of "terms and conditions", but the participants pointed out that these are often long and complicated and written in a language which is difficult to understand. Companies should make this information much easier, so that the users actually know what they agree to and hence are able to protect their privacy and not use the service if they find the terms and conditions invading.

4.4.4 Trading privacy?

The idea that there is a trade-off between security and privacy is quite common - that an increase in security must lead to a decrease in privacy (or vice versa). At the citizen summit, the participants were asked to assess the intrusiveness and usefulness of the two security technologies. The questions were meant to identify if they supported the trade-off model or not.

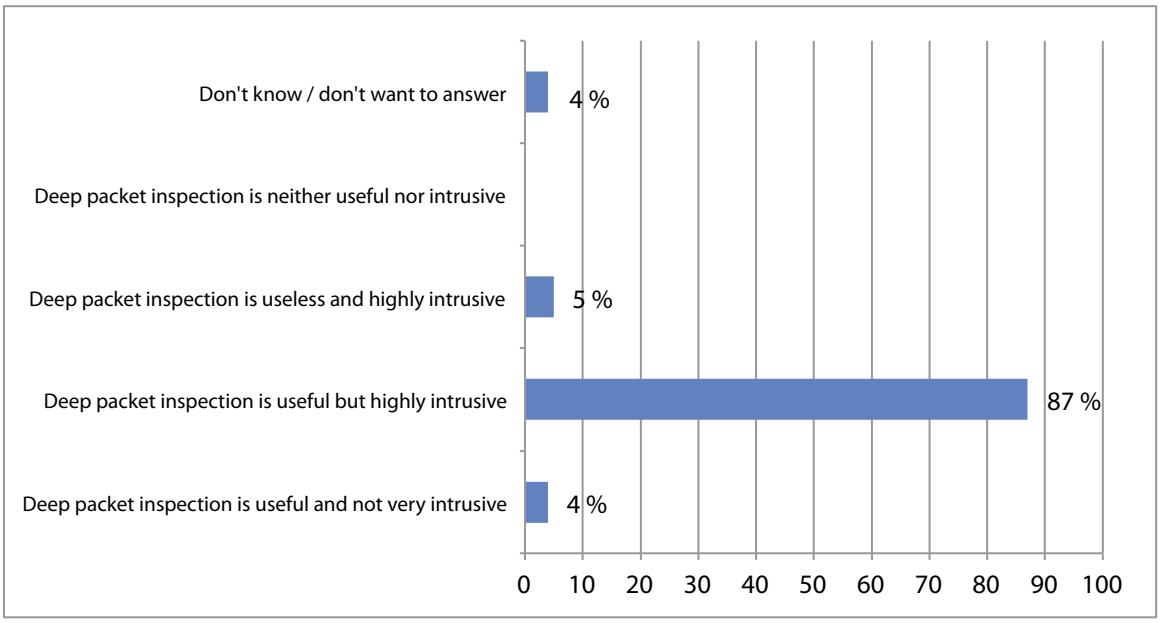


Figure 16: "Choose the option which better reflect your opinions" (Q79)

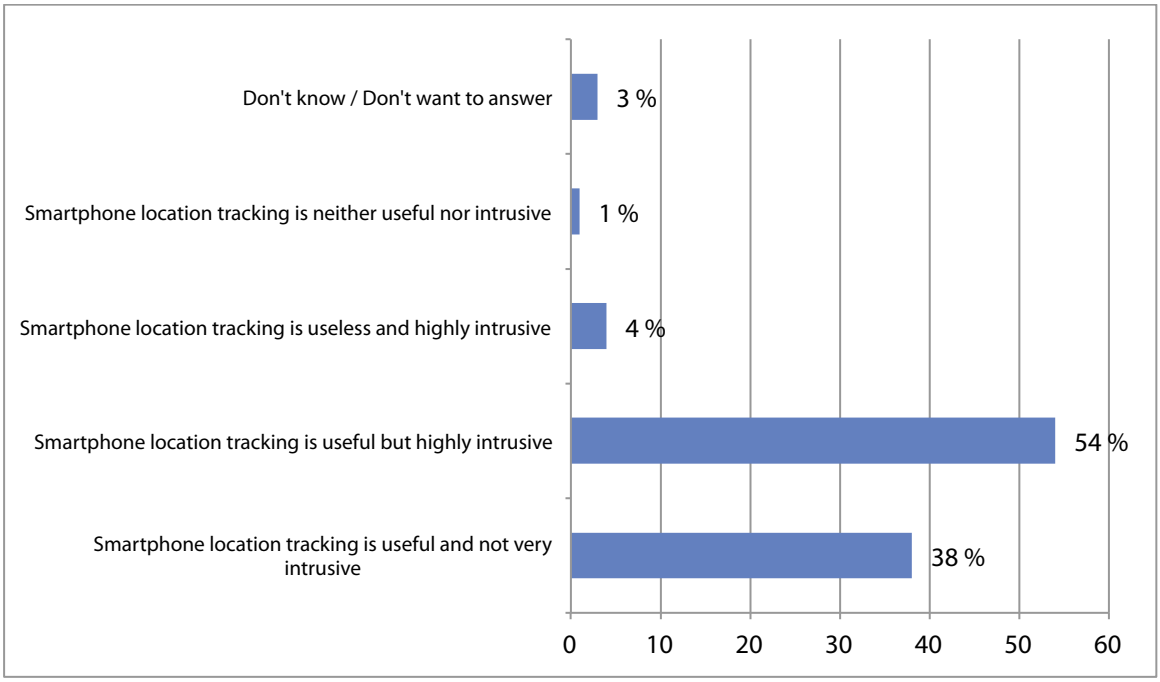


Figure 17: "Choose the option which better reflect your opinions" (Q80)

In Figure 16 and Figure 17, the participants who answered "[the technology] is useful but highly intrusive", are the ones who are likely to support the trade-off model. They consider the technology to be highly intrusive, but also find it useful for improving security. At the same time, the answers do not show the nuances in the participants' attitudes towards the technology or in what way they find it intrusive and/or useful.

During the table discussions the intrusiveness and usefulness were reoccurring topics. In Figure 16 and Figure 17, we see that there are few participants which find the technologies useless. In the discussions they separated between different uses, and made a distinction between uses that were acceptable and uses that were unacceptable and too intrusive. For deep packet inspection, there were many participants who supported the use if the goal was to reveal terrorism or prevent organized crime. A prerequisite for this use was that the security agency had a specific target and goal. Most of the participants expressed strong negative attitudes towards mass-surveillance of online activities of the general public.

"NO TO MASS SURVEILLANCE!!!" Postcard from participant

Localization of smartphones was considered highly useful by many of the participants. But in the same way as with deep packet inspection, the participants made distinctions between different kind of uses and users. While deep packet inspection is a technology used by private companies or security agencies, localization of smartphones can also be used by the citizens themselves. Many of the participants used this technology frequently, both for services and localization of family members (for example children or demented parents). This might be one of the reasons why quite many chose to answer that the technology is "[…] useful and not very intrusive" Figure 17). At some tables the participants expressed that they found location as less sensitive type of data then for example the content of their communication (which can be accessed through deep packet inspection).

4.5 Perceptions on the trustworthiness of security authorities

The trustworthiness of the institutions which use surveillance-oriented security technologies is an important aspect of how citizens assess the measures. From the discussions at the citizen summit we know that the participants were more positive towards these technologies when they were used for security reasons compared to commercial use.

Table 1 shows that there are also differences in the participants' attitudes towards security agencies, depending on technology. In general, the participants were more positive towards security agencies when they used smart phone location tracking compared to deep packet inspection.

Security agencies which use deep packet inspection / smartphone location tracking are trustworthy (N: 117 /114)		**Deep packet inspection**	**Smartphone location tracking**
	Strongly agree /agree	35.9 %	50 %
	Neither agree nor disagree	26.5 %	25.4 %
	Strongly disagree / disagree	33.4 %	9.6 %
Security agencies which use deep packet inspection / smartphone location tracking are concerned about the welfare of citizens as well as national security (N: 114 /115)			
	Strongly agree /agree	28.1 %	54.8 %
	Neither agree nor disagree	36.8 %	25.2 %
	Strongly disagree / disagree	28.1 %	15.6 %
Security agencies which use deep packet inspection / smartphone location tracking do not abuse their power (N: 117 / 114)			
	Strongly agree /agree	18 %	36.2 %
	Neither agree nor disagree	39.3 %	31.6 %
	Strongly disagree / disagree	36.8 %	28.1 %

Table 1: "Attitudes towards security agencies"

In the discussions the participants mentioned the uncertainty connected to deep packet inspection as one of the main reasons for their skepticism towards security agencies. Since they don't know who does this, and when it is going on, it is difficult to know whether to trust the authorities. In Figure 15, we also see that there are a quite high number of participants answering that they neither agree nor disagree to the statements.

Several participants mentioned NSA as an example of a security agency that didn't improve their trust in security agencies. After Edward Snowden's revelations about their methods of mass-surveillance, the participants at the summit found it difficult to believe that security agencies didn't abuse their power, or that they had the welfare of citizens in mind when they did their work.

The use of smartphone location tracking in investigations was more familiar to the participants. It is a common measure by the police, and is quite frequently mentioned in media coverage of criminal cases. This might have influenced their views on this technology and the security agencies which use location tracking in their work. One participant mention that the police often use location tracking to exclude people from their list of suspects, and that this "positive" use for innocent people made him think that the police also cares about the welfare of the citizens. For him, it was better to give up his location at the time of a crime (and therefore being excluded as a suspect), than going through immense questioning by the police.

4.6 Role of alternative security approaches

There are several alternative approaches to security which does not involve surveillance or collection of personal data. This could be neighborhood watch programs, more streetlights or a stronger focus on socio-economic factors that might lead to criminal activity. Some information on such approaches was presented in the information magazine that was sent to the participants before the summit.

When asked if they wished alternative approaches got higher priority, almost half of the participants agreed, while almost 30 percent neither agreed nor disagreed. These attitudes stayed the same throughout the summit. Although this could be interpreted as strong support for alternative approaches, the participants hardly mentioned this in the discussions. There were few concrete examples made, and none of the recommendations put focus on alternatives to surveillance and data collection in security-enhancing measures.

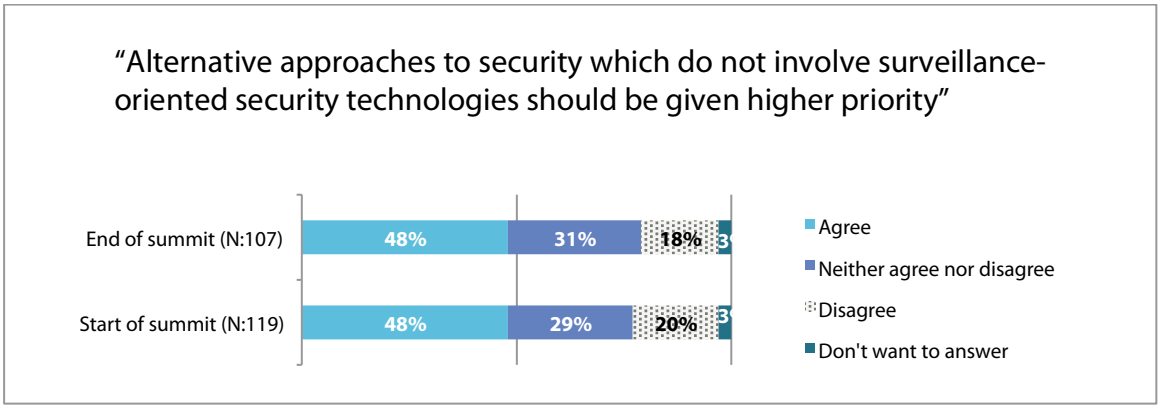


Figure 18: "Alternative approaches to security which do not involve surveillance-oriented security technologies should be given higher priority" (Q10 and Q97)

However, some of the discussions and recommendations included elements that could be interpreted as alternative approaches. One of these approaches is the need for information and education. The citizens wanted more information about what kind of data is collected about them, and when and how this is done. By having more information and educating children in school about privacy and technology, the citizens thought they would be able to take informed choices about their own use of technology. This included the right to refuse to use technology that bases its functionality on extensive use of surveillance.

The citizens were also concerned about the actors which use surveillance-oriented security technologies, and many tables mentioned the need for oversight bodies to "watch the watchers". They suggested the establishment of such bodies on an international or European level.

4.7 Citizens' recommendations to policy makers

For the last part of the citizen summit, the participants formulated their own recommendations to Norwegian and European policy makers. Every table made one recommendation, with a total of 24 recommendations[35].

The participants were free to include whatever they wanted in the recommendations, however most of them were along the lines of the specific topics which were discussed during the summit. Some included concrete advice on specific topics, while others were more general. Each table wrote one recommendation and elaborated on why they thought this was important and made suggestions for implementation of their recommendations.

[35] All recommendations are listed in Annex 10.1

4.7.1 Transparency, information, international regulations and education

There were four topics that recurred in almost all the recommendations. These were topics that had also been discussed repeatedly in the groups throughout the day. Below are presentations of the four topics, together with some of the arguments behind the recommendations.

Transparency

Organizations, both private and governmental, which collect data, must be open about this. They should state what kind of data they collect and why. Several groups made a concrete suggestion to create a "My page", where one can see a list of everyone who have stored your personal data, and a log of when it is used. One should also be able to block certain actors from using your personal data.

Information

In order to make informed choices, the citizens stressed the importance of getting enough information. How technology works and what kind of data is collected needs to be explained in an easy and acceptable way. Todays "terms and conditions"-texts are too complicated and often written in a language that is difficult for citizens to understand.

International regulations

Issues related to technology, security and privacy have become an international concern, and this should be reflected by having international regulations.

This will help to address the challenge of American apps and services not having to follow European regulations, even though the user is located in Europe.

In addition to international regulations, there should also be an international control body that can "watch the watchers" and make sure that the organizations that do collect personal data about citizens, does this within the limits of the law.

Education

Technology and privacy should be implemented in school curricula. This will enable kids to reflect and take informed choices when it comes to technology and privacy, and be aware of the challenges related to data gathering and surveillance.

5 Summary and Conclusions

Since the 1990's The Norwegian policies on national security have been guided by three core principles: liability, decentralization and conformity. In 2012, a fourth principle was added: cooperation. National security and safety has been an important issue for the governments since the cold war. But fragmented coordination and few incremental changes have caused many debates. Until the 22nd of July 2011, Norway has had very few incidents that have made a crisis-driven change in policies.

After the terrorist attacks in 2011 there has been an increasing focus on security measures, both politically, in the media and in public debate. The about NSAs mass-surveillance has also sparked a public debate on surveillance and privacy.

The SurPRISE citizen summit in Norway was successful in collecting citizens' views on surveillance, privacy and security, with specific focus on deep packet inspection and smartphone location tracking. Engaged citizens participated in lively discussions throughout the event, and contributed to the debate on surveillance and privacy in Norway.

The Norwegian participants had an inherent feeling of safety in their everyday life, and they consider Norway a safe country to live in. The Norwegian society has a high level of trust between the government and the citizens; and the participants assessed implementation of security technology by the government as effective and useful. But at the same time, our increasing digital society brings new challenges and treats that need to be considered. Even though the participants supported use of surveillance-oriented security technology to increase national security, they were more hesitant when private companies used the same technology for marketing or other commercial uses.

One of the things that concerned the participants was online security. Deep packet inspection is a technology that can be used to improve online security, but this was not a security measure that made the citizens feel safer. The effectiveness of the measure on individual security was overshadowed by the level of intrusiveness on the participants' privacy. They found deep packet inspection highly intrusive, and were worried about how the use might develop in the future.

Smart phone location tracking, was to a larger degree than deep packet inspection, enhancing their feeling of safety. This might be explained by a stronger familiarity with the technology, that the citizens know more about it and that they in many cases use the tracking-technology themselves. On a more general level, deep packet inspection was seen as positive for national security, while smartphone location tracking was assessed positive for both national and individual security. The participants found it worrying that they could not deactivate all tracking functions in their smartphones, and feared that it in the future would be impossible to move around without anyone knowing where you are.

The discussions at the summit gave a general support for the use of surveillance-oriented security technologies. The participants showed support for implementation, and this support increased during the summit. At the same time, the participants were concerned about infringement of their privacy, especially on the collective level. This concern did also increase during the summit. They were concerned that mass-surveillance could erode privacy (both at collective and individual level) and they wanted to protect this fundamental right.

Support for implementation of surveillance-oriented security technologies and concern for privacy increased during the summit. An explanation for this shift could be that discussing and learning more about technology and privacy, convinced some participants of the security-enhancing possibilities that lie in the technology, but also made them more aware of the intrusive nature of the same measures.

While it might seem that many of the participants were willing to trade their privacy for increased security, it is difficult to make a clear statement about this. The definitions and understanding of both privacy and security are blurred, and individual interpretations differ widely. Different use for different purposes and the different levels of privacy makes it difficult to make a clear statement about the trading of privacy for security.

When writing their own recommendations to policy-makers, there were few groups who recommended stopping surveillance completely. From the discussions, we know that many participants thougth that since surveillance already exists, it will be impossible to eliminate. Instead they wanted policy-makers to work for international regulations and control bodies and to limit surveillance to cases where there are

proven suspicion of criminal activities. The recommendations also focused on transparency and information to citizens – that we should know what kind of information is collected about us and our activities, and how this information is used. To make children able to take informed choices in the future, the participants also recommended stronger focus on technology and privacy in education.

6 Bibliography

Baugerød Stokke (2010): Mobiltjenesten Bipper overvåker barn ("Bipper monitors children") http://www.vg.no/teknologi/artikkel.php?artid=10017672

Bygrave and Aaø (2001): Privacy, Personality and publicity – An overview of Norwegian Law, in M. Herny (ed), international Privacy, Publicity and personality Laws. London: Butterworths http://folk.uio.no/lee/publications/Overview_Butterworths.pdf

Christensen, Lægreid og Rykkja (2012): How to cope with a terrorist attack? – A challenge for the political and administrative leadership. COCOPS Working Paper No. 6 (http://www.cocops.eu/wp-content/uploads/2012/08/COCOPS_workingpaper_No6.pdf)

Collective security – a shared responsibility. Action plan to prevent radicalization and violent extremism (2011) http://www.regjeringen.no/upload/JD/Vedlegg/Handlingsplaner/Radikalisering_engelsk.pdf

Data Protection Agency: http://datatilsynet.no/English/

Digitalt personvern (the organization «Digital privacy») http://www.digitaltpersonvern.no/

Meld. S 21 (2012-2013): Terrorberedskap. Oppfølging av NOU 2012:14 Rapport fra 22. juli-kommisjonen. (White Paper) http://www.regjeringen.no/nb/dep/jd/dok/regpubl/stmeld/2012-2013/meld-st-21-20122013.html?id=718216

Meld. St. 29 (2011–2012). Samfunnssikkerhet (White Paper) http://www.regjeringen.no/nb/dep/jd/dok/regpubl/stmeld/2011-2012/meld-st-29-20112012.html?id=685578

Meld. St 17 (2001-2002). Samfunnssikkerhet - Veien til et mindre sårbart samfunn (White Paper) http://www.regjeringen.no/nb/dep/jd/dok/regpubl/stmeld/20012002/stmeld-nr-17-2001-2002-.html?id=402587

NOU 2012: 14 Rapport fra 22. juli-kommisjonen (Green Paper) http://www.regjeringen.no/nb/dep/smk/dok/nou-er/2012/nou-2012-14.html?id=697260

NOU 2009:1 Individ og integritet. Personvern i det digitale samfunnet. (Green Paper) http://www.regjeringen.no/nb/dep/kmd/dok/nouer/2009/nou-2009-1.html?id=542049

NOU 2006: 6. Når sikkerheten er viktigst - Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner (Green Paper) http://www.regjeringen.no/nb/dep/jd/dok/nouer/2006/nou-2006-6.html?id=157408

NOU 2000: 24. Et sårbart samfunn - utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet (Green Paper) http://www.regjeringen.no/nb/dep/jd/dok/nouer/2000/nou-2000-24.html?id=143248

PRISE (2008): D 5.8 Synthesis Report –Interview meetings on Security Technology and Privacy

Privacy International (2011): Global surveillance monitor 2011.

Privacy International (2007): Global surveillance monitor 2007.

Rapport til Stortinget fra kommisjonen som ble oppnevnt av Stortinget for å granske påstander om ulovlig overvåking av norske borgere («Lund-rapporten») https://www.stortinget.no/Saker-og-publikasjoner/Publikasjoner/Dokumentserien/1995-1996/Dok15-199596/

Ravlum (2005): Pinning our faith on Big Brother … together with all the little brothers? Oslo: Transportøkonomisk institutt

Teknologirådet og Datatilsynet (2014): Personvern – Tilstand og trender (The Norwegian Board of Technology and the Data Protection Authority : «Privacy – status and trends»)

The Personal Data Act of 14 April 2000 No. 31 in English http://www.ub.uio.no/ujur/ulovdata/lov-20000414-031-eng.pdf

The PRISE project: http://www.prise.oeaw.ac.at/

7 List of Figures

8 List of Tables

9 List of Abbreviations

Abbreviation	Definition
BNP	Bruttonationalprodukt ("Gross domestic product")
CCTV	Closed circuit television
COCOPS	EU Project ("Coordinating for Cohesion in the Public Sector of the Future")
DPA	Data Protection Authority
DPI	Deep Packet Inspection
EC	European Commission
EOS-utvalget	Norwegian Parliamentary Intelligence Oversight Committee
EU	European Union
EURODAC	European Dactyloscopy
ICT	Information and communication technology
NIS	Norwegian Intelligence services
NSA	National Security Agency
OECD	Organization for Economic Co-operation and Development
PDA	Personal Data Act
PST	Police Security Services
PPP	Purchasing Power Parity
PRISE	EU Project ("Privacy enhancing shaping of security research and technology")
PRISM	Planning Tool for Resource Integration, Synchronization, and Management ("Surveillance program under the National Security Agency")
SLT	Smartphone Location Tracking

10 Annex

10.1 Table recommendations

Template[36]

Recommendations – content[37]

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?
1		
We think that the politicians' main responsibility is to 1) Write a legislation that is clear and unambiguous 2) ensure that the necessary resources are allocated to the task at hand and 3) control the use of DPI and geotracking and geotagging.	It is important to maintain the level of safety in the "Norwegian society". Appropriate resources should be made available to monitor the continuous innovation and development of IT-technology ("hardware", systems and "software"). Institutions such as the police, the	Surveillance, privacy and safety should not be politicized. A continuous assessment of, and public debate over, legislation, resources and the structure of societies control bodies is to be recommended. The police and other public institutions must be allocated enough resources for them to be at the very least on par with, if not

[36] 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.

[37] Translated from Norwegian

The politicians should be held accountable for the allocation of resources to these three recommendations.	military, and the Norwegian directorate for civil protection must have high-level competence which is future-oriented.	ahead of, criminals and others guilty of abusing information.
2		
A deliberate approach to the threats and challenges posed by technological development. Focus on the implementation of national as well as international measures. The consumers must be better informed and made more aware.	Technological development is irreversible and the judicial and legal institutions must pay attention to this.	Individual users of ICT must be given clear information about the consequences of that use. Build institutions which are competent and capable to judicially safeguard and preserve personal privacy and data storage. There should be clear and unambiguous guidelines, increased sharing of information and knowledge. Openness: knowing when we are under surveillance, and to what end and purpose. Limit the surveillance to specific actors with a predefined, overarching purpose. Allocate resources to and prioritize the writing of legislation regarding computer activity International cooperation.
3		
Develop a system of certification for apps and webpages where users actively grant their consent and are given information in a concise way, and are presented to what purposes this can and cannot be used. The service must clearly highlight whether or not the app/webpage is certified in accordance to Norwegian legislation.	Not knowing what information is stored and what legislation the information which is generated from the app is subject to.	
4		
Surveillance: Promote international/regional agreements covering what is allowed in what situations, and which rights internet-users should have. The people and especially children must be educated on the dangers of information sharing, and on which rights they possess. One must be able to sanction infringements.	Privacy on the internet is an illusion. People carelessly share sensitive information without there being any rules regulating the further use of that information. There is insufficient openness and transparency into what happens to that information. The information can be abused.	Educate teachers. The curriculum must be updated and have far greater ambitions than teaching "netiquette" to pupils. Informational campaigns. Diplomacy. Legislation. Supervisory body.

5		
The use of security technologies must be regulated in accordance with fundamental human rights, while important societal concerns must be safeguarded.	Preventing abuse Having the freedom to choose not to be under surveillance when on the move (freedom of choice). Example: «hiking without anyone seeing it». Who has the permission to do what? This should be monitored and shared (openness/ transparency). Safeguard and preserve national sovereignty and the rights of citizens.	Legislative regulation A global supervisory body. Norway as a nation should contribute and participate in international collaborative efforts. Knowledge/education Secure the IT-infrastructure.
6		
Regard for privacy, and property rights over one's own personal information should be a right.	Lack of information on how personal information is stored, shared and used.	Strict legislation, regulation and more transparency. Independent supervisory bodies (such as the Norwegian Consumer Council) should inspect foreign technologies and inform if they infringe on the consumers freedom of choice.
7		
Regulations and legislation on an international level (more integrated cooperation on privacy). Demand privacy by design, more transparency regarding what purpose the gathered data can be used for.	Global media -> requires international solutions across countries. Operators have too much power regarding the storage and use of data gathered from individuals/consumers.	Write a set of shared guidelines, legislation and regulations for the use of metadata. International body and cooperation on follow up of these. (Interpol as a start?) (Nobel Peace prize to Snowden)
8		
Strengthen self-determination through information- and knowledge proliferation at school, through informational campaigns etc. Empower citizens to be capable of making informed choices in the digital world and, of giving their informed consent when sharing personal data.	We are not truly aware of what services and products we are choosing, and do not know when our privacy is in danger.	- Educating teachers, also in kindergarten - Keeping the curriculum up to date - The terms and services agreements are difficult to understand. They have to be simplified. The governments must ensure that service providers are compelled to list both the advantages and inconveniences of data-collection.
9		
The competency and expertise on computer safety exists already. Listen to expert advice on risks, consequences, and suggestions	We not sure of how government authorities are storing and treating our personal information. Businesses and citizens need	Better awareness and an increase in competency on every level. International legislation.

for solutions. The efforts to make stored data safer are under continuous development. Systems must be subject to strict regulations.	information on surveillance – DPI is particularly disquieting. Not using such technology is no longer a real alternative. What is criminal behavior? What makes one a suspect?	Servers should be located in Europe. Require that commercial actors give consumers an informed alternative to being monitored, enforced by legislation which includes punitive measures.
10		
There are definitions in the Norwegian constitution which have to updated in the context of modern technology. We need to safeguard the fundamental rights and freedoms that the constitution has given us!	The definitions of today are outdated. The individual is not well enough protected. Freedom of expression/privacy are keywords.	The legislation should be international A change of legislation should focus on privacy No to surveillance which is in conflict with personal privacy (the Norwegian constitution) Strict rules and regulations for surveillance (safety-wise) Snowdens arguments: "It is cheaper to ask people than to have them under surveillance".
11		
Write a clear and unambiguous international legislation, regulating surveillance, privacy and security.	The abuse of communications data is an international problem which must be solved through international legislation.	-The EU should establish an independent supervisory body - Requirement of governments to inform its citizens of the consequences of the use of ICT.
12		
Every user should have the means to control their own use of technology. This principle should be written into international law. The general level of competency on privacy must be raised.	We as citizens and consumers have limited control of our own privacy. We know little about what personal information is used, to what purpose and by whom. As we have seen in the Snowden-case, the information is subject to misuse.	We must raise the awareness in the population, put pressure on service providers to provide open source codes, and to establish a functioning legislation. Limit the demographic and material growth worldwide. Establish a UN supervisory body for computer-technology and ICT.
13		
They should strive to write an international legislation (at the very least European) and establish a supervisory body which can enforce and regulate strict European/international privacy laws regarding DPI and smartphone geotracking.	Citizens and consumers are provided with too little information to make informed choices. *Citizens and consumers therefore have little control over their own privacy. *The advantages provided by security technologies such as DPI and geotracking are recognized, and their use must continue but only under strict conditions and with considerable transparency.	Deep Packet Inspection: it is acceptable if strictly regulated. DPI-surveillance should only be used after an individual is proven to be a suspect beyond reasonable doubt. The rules defining who are to be monitored should be very strict. Those who do the surveillance must themselves be subject to strict inspection, and the abuse of DPI-technology should be punished. Geotracking and smartphones: Consumers should be adequately

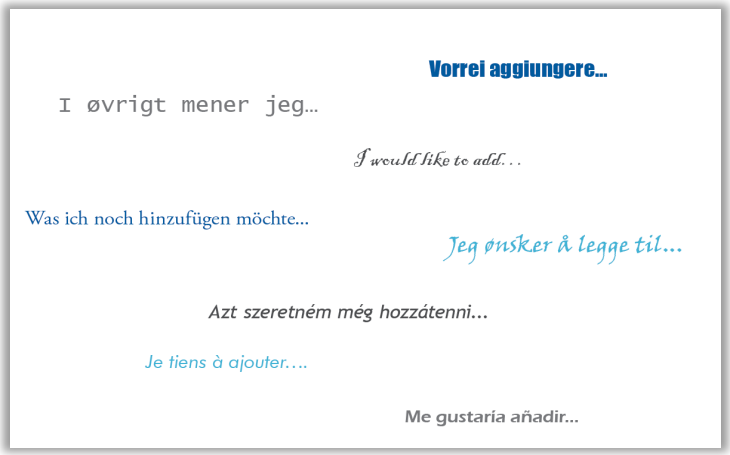
		informed by service providers so as to make them able to make informed choices, and give their informed consent, or provide them with viable alternatives should the searches not match their expectations regarding privacy. Geotracking is a very useful tool in search and rescue-operations, as well as other emergencies.
14		
Individuals must gain a complete overview of all data on them being stored. They must also be able to see which actors have applied to use the information, and what it is used for.	We will in any case not be able to stop the storage of data. To be able to safeguard rule of law, privacy and democracy transparency must be mutual.	This should be stipulated in national and international regulations. The law should comprise all actors, both public and private who stores information on individuals. One must also have the opportunity to reserve oneself for who shall have access on their data.
15		
Be proactive in legislation, where the overarching control lies in the political system.	Technology is ahead of legislation / The technological development is happening fast / Uncertainty concerning the political management, does it keep up? That privacy is maintained, even under changing technological circumstances.	-Political management -Legal basis -Focus on privacy -Control bodies are needed to ensure follow-up and prevention of abuse -Long-term goal: make the regulations international.
16		
Information and training: openness concerning authorities use of surveillance, as well as introduction of mandatory training in computer safety, privacy and ethics in schools.	The problem: The technology is vast, complex and has come about quickly. People know too little. [We] immediately see our own advantages of technology without understanding the scope of the consequences. Will function preventatively on criminals and create more security for the population in the use of the Internet. Learn benefits and disadvantages of technology, and make children able to make independent choices.	Mandatory training in schools Information campaigns to reach out to larger parts of the public (for instance through TV) "My page"-concept: what information exists about me? Webpage with information on what we are (concretely) monitored on (for instance: if you are a farmer it will be made clear to you that you are being monitored when buying fertilizer.)
17		
Computer technology is undergoing rapid development. The regulations must quickly take into account the development, set limitations and provide information necessary to ensure	We know too little about the technology we use every day.	There is a need for international regulations, as well as national information bureaus for information technology.

privacy. Producers must be made responsible.		
18		
Establish sound regulations to increase control over the use of the technology and to define acceptable use. The regulations must be international.	Minimize the risk of abuse (criminal acts) Ensure privacy Sanction criminal behavior	Develop regulations and guide lines and an independent control body. International cooperation Increase expertise and knowledge to be ahead (with political decision makers)
19		
More transparency. We want to have stricter regulations. A control body paying attention to the institutions that have access to people's personal information should be established.	Avoid abuse of a technology that provides many unknown possibilities. We do not wish that those with the most resources/capital shall decide. In that case technology might quickly come out of hand.	Look at the current regulations. Stricter criteria for providing concession for surveillance. It must be possible give (perform) sanctions towards institutions that do not operate by the book. The current regulations came before this young technology, one must therefore look at it attentively nowadays. People who are innocently affected or accused, should be deleted from the register, and get to know about it. Possibility for a right of reservation against unwanted technology that wants to collect data. Finally: We want the authorities to provide a correct list over which institutions are monitoring us. This also applies for tracking.
20		
International regulations: Requirement of court ruling/concrete suspicion before the authorities can gain access to private data. Only consensually based commercial utilization that must be optional.	Those who perform deep packet inspection and location tracking of smart phones both in and outside of Norway, are not comprised by sufficient regulations. Privacy is therefore not well enough maintained. The regulations must also apply outside of Norway for them to have effect.	-Regulation and effective enforcement (appeal body, judicial court etc.) -Facilitate motivation for development of technology that safeguard privacy.
21		
You must ensure that private and public actors are open about which data they collect and for which aims, as well as make sure there are national and international regulations that protects privacy.	-Users need to know how their information is being used and have the possibility to make their own decisions.	-Because the data traffic is flowing freely over national borders there is a need for international collaboration to maintain privacy. -Strict control bodies ensuring that the regulations are being followed.

22		
Raising of awareness through information and raising of competence in the population.	Need of updated competence in the technological development for increased safety.	"The Norwegian mountain rules" for internet, TV-programs (consumer help programs and children's programs)/commercials with simple messages/information, TV-debates. More focus in schools through projects, awareness-raising through lectures/tasks/films online. Important to include parents.
23		
To maintain the rule of law in Europe and globally there is a need for international control bodies of information gathering and storing.	Prevent abuse, safeguard privacy and rule of law.	Can it go through the United Nations? There must be an authority that can make decisions and administer this task.
24		
We recommend stricter demands for competence development, work towards changing attitudes and education of the population and authorities concerning privacy (including deep packet inspection and localizing functions).	We experience that the population does not know the consequences of leaving information on the net. We experience at the same time that the authorities must become even better and gain better competence in the field.	-The public sector must use media for education of the population -> ethics, values and campaigns for changing attitudes. Knowledge concerning dangers. -We demand to get information of when personal data is being used by externals (either public authorities or private actors) -> duty of disclosure. -Information on privacy and security must be incorporated in the educational system.

10.2 Postcards

Template



Postcards - content[38]

I.

1. Attend to privacy – Safeguard privacy laws
2. The democracy must be protected
3. Take care of every citizens safety without infringe on privacy
4. Work for approximately the same legislation in every country.
5. Develop technology on fax, so there can be a one-to-one connection in addition to the internet.

II.

Inform the public about what privacy is and what our use of information technology entails. Establish a international control body, and legislation which strengthens all consumers rights. Make information on privacy easily accessible and easy to understand. Regulate and make demands for providers of security- and information-technology so that they do not have the right to decide over the information they have on consumers.

---

[38] Translated from Norwegian

III.

- Demand built in privacy as default settings.
- Make technology-neutral laws which cover old and new laws.

IV.

Forms of consent should be simple and easy to understand, a point wise fashion is recommended, so people have an opportunity to see the consequences of the choices they make on the internet.

V.

Transparency and information on benefits and disadvantages related to the use of computer technology such as Internet, social media, smart phones and e-mail provided to the public is very important.

VI.

Stop material growth! –Smartphone technology is a result of growth as well as a driver of growth. Unlimited growth on a limited growth-bearing planet is now unsustainable. Technology must now be given explicit priority to serve the "general welfare", in a materially sustainable manner. Individual rights – of UNDHR – must be protected well in this context.

VII.

A simple wish, don`t store data you don`t absolutely need. Don`t use surveillance without suspicion of serious crime.

Demand secure and reasonable use of data from private companies.

Punish those who don`t.

Remember Franklin`s words on safety vs freedom.

VIII.

Remember that you can`t catch those you claim you`re after, with these tools.

IX.

Be precautionary. Protect privacy.

X.

-Internet and phones have been made into necessary tools for society. Society must therefore make these safe and make sure that privacy is maintained.

-Even the access into personal information is trans boundary, and judicial warrant based on concrete suspicion must be required, before access is given.

-If this is not done, personal integrity and behavior is violated on all levels, even on societal level, so that utterances concerning society, and therefore the democracy suffers.

-The state must secure its population deletion of information. Sale of information should be based on consent, and be a voluntary alternative for the user: ie. a right to gain access to the program/product without giving up information.

XI.

Technology that can be abused will be abused!

-This appears to be an inherent law, which must be observed, in all practical applications of technology. I.e. abuse – protection must be built-in.

XII.

[I] wish to receive annual "reports" on who stores and uses information on me.

XIII.

Reverse the Data Retention Directive. Based on privacy concerns.

XIV.

NO TO MASS SURVEILLANCE!!!

XV.

Tighten in what information (national insurance number) in the population register that is being handed out. Not a enough with a phone call. Becomes exploited by criminals. Can open bank account. Have been subjected to this through a not-for-profit organization.

XVI.

Use open source software.

XVII.

I think that every single user has the right to get the information gathered on oneself handed out, and also to ask for the information to be deleted.

XVIII.

As long as we have Democracy and Rule of law our human rights will be safeguarded. Privacy is a part of that.

XIX.

[I] see it as very important to keep an analog net (landline) as an "aggregate" in crisis situations. For instance: The fire in Flatanger, where the police had to use landline for internal communication. Base stations can fall out!

[I] hear that Telenor is shutting down the analog net in few years. Allow us to keep the "safety net" which the landline is!

XX.

We cannot facilitate a world where everyone is treated as a suspect. To combat terror and other crimes one must allocate more resources to police and psychiatry.

I am completely against mass surveillance.

XXI.

Introduce information/computer safety as a mandatory subject in primary education. Those growing up should learn the benefits and disadvantages of their use of computers, and develop an informed relationship to privacy from an early age. They are active users of the Internet from 7-8 years of age.

XXII.

GIVE EDWARD SNOWDEN ASYLUM IN NORWAY!

XXIII.

Give Edward Snowden asylum in Europe!

XXIV.

Give Edward Snowden asylum in Norway.

Edward Snowden is a hero of our time.

XXV.

HELP EDWARD SNOWDEN.